PsySecure

MINIMIZE WHAT CAN BE KNOWN

OSINT DEFENSE & SECURITY FRAMEWORK

A COMPREHENSIVE FRAMEWORK FOR ORGANIZATIONS TO DEFEND AGAINST THREATS LEVERAGING OPEN SOURCE INTELLIGENCE (OSINT)

The OSINT Defense & Security Framework (ODSF) is designed to help organizations protect against open-source intelligence gathering and minimize their digital footprint.

FA1	FA2	FA3	FA4	FA5
DIGITAL FOOTPRINT REDUCTION	SOCIAL ENGINEERING DEFENSE	TECHNOLOGY EXPOSURE MANAGEMENT	EXECUTIVE EXPOSURE PROTECTION	CONTINUOUS MONITORING AND RESPONSE

Version 0.3.0 · Public Draft

CONTENTS

Deny attackers the public information their reconnaissance depends on.

The complete framework: five focus areas, 34 subcategories, and 150 controls, with implementation guidance, evidence cores, scoring rubrics, and a baseline subset for small organizations.

THE FIVE FOCUS AREAS

ORIENTATION

FOCUS AREAS AND CONTROLS

ASSESSMENT AND ADOPTION

END MATTER

EXECUTIVE SUMMARY

OSINT Defense & Security Framework

Open-source intelligence (OSINT) is the collection and analysis of publicly available information. Investigators and security teams rely on it daily; attackers rely on it for the same reason: it is accurate, abundant, and free.

Reconnaissance opens the cyber kill chain. Adversaries piece together fragments of public data into detailed profiles of an organization, its technology, and its people, then turn those profiles into spear-phishing, social engineering, and technical exploits without touching the target's perimeter. In the 2023 MGM Resorts and Caesars Entertainment intrusions, Scattered Spider used LinkedIn data to impersonate staff convincingly enough to get past the IT help desk, and the same playbook took down UK retailers including Marks & Spencer in 2025, at a cost in the hundreds of millions of pounds.

The business risk is direct. An expanded digital footprint can reveal employee names and addresses, the technology stack, supplier relationships, and even staff photo identification: a roadmap for an attack. Exposed addresses feed credential stuffing, public detail about executives feeds business email compromise, and with enough minor personal detail a criminal can pose convincingly as a colleague or a trusted vendor.

Exposure carries physical consequences as well. High-profile executives are targets of doxing campaigns that publish home addresses, family details, and travel patterns. The murder of UnitedHealthcare CEO Brian Thompson in December 2024 is the starkest recent example: the attacker planned around a publicly announced investor conference and was waiting outside the venue. Ransomware crews now bring the same leverage into negotiation: Semperis' 2025 ransomware study found physical threats against staff in 40% of attacks as criminals look for new ways to force payment, intimidation assembled from the same public fuel of addresses, family ties, and routines.

OPERATING PRINCIPLE

Minimize what can be known. Every control in this framework reduces what an adversary can find, connect, and act on.

ODSF FOCUS AREAS

FA1	Digital Footprint Reduction
FA2	Social Engineering Defense
FA3	Technology Exposure Management
FA4	Executive Exposure Protection
FA5	Continuous Monitoring and Response

psysecure.com/odsf

EDITION NOTICE

About This Document

This is the published edition of the OSINT Defense & Security Framework (ODSF), version 0.3.0 (Public Draft), released June 11, 2026, generated from the canonical framework source maintained by PsySecure. The canonical JSON edition, changelog, and new releases live at the framework home: https://psysecure.com/odsf/.

- **Version**: 0.3.0 (Public Draft), released June 11, 2026
- **Author**: Ray Heffer
- **Publisher**: PsySecure
- **License**: CC BY 4.0 (https://creativecommons.org/licenses/by/4.0/)
- **Canonical home**: https://psysecure.com/odsf/
- **Changelog**: https://github.com/locksec/odsf
- **Copyright**: © 2025-2026 PsySecure

License notice. Framework content, including this document and the canonical JSON edition, is licensed under Creative Commons Attribution 4.0 International. You may copy, redistribute, adapt, and build on the framework in any medium or format, including commercially, provided you give appropriate credit, link to the license, and indicate any changes. The complete license terms, the trademark statement, and the license history are published with the framework at https://psysecure.com/odsf/.

Attribution. Attribute reuse and adaptations as: OSINT Defense & Security Framework (ODSF) v0.3.0. Author: Ray Heffer; Publisher: PsySecure. Source: https://psysecure.com/odsf/. License: CC BY 4.0.

Proprietary exclusions. The ODSF Mapping Library, PsySecure's control-level curated mapping database with its annotations, scoring, and APIs, is a separate proprietary product outside the open grant. Focus-area alignment metadata published in the framework itself is CC BY 4.0 content.

Licensing contact. https://psysecure.com/contact

Framework Positioning

The OSINT Defense & Security Framework (ODSF) is an OSINT risk management framework created by Ray Heffer and published by PsySecure. It exists to counter a specific and growing pattern: adversaries weaponizing public information against an organization's most valuable asset, its people. ODSF is a controls-based model. It gives organizations a structured way to reduce their digital footprint, defend against OSINT-driven reconnaissance, and protect the organization and its personnel from targeted attacks, treating open-source exposure as a primary attack vector.

The framework is openly licensed under Creative Commons Attribution 4.0 International (CC BY 4.0): organizations can adopt it, adapt it, and build on it with attribution, while PsySecure maintains the canonical source and version governance. The About This Document page states the license and attribution terms in full.

ODSF is organized into five focus areas, each owning one aspect of OSINT risk management:

- **Digital Footprint Reduction**: minimizing the public exposure of sensitive or exploitable information about the organization and its people.
- **Social Engineering Defense**: preparing people and processes to withstand attacks built on public information.
- **Technology Exposure Management**: controlling and hardening the technical attack surface discoverable through open sources.
- **Executive Exposure Protection**: safeguards for high-profile individuals who face elevated targeting and personal risk.
- **Continuous Monitoring and Response**: ongoing surveillance of public data for emerging threats and leaks, and the capability to respond quickly.

Each focus area divides into subcategories, and each subcategory states an objective and contains controls. Control descriptions state the outcome an adopting organization implements; implementation guidance illustrates how that outcome is commonly achieved. The conventions section defines this boundary precisely, the assessment section provides a scoring rubric and a baseline subset for small organizations, and the glossary defines the framework's load-bearing terms.

ODSF stands alone and is built to complement the standards an organization already runs. Each focus area carries category-level orientation to NIST CSF 2.0; control-level crosswalks to external standards are published separately as ODSF mapping packs. Many controls reinforce well-known security principles, so a program can connect its existing asset management,

awareness, and monitoring work to the framework without rebuilding it. The scope stays deliberately narrow: identifying and securing the information footprint adversaries target during reconnaissance, the gap general-purpose frameworks leave open.

Defending with ODSF is an ongoing cycle of assessment, reduction, monitoring, and adaptation. Public information regenerates: marketing publishes, employees post, vendors leak, data brokers re-list. Organizations that apply the controls on a cadence make OSINT collection expensive, slow, and unreliable for the adversary, and the effect compounds: each closed exposure removes raw material a later attack would have used.

The Control Confidence Gap

Every security control rests on assumptions about what an attacker cannot know or convincingly fake. Help-desk identity verification assumes a caller cannot recite an employee's manager, start date, and mobile number. Payment approval assumes a video call showing the CFO's face and voice is the CFO. Account recovery assumes the answers to fallback questions are private. Public information breaks these assumptions silently: the control still operates, the audit still passes, and the protection is gone. ODSF names this condition the Control Confidence Gap: the loss of justified confidence in a security control when publicly available information weakens an assumption the control relies on.

The framework treats the Control Confidence Gap as its triage lens. Exposure findings record which control assumption an exposure weakens, so remediation priority follows attacker value rather than data sensitivity alone: a staff directory is a low-sensitivity page and a high-value pretext kit, and the gap it opens in help-desk verification is what makes it urgent. The assessment section builds this into finding severity, and ODSF mapping packs will publish detailed gap records, with mappings to external frameworks, as versioned companion artifacts.

Conventions and Interpretation

The conventions below govern how every focus area, subcategory, and control in this framework is read.

Normative language. Control descriptions state the outcome an adopting organization implements and are the normative layer of the framework. Implementation guidance is informative: it illustrates how the outcome can be achieved and is neither exhaustive nor required verbatim. Focus-area descriptions, business rationales, and scope statements are informative context. Each control's evidence_core is the reference evidence set for scoring levels 2-3: the rubric's evidence requirement means those core fields or documented organization-defined equivalents that evidence the same outcome. The fuller evidence fields named in implementation guidance inform the level-4 verification depth. Glossary definitions are normative for the meaning of defined terms; any obligation a glossary entry states is owned by the control or section that cites it.

Routing and ownership. Statements that route work to another focus area, subcategory, or control are normative boundary assignments: they declare which part of the program owns the work and its evidence. A route to a focus area (for example, FA3) assigns ownership at program level; a route to a control ID assigns it to that control's evidence records. Where a route assigns implementation to another program or owner, the owning program's records satisfy the routed control's evidence expectation by reference; the routed control records the pointer rather than a duplicate ledger.

Control ID stability. Control IDs are stable: a published ID is never renumbered, reused, or reassigned, and numbering gaps left by retirements are permanent. When a control is merged or folded into another control, the ID is retired with an entry in the retired_controls registry recording its last name, the retiring version, the disposition, and the successor control that owns the scope; a citation of a retired ID resolves through the registry to that successor. New controls take the next unused number in their subcategory.

Related controls. Each control's related_controls field lists the control IDs its description and guidance explicitly reference. The field is navigational metadata derived from the prose at release time, never hand-edited, and carries no normative weight beyond the routes and references it indexes. Program-level routes to a focus area or subcategory are ownership assignments per the routing convention and are deliberately not expanded to control IDs.

Applicability and scale. Each control carries an applicability object. from_scale names the smallest organization scale where the control is ordinarily proportionate: micro (no security function; consultancy-delivered adoption per the assessment section), small (a part-time security owner), mid (a dedicated security function), large (a program with specialist owners). Controls above an organization's scale remain available as exposure and resources grow. condition, where present, names the predicate that makes the control applicable; when the

predicate is false the control is recorded as not applicable rather than scored. Reference cadences in guidance are defaults; organizations may substitute a documented equivalent cadence.

Tools and examples in guidance. Vendor, product, tool, and platform names appearing in guidance are illustrative examples only, never endorsements or requirements.

Planned companion artifacts. Mapping packs and executive-protection extensions are planned companion artifacts that are not yet published. Routes referencing them denote intended future ownership: until publication, mapping-pack questions are governed by FA5.SC6.C2, and executive-protection-extension routes default to FA4 ownership for any organization-relevant remainder.

External references. External standards are cited inline with edition or document number where they are load-bearing, for example NIST CSF 2.0, NIST SP 800-63B-4, RFC 9989, and RFC 9116.

Threat Model

Orientation for the adversary classes the controls assume. Control text says “attacker”; this section names the recurring capability classes behind that word so adopters can read each control against the adversaries that matter for their profile. Archetypes are generic capability classes, consistent with the conventions on illustrative naming. Operational threat assessment stays with the organization: FA1.SC1.C4 grades exposure findings, FA5.SC3 owns the scoring method, and control depth is calibrated to organization size, sector, public profile, and regulatory exposure.

The reconnaissance path

OSINT-driven attacks run a repeatable path: collect public information, correlate it into a target model, then run a pretext or exploit against the seam the model reveals. Each focus area interrupts named stages, and FA5 operates across all of them.

- **Collect.** Harvest reachable public material: websites, filings, social platforms, data brokers, breach and stealer data, certificates and DNS, code repositories, app-store artifacts, recruiting content, and archives. *Interruption:* FA1 shrinks what exists and governs what gets published; FA3 reduces the technical surface and resists bulk and AI-assisted collection (FA3.SC5.C1); FA4 reduces people-linked exposure for executives and high-risk personnel.
- **Correlate.** Link people, roles, infrastructure, schedules, and authority into a usable target model: org charts joined to broker profiles, personal telecom joined to recovery workflows, certificates joined to internal naming, calendars joined to travel. *Interruption:* FA1.SC4 suppresses people-linked records; FA4.SC5 governs location, calendar, and appearance signals; FA5.SC7 reviews and monitors identity linkage; FA3.SC1 keeps the public asset graph from disclosing internal structure.
- **Pretext and exploit.** Act on the model: impersonation and verification abuse, account-recovery and help-desk attacks, SIM swap, targeted phishing and deepfake requests, technical intrusion against exposed services, coercion and harassment. *Interruption:* FA2 supplies the verification spine for human seams (FA2.SC2, FA2.SC3, FA2.SC7); FA4.SC2 hardens executive accounts and telecom; FA3.SC2 closes externally exploitable technical exposure, including outbound domain authentication (FA3.SC2.C6).

FA5 operates across every stage: it detects exposure and abuse signals (FA5.SC1), responds and takes down (FA5.SC2), scores and reports (FA5.SC3), and feeds findings back into minimization, training, and hardening across FA1 through FA4.

Adversary archetypes

ADVERSARY 01

Opportunistic fraud operator

01

Objectives. High-volume financial fraud at low cost per attempt: payment redirection, payroll diversion, gift-card and purchase-card lures, credential phishing.

Tradecraft. Bulk harvesting of contact directories, breach dumps, brokered lists, and public role data; light correlation; templated pretexts sent at scale and abandoned quickly when verification friction appears.

Framework response. FA1 data minimization cuts the harvestable fuel; FA2.SC2.C1 request classes and out-of-band verification break the lure-to-payment chain; FA2.SC3 phishing-resistant authentication removes the replayable-credential payoff; FA3.SC2.C6 outbound domain authentication blocks lookalike mail; FA5.SC1 breach monitoring catches credential supply early.

ADVERSARY 02

Targeted intrusion crew

02

Objectives. Interactive intrusion against a chosen organization for ransomware staging, data theft, or fraud, run through human and recovery seams rather than software exploits.

Tradecraft. Deliberate correlation of org charts, role and vendor relationships, personal telecom exposure, and stealer-log credentials; help-desk and service-desk impersonation, SIM swap, MFA fatigue and session-token replay, voice pretexts against named staff.

Framework response. FA2.SC3.C3 and FA2.SC3.C4 close the recovery seam with identity proofing before authenticator changes; FA2.SC7 verifies voice and video requests without personal-knowledge questions; FA4.SC2.C2 hardens executive telecom against port-out and SIM swap; FA5.SC1.C1 treats stealer-log session tokens as MFA bypass with revocation triggers; FA2.SC1.C4 makes pressure to bypass verification a reportable event.

ADVERSARY 03

Doxing and harassment actor

03

Objectives. Intimidation, coercion, retaliation, or extortion against staff, executives, or their households; exposure itself is the weapon.

Tradecraft. Assembly of home addresses, relatives, photos, routines, and contact paths from broker profiles, social platforms, public records, and historical archives; publication or threatened publication to apply pressure.

Framework response. FA1.SC4.C1 suppresses workforce broker exposure before it is weaponized; FA4.SC1 and FA4.SC5 reduce executive and household exposure under consent-scoped authority; FA5.SC2.C1 carries the employee doxing and harassment playbook class with HR ownership; FA1.SC6 manages archive persistence honestly where removal is impossible.

ADVERSARY 04

Persona infiltrator

04

Objectives. Access through assumed identity rather than intrusion: fraudulent employment, fake recruiters harvesting credentials or payments, synthetic candidates, paid insider recruitment.

Tradecraft. Personas built from recruiting posts, org charts, project names, and staff profiles; deepfaked interviews and references; outreach to employees through hiring and professional channels where trust defaults are high.

Framework response. FA2.SC1.C5 trains high-risk roles on hiring-lifecycle attack paths; FA2.SC7.C2 verifies candidate identity live during interviews; FA1.SC3.C5 limits the recruiting-content intelligence personas are built from; FA5.SC1.C2 watches for insider-recruitment solicitation; FA5.SC5.C4 governs the org-structure exposure that makes outreach credible.

ADVERSARY 05

Persistent targeted collector

05

Objectives. Long-horizon advantage: espionage, durable access, supply-chain positioning, or market-moving fraud against a high-value organization or person.

Tradecraft. Patient, well-resourced collection sustained across years: archives and caches, AI-assisted correlation at scale, supplier and household context, travel and event patterns; collection persists even when individual exposures close.

Framework response. FA1.SC6 records what cannot be removed and compensates, including AI training-corpus persistence; FA3.SC5.C1 resists automated and AI-driven collection; FA5.SC7 limits identity correlation across platforms; FA4 applies its full consent-scoped depth to the people such programs target; FA5.SC3 keeps severity honest when exposure is irreducible.

Digital Footprint Reduction

Digital Footprint Reduction involves identifying, managing, and minimizing the online information exposure of an organization and its members. This category covers controls that limit the amount of sensitive or exploitable data available to adversaries via open sources. Reducing the digital footprint helps deny attackers the raw material for reconnaissance, shrinking the attack surface that an adversary's OSINT collection can reach. This focus area broadly orients to NIST CSF 2.0 governance, policy, asset management, and risk assessment categories. It also reflects data minimization principles found in privacy laws and standards, keeping only necessary information publicly accessible.

Business rationale. In any business environment, completely hiding all information is unrealistic since companies need an online presence to operate. However, many organizations unknowingly expose far more data than necessary, which attackers can exploit. Public websites, social media, marketing materials, domain records, Git repositories, case studies, and cloud services may all leak details useful to attackers. By systematically closing these exposures, organizations reduce the chance that this data falls into the wrong hands. Fewer exposed details mean fewer clues for attackers, directly reducing the likelihood of targeted social engineering or technical attacks succeeding. For example, if an attacker cannot easily find employee emails, the technology they work with, or their team structure, then it becomes far more difficult for them to craft convincing phishing campaigns or find known vulnerabilities to exploit. Therefore, digital footprint reduction provides preventive security value and peace of mind to business owners, who might otherwise be unaware of how much of their organization's data is 'floating' around publicly.

Scope. This category includes both organizational data (e.g. network info, documents, websites) and personal data of employees and key individuals. It spans policy measures, technical measures, and proactive clean-up efforts.

NIST CSF 2.0 orientation: GV.RM · GV.PO · ID.AM · ID.RA

Focus-area alignment entries are broad orientation metadata indicating thematic overlap with NIST CSF 2.0 categories. They are not conformance mappings, control-level crosswalks, or claims of coverage. Control-level mappings to external standards are published separately as ODSF mapping packs.

FA1.SC1: Footprint Inventory and Assessment

Objective. Establish and maintain an evidence-backed view of the organization and workforce information that an external actor can discover. The inventory should connect each exposed item to an owner, source, affected business process, likely abuse path, Control Confidence Gap,

remediation status, and review cadence so footprint reduction can be governed rather than treated as a one-time cleanup.

FA1.SC1.C1: Identify Public Assets and Data

Maintain an owner-assigned inventory of public-facing organizational assets, data sources, and workforce identifiers that can be discovered through open sources.

Implementation guidance:

- Catalog corporate websites, subdomains, microsites, landing pages, developer portals, support portals, app store listings, and other official public properties.
- Record domains, DNS records, certificate transparency entries, WHOIS/registrar records, public IP ranges, externally reachable cloud resources, and storage locations that expose organizational context.
- Inventory official social media accounts, executive or spokesperson profiles used for business communications, support/community spaces, and other channels that represent the organization.
- Document third-party locations where organizational information appears, including job boards, press wires, customer directories, analyst pages, case studies, vendor listings, and partner portals.
- Identify workforce identifiers that create business risk when public, such as role-linked email formats, named privileged users, finance/procurement contacts, security team members, and support escalation paths.
- For each inventory item, capture source URL, owner, data category, business context, last verified date, intended public status, and evidence artifact.

Evidence core:

- Inventory of public assets, accounts, and workforce identifiers with owner per entry
- Source URL and last-verified date per inventory entry

Applicability: from micro scale.

FA1.SC1.C2: OSINT Footprint Assessment

Perform recurring externally oriented OSINT assessments that validate the inventory and discover public exposures from an attacker perspective.

Implementation guidance:

- Use search engines, archived pages, certificate transparency, DNS/subdomain enumeration, breach corpuses, paste sites, code platforms, data brokers, public records, and social platforms to test what an external actor can collect.
- Search for sensitive documents, credentials, API keys, internal names, exposed cloud assets, personal data tied to business roles, and unauthorized copies of organizational content.

- Include controlled use of common OSINT collection tooling, such as host and service search engines, DNS and subdomain enumeration utilities, link-analysis platforms, public code search, and repository secret scanners, where legally and operationally appropriate.
- Compare assessment results against the approved inventory to identify newly exposed assets, stale records, unauthorized publications, and outdated assumptions.
- Run assessments on a defined cadence and during high-risk events such as acquisitions, product launches, layoffs, executive changes, incidents, or major vendor changes.
- Store repeatable evidence: query examples, screenshots or exports, timestamps, source URLs, assessor notes, severity rationale, and remediation tickets.
- Reference cadence: annual assessment; organizations may substitute a documented equivalent cadence.

Evidence core:

- Dated assessment record with assessor, sources queried, and screenshots or exports
- Findings reconciled against the approved inventory with new exposures flagged
- Remediation ticket or risk decision per confirmed exposure

Applicability: from micro scale.

FA1.SC1.C3: Third-Party Footprint Mapping

Map third-party and affiliate publications that expose organizational information, and track whether each disclosure is authorized, necessary, and risk-accepted.

Implementation guidance:

- List vendors, partners, subsidiaries, agencies, contractors, marketplaces, integrators, customer references, and affiliates that publish or host information about the organization.
- For each third party, identify the exposed data elements, publication source, data-sharing agreement or approval basis, business owner, and permitted disclosure level.
- Review partner case studies, testimonials, support docs, marketplace listings, shared documentation, public project pages, and integration guides for unauthorized or excessive details.
- Separate content exposure from technical third-party infrastructure risk. Technical shared infrastructure and access should be mapped in FA3, while FA1 records what the third party publishes or reveals publicly.
- Categorize third-party exposures by reconnaissance value, such as named contacts, customer logos, project names, technologies, facilities, timelines, or internal process details.
- Create notification and remediation paths for unauthorized disclosures, including takedown contacts, contract owner, legal reviewer, target response time, and closure evidence.

- Monitor third-party changes and breach notices that could alter the organization's public footprint or expose previously non-public information.

Evidence core:

- Third-party publication map naming exposed data elements and approval basis per source
- Takedown or remediation request record with response and closure evidence
- Risk-acceptance record for disclosures that remain published

Applicability: from small scale.

FA1.SC1.C4: Risk Analysis of Exposed Information

Evaluate each discovered exposure for sensitivity, abuse path, weakened control assumption, business consequence, and remediation priority.

Implementation guidance:

- Classify exposures by category, such as credentials/secrets, technical stack, network/service details, workforce PII, customer/prospect data, financial/procurement context, facilities/location data, and corporate strategy.
- Document how an attacker could use the item for phishing, impersonation, account recovery abuse, vendor fraud, vulnerability targeting, physical targeting, privacy harm, competitive intelligence, or incident escalation.
- Identify the Control Confidence Gap created by the exposure, such as weakened identity verification, weakened access-control assumptions, exposed vendor-management dependencies, reduced fraud detection confidence, or impaired incident response.
- Assign severity using impact, likelihood, exploitability, freshness, role sensitivity, and whether the information is already indexed, cached, archived, or replicated by third parties.
- Prioritize remediation for business-critical systems, privileged roles, finance/procurement workflows, customer data, authentication data, material operations, and regulated information.
- Record risk decision, owner, due date, remediation ticket, verification evidence, residual risk, and board/auditor-ready summary language where applicable.

Evidence core:

- Severity rating with abuse path and weakened control assumption per exposure
- Risk decision record with owner, due date, and remediation ticket or residual risk

Applicability: from micro scale.

FA1.SC1.C5: Asset Decommissioning and Digital Remnants

Retire public-facing assets and external records through a controlled lifecycle so stale properties do not become unmanaged reconnaissance sources.

Implementation guidance:

- Define decommissioning requirements for public domains, subdomains, microsites, landing pages, cloud-hosted pages, social profiles, app listings, support portals, and third-party integrations.
- Before retirement, inventory public references to the asset and decide which should be redirected, removed, archived internally, or preserved for legal/business reasons.
- Verify removal or secure transfer of DNS records, certificates, cloud resources, storage locations, analytics tags, support links, API documentation, and vendor integrations associated with the asset.
- Check for dormant accounts, abandoned brand profiles, stale help-center pages, and forgotten campaign sites that continue to expose contacts, technologies, or customer information.
- Trigger the same DNS and reference cleanup when assets disappear outside planned retirement, such as expired vendor contracts, lapsed SaaS subscriptions, deleted cloud resources, or abandoned campaigns, and reconcile with FA3.SC1.C5 discovery so out-of-band deprovisioning cannot leave dangling records.
- Document redirect handling, ownership transfer, takedown requests, final verification screenshots/exports, and residual references that remain outside direct control.
- Hand archive/cache/search-index persistence to FA1.SC6 rather than treating it as live asset decommissioning, and record any residual exposure in the risk register.

Evidence core:

- Decommissioning record per retired asset with owner and completion date
- Verification screenshot or export confirming DNS, certificate, and reference cleanup
- Residual-reference record with risk disposition where removal is outside direct control

Applicability: from small scale.

Related controls: FA3.SC1.C5.

FA1.SC2: Data Exposure Minimization

Objective. Reduce sensitive organizational data that is currently exposed through public or externally shared content. This subcategory governs removing, redacting, access-restricting, or risk-accepting live data exposures after the footprint assessment identifies them, while routing asset retirement, archive/cache persistence, workforce PII suppression, media metadata, code leakage, and technical cloud exposure to their primary control homes.

FA1.SC2.C1: Current Public Data Remediation and Minimization

Remove, redact, access-restrict, minimize, or formally risk-accept sensitive organizational data in currently controlled public content, applying the least-exposing treatment that still serves the business purpose, and preserve evidence that each exposure was closed,

minimized, or transferred to the right control owner.

Implementation guidance:

- Triage footprint assessment findings into live public content, third-party disclosures, retired assets, archived or cached content, workforce PII, media metadata, code repositories, cloud storage, or externally reachable technical systems before assigning remediation ownership.
- Identify the specific data elements exposed in live public content, externally shared files, portals, dashboards, listings, or support materials, such as direct contact paths, internal role names, process steps, customer or vendor identifiers, project names, schedules, location details, financial/procurement context, and operational metrics.
- Include calendar and scheduling surfaces in minimization review: tenant default free/busy visibility, public booking or scheduling links, shared calendars, and embedded availability widgets expose schedules, attendee names, and meeting context across the organization; route executive-specific calendar exposure to FA4.SC5.C6.
- Remove, redact, or access-restrict sensitive documents, contact lists, internal procedures, procurement details, support workflows, customer or partner details, architecture diagrams, project names, and operational data exposed through official websites, portals, shared documents, help centers, public workspaces, or externally distributed files.
- For content that must remain public or externally shared for legal, customer, investor, or operational reasons, choose the least-exposing treatment that still satisfies the purpose: redaction, aggregation, summarization, generalization, role aliases or team queues, generic location descriptions, partial identifiers, sanitized or synthetic examples, delayed release, or authenticated access.
- For required public disclosures, externally shared reports, customer-facing documents, support content, or investor materials, record which details are mandatory, which details were minimized, and which details remain as accepted residual risk.
- Verify the active source and the released version after treatment, including page source, downloadable attachments and alternate formats, generated PDFs and previews, embedded objects, structured data, public folder indexes, sitemaps, copied excerpts, tables and charts, and alternate URL variants, so removed or minimized data is not still exposed through another representation.
- Record source URL, data element, evidence before remediation, owner, business reason for removal, minimization, or retention, the approved replacement detail, remediation ticket, implementation date, validation evidence, exception rationale, compensating controls, residual exposure, and auditor-ready closure language.
- Transfer residual archive, cache, and search-index persistence to FA1.SC6; image, document, and file metadata sanitization to FA1.SC5; workforce, customer, prospect, or partner personal identifiers and data broker suppression to FA1.SC4; recruiting and job-posting intelligence leakage to FA1.SC3.C5; current publication workflow to FA1.SC3; retired asset cleanup to FA1.SC1.C5; executive household, family, and private-life protection to FA4; and code, cloud, server, API, domain, or repository hardening to FA3.

Evidence core:

- Remediation record per exposure with source URL, owner, and implementation date
- Post-treatment validation evidence showing removal, minimization, or restriction took effect
- Exception or residual-risk record where data must remain public

Applicability: from micro scale.

Related controls: FA1.SC1.C5 · FA1.SC3.C5 · FA4.SC5.C6.

FA1.SC2.C3: External Data Release Rules

Define reviewable rules for what organizational data elements may be published or externally shared, and preserve evidence that releases follow approved minimization criteria.

Implementation guidance:

- Define data-release criteria for common exposure categories such as internal procedures, customer or vendor references, architecture details, support workflows, procurement information, metrics, locations, business timelines, screenshots, documents, and externally shared datasets.
- Require each release decision to identify the business purpose, intended audience, approved detail level, source owner, review owner, retention or review date, and exception path for information that remains sensitive but must be shared.
- Embed the criteria in publication checklists, external-sharing templates, data-room processes, customer-documentation release steps, and public-content review forms so minimization decisions are repeatable and auditable.
- Use data classification and handling policy as an input, but keep broad enterprise policy governance, training program ownership, and compliance evidence in FA5.
- Route channel-specific publication approval and communications workflow to FA1.SC3, third-party publication and partner-disclosure management to FA1.SC1.C3, personal-account or private-life guidance to FA4, and code, secrets, repository, or technical release controls to FA3.
- Retain release-rule evidence such as checklist results, reviewer approvals, exception rationales, data fields removed or retained, validation samples, and residual-risk acceptance.

Evidence core:

- Release criteria embedded in publication checklist or external-sharing template
- Completed checklist or reviewer approval per release with fields removed or retained
- Exception record with rationale and residual-risk acceptance

Applicability: from small scale.

Related controls: FA1.SC1.C3.

FA1.SC2.C5: Exposure Minimization Review Triggers

Review and update data minimization rules when assessments, incidents, platform behavior, or collection capability changes show that previously acceptable public data now creates material exposure risk.

Implementation guidance:

- Trigger a minimization review after footprint assessments, exposure incidents, abuse attempts, public-content changes, platform indexing changes, archive/search persistence, scraping at scale, data aggregation, or new collection methods materially change the risk of existing public data.
- Evaluate whether exposed data elements that were once acceptable now weaken identity verification, access control, fraud detection, vendor management, incident response, physical security, privacy, or executive-support assumptions.
- Update SC2 release rules, minimization checklists, redaction patterns, exception criteria, and routing guidance when the review changes the approved treatment for a data category.
- Transfer recurring threat monitoring, OSINT program management, and control-testing cadence to FA5; transfer footprint assessment methodology changes to FA1.SC1.C2; and transfer technical remediation, code leakage, API hardening, or platform configuration changes to FA3.
- Record the trigger, source evidence, changed assumption, affected data category, decision owner, updated control artifact, remediation or exception ticket, validation result, and residual-risk summary.

Evidence core:

- Trigger record naming source event, changed assumption, and affected data category
- Updated rule or checklist version with decision owner, date, and validation result

Applicability: from small scale.

Related controls: FA1.SC1.C2.

FA1.SC3: Public Presence and Content Management

Objective. Govern official public content so websites, social channels, recruiting materials, press releases, case studies, conference materials, and customer-facing publications serve business needs without exposing roles, workflows, technologies, business tempo, customer/vendor relationships, locations, or support processes that materially improve adversary reconnaissance.

FA1.SC3.C1: Corporate Website Content Governance

Review and control official website content, embedded materials, and discoverability settings so the site does not publish unnecessary reconnaissance value.

Implementation guidance:

- Review public pages, landing pages, help centers, documentation, forms, downloads, HTML comments, structured data, sitemaps, social previews, and embedded objects for sensitive organizational details before publication.
- Remove or redact unnecessary references to internal processes, support workflows, identity-verification steps, unpublished products, customer/vendor details, internal project names, non-public locations, directory structures, debug output, stack traces, or administrative paths.
- Use indexing controls such as noindex tags, response headers, cache-control headers, robots directives, and removal tools only as part of a broader exposure treatment. Access-restrict or remove sensitive content when confidentiality matters, and route cache/archive persistence to FA1.SC6.
- Review third-party scripts, analytics, pixels, forms, and embedded services for leakage of sensitive URL parameters, form data, user identifiers, internal campaign names, or partner/customer context.
- Route webserver banners, CMS patching, WAF/CDN hardening, API behavior, and technical exploitability to FA3, while FA1 records what information the website reveals to an external observer.
- Maintain publication evidence such as reviewer, approval date, content owner, change record, exposure checklist, exception rationale, and post-publication verification.

Evidence core:

- Pre-publication review record with reviewer, approval date, and content owner
- Change record per sensitive finding removed, redacted, or access-restricted
- Post-publication verification result or exception record with rationale

Applicability: from small scale.

FA1.SC3.C2: Controlled Sharing on Social Media

Apply approval, timing, and review controls to official social channels and business-used public profiles so posts do not leak operational intelligence.

Implementation guidance:

- Define which topics, timing details, images, videos, locations, customer references, employee names, and operational updates may be shared through official channels.
- Delay or avoid posts that reveal executive travel, facility attendance, incident response activity, product launch timing, layoffs, acquisitions, vendor transitions, or other high-risk business events before the exposure is necessary.

- Disable routine geotagging for official posts and review location references that could reveal employee routines, executive movement, restricted facilities, or sensitive customer sites.
- Review social images, videos, livestreams, and short-form clips for badges, screens, whiteboards, shipping labels, calendars, documents, visitor logs, facility layouts, or unreleased product details before publication.
- Monitor replies, tags, impostor interactions, and fake support links that use the organization's social presence to redirect customers, vendors, applicants, or employees into phishing or fraud workflows.
- Where executives or spokespeople use personal accounts for business communications, record the organizational exposure in FA1 and route personal-account hardening and executive-specific protections to FA4.

Evidence core:

- Review record per sensitive post with approval, delay, or decline outcome
- Geotag-disabled configuration evidence for official accounts

Applicability: from micro scale.

FA1.SC3.C3: PR and Communications Management

Govern press releases, analyst statements, case studies, conference materials, media appearances, and other external communications for reconnaissance value before release.

Implementation guidance:

- Review press releases, executive quotes, customer stories, partner announcements, analyst briefings, podcasts, webinars, conference talks, and published slide decks for unnecessary exposure of internal processes, customers, vendors, technologies, roadmap, staffing, or operating constraints.
- Use a risk-tiered review workflow: low-risk communications may require communications-owner approval, while high-sensitivity releases should include security, legal, privacy, and business-owner review.
- Apply heightened approval controls during product launches, acquisitions, layoffs, incidents, financing events, executive transitions, regulatory events, and major vendor or technology changes.
- Provide approved talking points and disclosure limits for employees who speak externally, brief media, join webinars, attend conferences, or participate in public customer/prospect calls.
- Review remote-work and recorded-video environments for visible whiteboards, calendars, badges, documents, device screens, unreleased products, customer names, or sensitive facility details before external use.

- Monitor public review sites, media coverage, forums, and community spaces for unauthorized disclosure, then document triage, takedown attempts, internal policy changes, residual risk, and any decision not to escalate.

Evidence core:

- Pre-release review record per high-sensitivity communication with reviewer and date
- Approved talking points or disclosure limits issued for external speakers
- Triage or takedown record for unauthorized disclosures found in coverage

Applicability: from small scale.

FA1.SC3.C4: Technology Exposure via Content

Control public references to technologies, vendors, architecture, security posture, and operational dependencies when those details would materially aid targeting.

Implementation guidance:

- Review public content for technology names, versions, cloud providers, regions, identity providers, security tools, remote access products, ticketing systems, payment platforms, telecom dependencies, and support tooling before publication.
- Use generic capability language unless naming a technology or vendor is intentional, approved, and risk-accepted for business reasons.
- Scrub screenshots, videos, diagrams, architecture slides, office photos, demos, and command-line examples for internal hostnames, environment names, product logos, service URLs, account names, API paths, and role names.
- Review bug bounty pages, vulnerability writeups, security advisories, release notes, open-source documentation, and customer implementation guides so they do not provide reusable attack guidance before fixes are fully deployed.
- Record approved technology disclosures, rationale, reviewer, date, intended audience, residual risk, and related remediation or monitoring actions.

Evidence core:

- Pre-publication review record flagging technology, vendor, and architecture references
- Approved-disclosure record with rationale, reviewer, date, and residual risk

Applicability: from small scale.

FA1.SC3.C5: Recruiting and Job Posting Intelligence Leakage

Govern hiring and recruiting materials so they attract candidates without disclosing internal technology, team structure, security gaps, business tempo, or operational dependencies that materially improve adversary reconnaissance.

Implementation guidance:

- Require security-aware review for job postings, recruiter outreach, career pages, contractor listings, agency briefs, interview packets, take-home exercises, and public hiring announcements for sensitive roles.
- Prefer capability categories over specific product names, versions, internal project names, cloud architecture details, regions, security tooling, or unusual workflow descriptions unless the disclosure is necessary and risk-accepted.
- Avoid revealing staffing gaps, team size, reporting lines, on-call coverage, planned migrations, incident response weaknesses, compliance deadlines, major vendor transitions, privileged access models, or internal delivery timelines.
- Review recruiting content for indirect role exposure, such as named hiring managers, security team members, finance approvers, administrators, executive assistants, help desk personnel, or support escalation contacts.
- Maintain approved language banks for common roles so recruiters and hiring managers can describe responsibilities without exposing specific internal systems or control gaps.
- Capture evidence of review, including posting version, reviewer, date, disclosure exceptions, business rationale, expiration or takedown date, and post-close verification that active postings and recruiter mirrors were updated or removed.
- Route cached, archived, or mirrored copies of closed postings to FA1.SC6 for historical persistence handling.

Evidence core:

- Review record per sensitive-role posting with version, reviewer, and date
- Disclosure exception record with business rationale
- Post-close verification that postings and recruiter mirrors were removed or updated

Applicability: from small scale.

FA1.SC4: Privacy and Personal Data Protection

Objective. Govern public exposure of workforce, customer, and business-linked personal data that can fuel reconnaissance, impersonation, account recovery abuse, harassment, fraud, or other Control Confidence Gaps. This subcategory focuses on organizational exposure reduction, consent-to-publish controls, removal request evidence, recurrence monitoring, and residual-risk decisions. Executive and private-life hardening belongs primarily in FA4, while broad privacy compliance governance belongs in FA5.

FA1.SC4.C1: Data Broker and People-Search Exposure Suppression

Reduce role-linked workforce and customer-contact personal data in broker, people-search, public-record aggregation, and contact-enrichment sources when that data creates organizational reconnaissance or impersonation risk.

Implementation guidance:

- Identify broker, people-search, public-record aggregation, contact-enrichment, and scraped-directory sources that expose home addresses, personal phone numbers, personal email addresses, relatives, aliases, or other personal data linked to workforce members or customer-facing contacts.
- Prioritize exposures by role sensitivity, business process, and abuse path, including identity verification, account recovery, help desk support, finance/procurement approval, executive support, security operations, and customer escalation workflows.
- Submit removal, suppression, correction, or opt-out requests through source-specific processes, privacy rights processes, or managed data broker removal services where appropriate.
- Where budget allows, offer managed data broker removal to the whole workforce as an opt-in benefit alongside the role-prioritized program, in the way many organizations already offer employees a password manager for personal use; participation stays voluntary, and enrollment never requires employees to disclose additional private information to the organization.
- Record source URL, exposed data categories, affected role or business process, abuse path, request date, request owner, provider response, validation date, recurrence monitoring cadence, and closure evidence.
- When suppression is unavailable or the exposure recurs, document residual risk and compensating controls such as stronger help desk verification, phishing-resistant MFA, account recovery changes, call-back procedures, monitoring, or exception approval.
- Provide board/auditor-ready summary language showing whether public PII exposures were reduced, compensated, or formally accepted, drawing on the request, exception, and residual-risk records across this subcategory.
- Route executive household, family, and private-life protection requirements to FA4 while retaining the organizational exposure and remediation evidence in FA1 where it affects business workflows.
- Reference cadence: twice-yearly suppression sweeps; organizations may substitute a documented equivalent cadence.

Evidence core:

- Prioritized exposure list naming affected role and abuse path
- Suppression request log with provider response and validation date
- Residual-risk record with compensating controls where suppression fails or recurs

Applicability: from micro scale.

FA1.SC4.C2: Legal Removal and Delisting Requests

Use applicable privacy, erasure, correction, and search-result removal processes to reduce public personal-data exposures, while preserving evidence of the request, outcome, and residual risk.

Implementation guidance:

- Create an intake path for public personal-data findings that may qualify for deletion, correction, suppression, objection, delisting, or similar privacy-rights requests under applicable laws or platform policies.
- For each request, record the source, exposed data elements, affected person or role, business risk, legal or policy basis, request owner, request date, response deadline, response outcome, and validation evidence.
- Use search-result removal and delisting tools for qualifying personal data where the source cannot be immediately changed, but do not treat delisting as deletion of the underlying exposure.
- Transfer cache, index, archive, and historical persistence handling to FA1.SC6 so removal mechanics and residual-risk decisions are handled consistently.
- Transfer broad privacy-program interpretation, regulatory evidence, retention policy, and data subject rights governance to FA5; FA1 should retain the public-exposure finding, remediation record, and residual-risk summary.

Evidence core:

- Request record per exposure with source, legal basis, owner, and date
- Response outcome and validation evidence per request
- Residual-risk record where removal or delisting was refused or partial

Applicability: from small scale.

FA1.SC4.C3: Public PII Minimization in Organizational Systems

Minimize, anonymize, or role-alias personal identifiers in public-facing organizational systems and content when named or contactable individuals are not required for the business purpose.

Implementation guidance:

- Avoid placing usernames, personal email addresses, employee IDs, customer IDs, personal phone numbers, or other persistent identifiers in public URLs, page source, downloadable files, dashboards, forms, search results, analytics parameters, or shared reports.
- Use role-based contact points, aliases, team queues, aggregate descriptions, or delayed publication where direct named contact is not necessary for the business purpose.
- Review public dashboards, status pages, support portals, help centers, customer communities, marketing pages, testimonials, references, and case studies for unnecessary personal identifiers.
- For testimonials, references, customer stories, employee spotlights, and similar content, capture consent basis, approved display fields, expiration or review date, withdrawal process, business owner, and post-publication verification.

- Document exceptions where named personal data must remain public, including business rationale, affected workflow, residual risk, compensating controls, and approval owner.
- Route technical public-application design and access-control weaknesses to FA3 while FA1 records what personal data is externally visible.

Evidence core:

- Review record of public surfaces with unnecessary personal identifiers flagged
- Replacement evidence showing role aliases or team queues where names were removed
- Exception record with rationale and compensating controls where names remain public

Applicability: from small scale.

FA1.SC4.C4: Role-Based PII Exposure Awareness

Educate workforce members in sensitive or public-facing roles on how role-linked personal data can weaken organizational controls and how to report or reduce such exposures.

Implementation guidance:

- Explain how public personal phone numbers, addresses, relatives, personal emails, birthdays, photos, badges, and social posts can support help desk impersonation, account recovery abuse, vendor fraud, targeted phishing, harassment, or executive-support pretexts.
- Provide role-specific examples for finance, procurement, help desk, IT administration, security operations, HR, legal, executive support, customer support, and other high-risk workflows.
- Train employees to report public role-linked personal-data exposures through the same finding intake used for other footprint issues, including source URL, screenshot, affected workflow, and suspected abuse path.
- Provide approved guidance for reducing business-linked public personal data without requiring employees to disclose additional private information to the organization.
- Route general security awareness to FA2 and executive/private-life privacy hardening to FA4; this control should support SC4 evidence, reporting, and remediation workflow.

Evidence core:

- Briefing delivery record naming covered roles and date
- Role-linked exposure reports received through the finding intake

Applicability: from small scale.

FA1.SC5: Media and Metadata Sanitization

Objective. Sanitize and verify public media, documents, screenshots, recordings, and other externally shared files so hidden metadata and visible background artifacts do not expose people, systems, locations, workflows, customers, or internal context. This subcategory requires repeatable release workflows, tooling evidence, verification records, exception handling, and remediation closure for files that have already been released.

FA1.SC5.C1: Image and Screenshot Sanitization

Remove unnecessary metadata and visible sensitive content from images and screenshots before they are published or shared externally.

Implementation guidance:

- Remove EXIF, GPS, device, software, edit-history, author, thumbnail, and other metadata that is not needed for the public purpose.
- Review screenshots for usernames, emails, URLs, account names, internal hostnames, customer names, document titles, browser tabs, calendars, chat content, support tickets, logs, tokens, and environment labels.
- Review images for badges, screens, whiteboards, shipping labels, visitor logs, facility layouts, unreleased products, customer-site details, and identifiable people where identification is not necessary.
- Use approved sanitization tools or workflows and record the tool, configuration or preset, reviewer, release date, and sample verification evidence.
- Document exceptions where metadata or identifiable content is intentionally retained, including business rationale, owner, audience, and residual risk.
- Route public-content approval decisions to FA1.SC3 and personal/executive protection concerns to FA4 while SC5 owns sanitization evidence.

Evidence core:

- Sanitization record per released image with tool, reviewer, and date
- Sample verification showing metadata stripped from published files
- Exception record where metadata or identifiable content is retained

Applicability: from small scale.

FA1.SC5.C2: Document and PDF Sanitization

Clean documents, spreadsheets, presentations, PDFs, and externally shared files of metadata, hidden content, and internal references before release.

Implementation guidance:

- Remove author names, usernames, revision history, comments, tracked changes, hidden text, hidden rows or sheets, embedded objects, document properties, template names, internal file paths, server paths, printer names, and software/version details where not needed.
- Sanitize PDFs for hidden information, attachments, layers, comments, redaction artifacts, embedded metadata, and prior-version remnants before publication.
- Require document sanitization for customer documentation, press materials, regulatory-adjacent public documents, research papers, white papers, product collateral, templates, and externally shared spreadsheets or slide decks.
- Use approved document-inspection, redaction, export, or sanitization tooling and preserve a release checklist or verification log showing the file version, reviewer, tool, date, and result.
- Where a document must preserve metadata for authenticity, legal, accessibility, or chain-of-custody reasons, record the exception, approved metadata fields, and residual exposure.
- Route historical document exposure and republication limits to FA1.SC6 while SC5 owns current file sanitization.

Evidence core:

- Release verification log per external file with reviewer, tool, date, and result
- Exception record naming retained metadata fields and residual exposure

Applicability: from micro scale.

FA1.SC5.C3: Content-Capture Device Metadata Controls

Configure devices, capture tools, and export workflows so official media and documents do not add avoidable location, device, user, or system metadata.

Implementation guidance:

- Disable geotagging by default on organization-managed cameras, phones, tablets, drones, scanners, screen-recording tools, and other devices used to create externally shared content where location data is not required.
- Configure PDF printers, export presets, design tools, screen capture tools, document generators, and media-production workflows to avoid stamping usernames, device names, machine names, local paths, internal project names, or software details.
- Document managed-device or tool settings, configuration owner, affected content channels, review cadence, and exception process.
- For field, customer-site, event, or remote-work content, define pre-publication checks that verify location and device metadata were removed or intentionally retained.
- Record validation samples showing that generated files do not contain unexpected device, location, user, or system metadata.

Evidence core:

- Capture-device and export-preset configuration record with owner
- Validation sample showing generated files free of device and location metadata

Applicability: from small scale.

FA1.SC5.C4: Physical Artifact Review in Media

Review visual and audio media for physical artifacts that reveal organizational locations, workflows, documents, identities, customers, or operations.

Implementation guidance:

- Before publishing office, facility, event, product, customer-site, field-service, remote-work, or executive-communication media, review backgrounds for whiteboards, documents, badges, visitor logs, calendars, screens, shipping labels, device names, facility layouts, access controls, and customer or vendor details.
- Use staging, sweep, crop, blur, redaction, reshoot, or alternate-media workflows to remove unnecessary physical artifacts before release.
- Review video and audio recordings for visible screens, spoken customer names, internal project names, incident activity, meeting details, access-control behavior, or sensitive site information.
- Record media owner, reviewer, review date, artifacts found, remediation action, residual risk, and release approval.
- Route general social engineering training to FA2 and private-life or household media concerns to FA4; SC5 should remain focused on organizational media and publication evidence.

Evidence core:

- Pre-release media review record with reviewer, date, and artifacts found
- Remediation or release-approval record per flagged artifact with residual risk

Applicability: from small scale.

FA1.SC5.C5: Tooling and Automation

Integrate managed sanitization, redaction, and verification tooling into publication and external-sharing workflows.

Implementation guidance:

- Define approved sanitization tools, redaction tools, upload checks, export presets, or automated workflows for common content channels such as CMS publishing, file sharing, documentation portals, design workflows, press releases, and customer deliverables.
- Assign ownership for tool configuration, supported file formats, update cadence, exception handling, failure handling, and verification sampling.

- Integrate sanitization checks into high-volume release paths where feasible, such as CMS image upload, document export, marketing asset review, customer documentation release, or repository-based documentation publishing.
- Provide simple approved workflows for employees who need to share external files outside automated channels, and require evidence that the workflow was used for sensitive releases.
- Periodically validate tooling against new formats and channels such as mobile screenshots, 3D models, AR/VR assets, design files, recordings, exported dashboards, and generated PDFs.
- Document tool results, false negatives, bypasses, remediation tickets, and exceptions so sanitization can be audited rather than treated as a best-effort habit.

Evidence core:

- Approved tool list per content channel with configuration owner
- Integration evidence showing sanitization checks active in release workflows
- Tool result log with false negatives, bypasses, and remediation tickets

Applicability: from mid scale.

FA1.SC5.C6: Verification of Sanitization

Verify released files and media for residual metadata or visible sensitive artifacts, and track remediation when sanitization fails.

Implementation guidance:

- Periodically sample public websites, documentation portals, app stores, social channels, press kits, customer materials, public repositories, and shared file locations for released files that may still contain metadata or visible artifacts.
- Use attacker-view checks to inspect file metadata, document properties, hidden content, thumbnails, embedded objects, screenshots, image backgrounds, and generated previews.
- For each finding, record source URL, file version, evidence, exposed data, affected workflow, severity, owner, remediation ticket, replacement or takedown action, verification result, and closure date.
- If the exposure cannot be removed or replaced, document residual risk, compensating controls, and formal acceptance.
- Feed recurring failures back into SC5 tooling, release checklists, training, and publication review workflows.
- Reference cadence: twice-yearly verification sampling; organizations may substitute a documented equivalent cadence.

Evidence core:

- Dated sample record naming released files checked and residual metadata findings

- Remediation ticket per finding with replacement, takedown, or risk-acceptance outcome

Applicability: from small scale.

FA1.SC6: Historical Information Management

Objective. Identify and manage organizational information that persists in archives, search indexes, caches, legacy repositories, filings, and third-party historical records. This subcategory treats removal as a request-and-review workflow rather than a guaranteed outcome, and requires validation, recurrence monitoring, compensating controls, and risk acceptance for content that cannot be removed.

FA1.SC6.C1: Internet Archive and Web Snapshot Management

Identify, request treatment for, and track residual risk from sensitive organizational content preserved in web archives and snapshot services.

Implementation guidance:

- Search web archives, snapshot services, and historical mirrors for sensitive historical pages, documents, job postings, support content, technical references, customer information, workforce PII, and retired asset references.
- For each archived exposure, record original URL, archive URL, capture date or period, exposed data, business owner, abuse path, current source status, and evidence artifact.
- Submit removal, exclusion, correction, or access-limitation requests where the archive service provides an appropriate request path, but treat the outcome as request-and-review rather than guaranteed deletion.
- Avoid assuming that robots directives, takedown requests, or source removal will eliminate existing historical copies. Validate the actual archive result and document any remaining captures.
- Monitor for recurrence or newly captured historical content after high-risk events such as site migrations, layoffs, acquisitions, product launches, incidents, or decommissioning.
- If archived content remains public, document residual risk, compensating controls, communication plan, and risk acceptance.
- Record content absorbed into AI training corpora as accept-and-compensate residual risk; removal is structurally impossible, so treatment is compensating controls and monitoring rather than takedown effort.

Evidence core:

- Archived-exposure record with original URL, archive URL, and exposed data
- Removal or exclusion request log with provider response and validation result
- Residual-risk record with compensating controls for captures that remain

Applicability: from small scale.

FA1.SC6.C2: Search Index and Cached Result Handling

Manage search-result, cached-result, and indexing persistence for sensitive content after the active source has been removed, restricted, or corrected.

Implementation guidance:

- First remove, redact, or access-restrict the active source when confidentiality matters; search-result removal alone should not be treated as remediation of the underlying exposure.
- Use appropriate indexing controls such as noindex directives, response headers, cache-control headers, canonicalization, and search removal tools as part of a broader exposure treatment.
- Do not rely on robots.txt as a deletion or confidentiality control. Where noindex is used, ensure crawlers can access the directive so the instruction can be processed.
- Submit urgent removal or refresh requests for qualifying search results, cached copies, snippets, thumbnails, previews, or indexed URLs when sensitive content remains visible after the source is corrected.
- Maintain documentation of source correction, removal request, query terms, affected URLs, request date, search provider response, validation date, and residual results.
- Verify removal across relevant search engines, query variants, snippets, previews, image results, and cached copies; document residual-risk acceptance where persistence remains outside direct control.

Evidence core:

- Source-correction evidence preceding each removal or refresh request
- Removal request log with affected URLs, provider response, and validation date
- Residual-results record with risk acceptance where persistence remains

Applicability: from small scale.

FA1.SC6.C3: Legacy Public Reference Cleanup

Identify and reduce historical public references to retired assets, platforms, campaigns, services, and repositories after live decommissioning is complete.

Implementation guidance:

- Use FA1.SC1.C5 for live public asset decommissioning and FA3 for technical system retirement. SC6 should focus on historical references, archived copies, indexed remnants, and third-party mentions after the live asset is retired.
- Inventory historical references to retired domains, subdomains, microsites, app listings, support portals, documentation sites, landing pages, campaigns, integrations, repositories, and vendor/customer materials.

- Update, remove, redirect, or risk-accept public references that continue to expose contacts, technologies, customer names, support workflows, internal project names, or outdated security assumptions.
- Coordinate with content owners, legal, communications, customer success, and third parties where historical references are controlled outside the retiring technical team.
- Record retired asset, public reference, source owner, requested action, response, validation evidence, remaining historical exposure, and residual-risk decision.
- Retain historical system inventory needed for incident response or legal purposes in internal repositories rather than leaving obsolete public references unmanaged.

Evidence core:

- Historical-reference inventory per retired asset with source owner
- Update, redirect, or takedown request record with response and validation evidence
- Residual-risk decision for references that remain public

Applicability: from mid scale.

Related controls: FA1.SC1.C5.

FA1.SC6.C4: Historical Document and Filing Exposure Review

Review historical publications, filings, records, and legacy document repositories for persistent exposure, republication risk, and limits on removal.

Implementation guidance:

- Inventory historical annual reports, investor materials, public filings, procurement records, case studies, white papers, technical papers, archived documentation, legacy slide decks, and public document repositories that contain sensitive organizational context.
- Assess whether historical documents expose customers, vendors, facility details, technologies, project names, security posture, workforce PII, financial/procurement context, or operational constraints that remain useful for reconnaissance.
- When documents are republished, migrated, or reissued, apply current redaction, minimization, metadata sanitization, and approval requirements before release.
- Document legal, regulatory, contractual, or records-retention constraints that prevent removal or redaction of public filings, regulator records, media coverage, procurement records, or other third-party records.
- For non-removable historical exposure, record compensating controls, affected assumptions, board/auditor summary language, and formal risk acceptance.
- Coordinate with FA1.SC3 for current publication workflow and FA5 for broad compliance, legal-retention, and regulatory evidence governance.

Evidence core:

- Reviewed historical-filing inventory naming exposed data per document

- Current-standards sanitization evidence for republished or migrated documents
- Risk-acceptance record with compensating controls for non-removable exposure

Applicability: from mid scale.

FA1.SC7: Mobile Application OSINT Exposure

Objective. Govern externally observable mobile application artifacts that reveal organizational context, privacy posture, support paths, exposed endpoints, developer identities, customer workflows, or technical clues. FA1 owns app-store listings, screenshots, privacy/developer metadata, public binaries as reconnaissance sources, and evidence handoff; FA3 owns mobile API security, application hardening, authentication, authorization, secure storage, and technical remediation.

FA1.SC7.C1: Mobile App Store and Developer Metadata Management

Control information revealed through app store listings, privacy declarations, screenshots, release notes, developer identities, support contacts, and related mobile marketplace metadata.

Implementation guidance:

- Inventory official mobile apps, app store listings, developer accounts, package names, publisher names, support contacts, privacy URLs, release notes, screenshots, videos, and marketplace metadata.
- Review descriptions, release notes, support links, screenshots, previews, and localization strings for sensitive organizational details, customer workflows, unreleased features, internal terminology, support processes, environment names, or screenshots of real data.
- Review privacy labels, data-safety declarations, permission descriptions, and developer disclosures for consistency with intended public messaging and unnecessary exposure of business processes or data flows.
- Use generic support channels and role-based contacts where individual names, personal emails, or direct phone numbers are not required.
- Record listing owner, reviewer, release version, approved disclosure rationale, screenshot sanitization evidence, privacy/developer metadata review, exception rationale, and post-release verification.
- Reassess listings, screenshots, release notes, privacy labels, and developer metadata from an external observer perspective after release updates, listing changes, or privacy-label updates, comparing findings against the approved public inventory and release records to catch unauthorized disclosures, stale metadata, or excessive permissions language.

Evidence core:

- Listing review record per release with owner, version, and date
- Screenshot and metadata sanitization evidence per listing update

- Post-release external-observer verification result with findings dispositioned

Applicability: from small scale; condition: public mobile apps.

FA1.SC7.C2: Mobile App Technical Disclosure Assessment and Handoff

Assess externally observable technical disclosures from mobile apps, including API clues and build or binary artifacts, record them as footprint findings, and route technical remediation to FA3.

Implementation guidance:

- Review app listings, public documentation, app configuration, visible URLs, error messages, support articles, demo screenshots, public traffic observations, and publicly distributed binaries, manifests, configuration files, strings, embedded resources, package metadata, debug flags, test endpoints, analytics keys, and environment names for API hostnames, paths, environment labels, internal service names, version details, account identifiers, or debugging output that improves reconnaissance.
- Identify hardcoded credentials, tokens, API keys, secrets, internal endpoints, customer identifiers, debug symbols, verbose logging, test data, or non-production references as exposure findings and transfer technical remediation to FA3.
- Use mobile analysis tools and manual review where legally and operationally appropriate, recording whether each finding is a public-content issue, a privacy or developer metadata issue (FA1.SC7.C1 or FA1.SC4), a binary artifact or API clue owned here, or an FA3 technical vulnerability.
- Record each finding with app version, distribution channel, source URL or artifact hash, screenshot or extracted evidence, exposed data category, affected business process, abuse path, owner, remediation ticket or handoff, replacement release, and validation result.
- Remove unnecessary API and technical details from public documentation, screenshots, release notes, support content, and client-visible messages where they are not needed for customers or developers.
- Do not make FA1 the primary home for code obfuscation, certificate pinning, secure storage, cryptographic design, or application hardening; those controls belong in FA3, while FA1 records what the public artifact reveals.
- Retest after replacement builds, content updates, listing changes, or FA3 technical remediation; validate that the externally observable exposure was reduced, document residual risk where legacy versions remain available, and retain closure evidence.

Evidence core:

- Assessment record per app version naming artifacts and sources examined
- Finding record with exposed data, owner, and remediation ticket or FA3 handoff
- Post-remediation retest result with residual risk for legacy versions

Applicability: from small scale; condition: public mobile apps.

Related controls: FA1.SC7.C1.

Social Engineering Defense

Social Engineering Defense encompasses policies, training, and technical controls aimed at preventing, detecting, and responding to attacks that trick people (users or employees) by exploiting information and trust. OSINT is often the first step for social engineering, and attackers gather personal and organizational details to make their deception more convincing. This focus area strengthens the human element of security so that even when attackers know details about the organization, they cannot easily manipulate people or processes. This focus area broadly orients to NIST CSF 2.0 policy, roles, awareness and training, identity verification, monitoring, and response communication categories. It also aligns with Zero Trust, which in a human sense means "never trust, always verify" requests even if they come with familiar details.

Business rationale. Social engineering such as phishing, pretext phone calls, and baiting with removable media targets the most unpredictable factor in any defense: human behavior. Attackers rely heavily on OSINT to improve their success rates in these attacks. For instance, knowing an organization's internal project names or the org chart, helps craft a believable phishing email ("Hi Alice, as per Project Zeus meeting with Bob..."). Defending against social engineering is critical to protect financial assets (fraudulent wire transfers), credentials (phished passwords), and system access. A single successful social engineering attack can bypass layers of technical security. Businesses must create a culture of skepticism and verification, especially for SMBs, where every employee often has broad access. A single mistake can be devastating, and for enterprises, social engineering is often how attackers bypass complex defenses (e.g., spear phishing an admin). This focus area strengthens employee and process resilience against such manipulation, reducing the impact of OSINT available to attackers.

Scope. This category covers security awareness training, social engineering testing, communication and transaction verification protocols, phishing/impersonation technical safeguards, and incident response for social engineering events. It addresses digital vectors (phishing emails, vishing calls, social media impersonation) and physical pretexts (tailgating, in-person impersonation). It overlaps with FA1: Digital Footprint Reduction, because less exposed data means fewer opportunities for social engineers, and with FA5: Continuous Monitoring and Response, which detects fake profiles and phishing campaigns early.

NIST CSF 2.0 orientation: GV.RR · GV.PO · PR.AT · PR.AA · DE.CM · DE.AE · RS.MA · RS.CO

Focus-area alignment entries are broad orientation metadata indicating thematic overlap with NIST CSF 2.0 categories. They are not conformance mappings, control-level crosswalks, or claims of coverage. Control-level mappings to external standards are published separately as ODSF mapping packs.

FA2.SC1: Security Awareness and Training

Objective. Educate and empower all members of the organization to recognize and resist social engineering attempts, with special emphasis on how attackers use OSINT to make those attempts credible.

FA2.SC1.C1: OSINT Awareness in Training Programs

Maintain security awareness training modules that demonstrate how publicly available information about the organization and its people is used to construct credible attacks.

Implementation guidance:

- Demonstrate how an attacker can combine professional-network profiles, social posts, public records, and organizational announcements into a phishing or pretexting approach that references real colleagues, projects, or events.
- Include recent real-world incidents where public information enabled social engineering, and identify which exposed details made each attack credible.
- Where approved, personalize training with sanitized findings from the organization's own OSINT assessments (FA1.SC1.C2); present findings as education and empowerment, never as blame.
- Require OSINT-awareness content for all personnel, including executives and the board; cover executive-specific abuse paths such as impersonation and synthetic media built from public video, audio, and press appearances, and route household or personal-account content to FA4.
- Record module owner, audience, scenario source, completion evidence, refresher cadence, and update triggers such as incidents, new exposure findings, or major business events.

Evidence core:

- Training module record with owner, audience, and scenario source
- Dated completion evidence covering all personnel including executives
- Module update record tied to incidents or new exposure findings

Applicability: from micro scale.

Related controls: FA1.SC1.C2.

FA2.SC1.C2: Recurring Training Delivery and Reinforcement

Deliver social engineering training on a recurring cadence with reinforcement between formal sessions, so awareness keeps pace with evolving tactics.

Implementation guidance:

- Run comprehensive training for all personnel at least annually, with a comprehension check and recorded completion evidence.

- Reinforce between formal sessions through short-form content such as briefings, newsletters, micro-modules, or posters that reflect current lures, active campaigns, and the business context attackers are likely to reference.
- Use interactive formats such as phishing simulations, role play, and tabletop exercises (FA2.SC1.C3) to convert awareness into practiced verification behavior.
- Recognize and reinforce reporting behavior; reward verification and fast reporting rather than penalizing failed recognition.
- Record delivery cadence, audience coverage, completion rates, comprehension results, content-refresh triggers, and the owner responsible for keeping scenarios current.
- Trigger training at start of employment, when public new-hire announcements make personnel most targetable, in addition to the recurring cadence.

Evidence core:

- Completion records with comprehension-check results for each annual cycle
- Dated reinforcement artifacts issued between formal sessions
- New-hire training completion evidence at start of employment

Applicability: from micro scale.

Related controls: FA2.SC1.C3.

FA2.SC1.C3: Social Engineering Drills

Conduct authorized social engineering simulations that measure training effectiveness and verification behavior across communication channels.

Implementation guidance:

- Run phishing simulations on a defined cadence with documented authorization, scope, lure rationale, and success criteria; track click, report, and credential-entry rates by population rather than by individual blame.
- Extend simulations beyond email where authorized, including vishing, SMS, chat, and QR-code lures, with legal, HR, and communications review recorded before execution.
- Design targeted exercises for high-risk roles such as finance, help desk, executive assistants, and administrators that mirror realistic public-source pretexts, with management approval recorded.
- Provide immediate, non-punitive feedback and learning material after each exercise; coach missed cues privately and feed systemic gaps into training content and verification rules.
- Record exercise owner, scope, population, results, improvement actions, retest date, and evidence artifacts for program reporting through FA5.

Evidence core:

- Authorization record per exercise with scope and lure rationale

- Population-level click, report, and credential-entry results with date
- Improvement actions with owner and retest date

Applicability: from small scale.

FA2.SC1.C4: Verification Culture and Non-Punitive Reporting

Maintain organizational norms, leadership messaging, and policy commitments that make verification expected behavior and make reporting safe.

Implementation guidance:

- Publish a leadership-endorsed, non-punitive commitment stating that personnel will never be penalized for verifying a request, declining to act pending verification, or reporting a suspected or successful social engineering attempt.
- Require leaders and managers to model verification behavior, including accepting callback verification of their own requests without friction; treat pressure to bypass verification as a reportable event.
- Provide simple, well-known verification channels such as a verified internal directory, a security hotline, or an approved workflow for confirming unusual requests (FA2.SC2.C1).
- Reinforce the norm through internal communications that recognize verified saves and reported attempts, using sanitized examples rather than identifying individuals.
- Measure culture signals such as report rates, verification-before-action rates in drills, bypass-pressure reports, and time-to-report trends; record owner, review cadence, and corrective actions through FA5 metrics.

Evidence core:

- Published non-punitive commitment with leadership endorsement and date
- Report-rate and bypass-pressure measures with owner and review date
- Sanitized recognition communications for verified saves or reported attempts

Applicability: from micro scale.

Related controls: FA2.SC2.C1.

FA2.SC1.C5: Risk-Tiered Training for High-Risk Roles

Define role-specific social engineering training requirements for personnel whose authority, access, public visibility, or support responsibilities create higher exposure risk.

Implementation guidance:

- Maintain a high-risk role roster covering finance approvers, HR, legal, procurement, help desk, administrators, incident responders, executive assistants, executives, board-facing staff, public spokespeople, vendor managers, and other personnel whose decisions can be abused through public-source pretexting.

- Define role modules by attack path rather than by job-title anecdotes, such as payment or payroll diversion, account recovery abuse, privileged-access requests, vendor impersonation, legal or regulatory document lures, executive override pressure, deepfake or vishing attempts, and requests based on public business context.
- For each role module, record owner, target population, learning objective, scenario source, required verification behavior, completion evidence, exception path, refresher cadence, and trigger events such as incidents, new public exposure findings, role changes, or major business events.
- Use sanitized ODSF findings to show how exposed authority, contact data, team structure, or public context weakens confidence in verification and approval controls, then connect the lesson to the relevant FA2 verification or incident-response procedure.
- Route technical dual-authorization, privileged-access configuration, IAM, and system-change controls to FA3 or the primary technical-control owner; FA2 retains the training evidence that personnel can recognize and follow the human verification process.
- Route executive private-life, household, personal-account, and family-adjacent protection modules to FA4 while FA2 records any role-based training requirement that supports organizational authority, fraud prevention, account recovery, or incident-response readiness.
- Include hiring-lifecycle attack paths in role modules: fake-recruiter approaches to employees on personal channels, synthetic or impersonated candidates in remote interviews, and lures timed to public new-hire announcements.

Evidence core:

- High-risk role roster with populations and covered attack paths
- Per-module completion evidence with owner and date
- Refresher or trigger-event training record after role or exposure changes

Applicability: from small scale.

FA2.SC1.C6: Physical Pretext Awareness and Reporting

Train personnel to recognize physical-world pretexts that use public information to create trust, urgency, or access pressure.

Implementation guidance:

- Cover suspicious gifts, post-event packages, visitor pretexts, courier requests, conference follow-ups, and office or remote-work deliveries that reference public events, public roles, published schedules, vendor relationships, or employee social media.
- Teach employees to pause, preserve evidence, and report unexpected devices, packages, badges, printed materials, QR codes, payment cards, storage media, or tracking concerns through an approved channel before using, connecting, discarding, or forwarding the item.
- Record training audience, scenario source, reporting channel, escalation owner, evidence to preserve, and expected response time for physical social-engineering reports.

- Route hardware inspection, device forensics, endpoint isolation, tracking-device handling, and facility-security procedures to FA3, physical security, or the designated technical owner while FA2 retains awareness and reporting behavior.
- Route executive event, travel, household, family, or personal-safety procedures to FA4 or an executive-protection extension; FA2 retains the training path for organization-relevant pretexts that could lead to fraud, access, coercion, or incident-response pressure.
- Feed confirmed physical pretext incidents into FA2.SC5 response records, FA1 publication or event-disclosure review, and FA5 monitoring or metrics where the pretext exploited public exposure.

Evidence core:

- Training completion record with audience and scenario source
- Named reporting channel and escalation owner for physical-pretext reports
- Preserved-evidence report record with disposition where pretexts occur

Applicability: from small scale.

FA2.SC2: Communication and Transaction Verification

Objective. Implement formal processes to verify the legitimacy of sensitive requests or communications, thereby thwarting social engineering attempts that rely on impersonation or fraudulent instructions.

FA2.SC2.C1: Out-of-Band Verification for Sensitive Requests

Define sensitive request classes and require independent verification through approved channels before action.

Implementation guidance:

- Define sensitive request classes such as payment or bank-detail changes, payroll or benefits changes, gift-card or purchase-card requests, bulk data release, privileged password or MFA reset, vendor onboarding, legal or regulatory document requests, emergency executive instructions, and unusual support escalations.
- Require verification through a pre-approved channel that is independent of the initiating request, such as an internal workflow, verified callback directory, approved collaboration channel, ticketing system, or other channel with authentication and audit evidence.
- Prohibit reliance on contact details, links, attachments, phone numbers, or account identifiers supplied inside the suspicious request; employees should use approved directories, workflow records, or previously validated contacts.
- Record request type, requester, claimed authority, verifier, verification channel, timestamp, result, exception or override, action taken, and residual-risk decision for requests above the defined threshold.

- Train personnel that urgency, secrecy, public business context, and familiar personal details are risk signals that trigger verification rather than reasons to bypass it.
- Review failed or bypassed verification attempts after incidents, drills, deepfake scenarios, or monitoring alerts, and update request classes, channel rules, training, and escalation paths.

Evidence core:

- Defined sensitive-request classes with required verification channels
- Verification record per request with verifier, channel, timestamp, and result
- Exception or override record with rationale and residual-risk decision

Applicability: from micro scale.

FA2.SC2.C2: Multi-person Approval

Require dual control for critical transactions, sensitive data release, and high-risk administrative actions that could be driven by social engineering.

Implementation guidance:

- Set approval thresholds for payments, bank-detail changes, payroll changes, bulk HR or customer data release, privileged-account recovery, DNS or domain changes, vendor onboarding, and other actions where public-source pretexts could create business harm.
- Use separate approvers, duties, or systems where feasible so one compromised conversation, mailbox, meeting, or voice channel cannot authorize the full action.
- Record request source, approving parties, verification evidence, system or workflow log, override rationale, and exception approval for every action that crosses a defined threshold.
- Route technical enforcement for privileged changes, workflow configuration, segregation of duties, and access control to FA3 or the primary business system owner while FA2 owns the social-engineering approval rule and evidence expectation.
- Retest approval procedures through drills or incident reviews and update thresholds when public exposure, role changes, payment patterns, or attack scenarios change.

Evidence core:

- Defined approval thresholds for payments, data release, and privileged actions
- Dual-approval record with both approvers and workflow log per threshold action
- Override or exception record with rationale and approval

Applicability: from micro scale.

FA2.SC2.C3: Authenticated Business Channel Rules

Require sensitive business requests to use approved channels with authentication, audit trails, and known recovery paths.

Implementation guidance:

- Maintain an inventory of approved channels for payment requests, vendor changes, HR changes, support escalations, legal requests, incident communications, partner file exchange, and executive instructions.
- Define which request types may be handled by email, ticketing, finance systems, HR systems, partner portals, collaboration tools, phone callback, or emergency channels, and define when an additional out-of-band verification record is required.
- Require channel evidence such as authenticated user, workflow ID, approver, audit log, file exchange record, callback record, exception owner, and closure decision.
- Route DMARC, DKIM, and SPF posture to FA3.SC2.C6; route secure portal configuration, collaboration-platform hardening, retention settings, and access-control implementation to FA2.SC3, FA3, or the relevant platform owner.
- Prohibit personal accounts or unsanctioned consumer channels for sensitive business workflows unless an approved incident or continuity exception records owner, duration, risk, compensating controls, and retirement date.
- Review channel rules after impersonation incidents, ransomware or outage scenarios, vendor fraud attempts, platform changes, and public-exposure findings that reveal approval paths or contact dependencies.

Evidence core:

- Approved-channel inventory mapping sensitive request types to channels
- Per-request channel evidence (authenticated user, workflow ID, or audit log)
- Exception record for personal-account use with owner and retirement date

Applicability: from small scale.

Related controls: FA3.SC2.C6.

FA2.SC2.C4: Verification Failure Escalation

Escalate failed, bypassed, or suspicious verification outcomes from sensitive-request workflows into the social engineering incident response path with the verification record attached.

Implementation guidance:

- Define escalation triggers within verification workflows, such as failed callback verification, mismatched requester details, refusal to use approved channels, urgency or secrecy pressure to bypass controls, and exception overrides granted under pressure.
- Require the verification record (request class, channel, claimed identity, verifier, result, and override rationale per FA2.SC2.C1) to accompany the escalation so responders inherit evidence rather than reconstructing it.

- Route report intake channels, capture fields, triage ownership, and acknowledgement expectations to FA2.SC5.C1, which owns the canonical social engineering reporting path; route recurring brand, domain, and fake-profile monitoring to FA5 and FA1/FA4 as applicable.
- Track workflows, roles, and request classes that generate repeated verification failures, and feed confirmed pretext patterns back into request-class definitions, approval thresholds, channel rules, and targeted warnings.

Evidence core:

- Defined escalation triggers for failed or bypassed verification
- Escalation record with the originating verification record attached
- Repeat-failure pattern record with resulting rule or threshold updates

Applicability: from small scale.

Related controls: FA2.SC2.C1 · FA2.SC5.C1.

FA2.SC3: Technical Anti-Phishing and Social Engineering Controls

Objective. Define the social-engineering outcomes, evidence, and handoffs for technical protections that reduce phishing, impersonation, credential theft, and malicious-link abuse while routing durable technical implementation to FA3 or the primary platform owner.

FA2.SC3.C1: Email Security Gateway and Phishing Filters

Operate email protections that reduce phishing delivery and preserve evidence for social-engineering response.

Implementation guidance:

- Define expected controls such as inbound phishing detection, malicious-link handling, attachment detonation or blocking, impersonation warnings, external-sender labeling, quarantine review, reporting integration, and user-facing warning validation.
- Preserve configuration owner, domain-authentication policy status (FA3.SC2.C6), filter rule changes, quarantine decisions, reported-message samples, false-positive handling, tuning records, and incident linkage for audit and board-ready evidence.
- Review whether warnings and banners help employees distinguish public-source impersonation from legitimate requests, and update training when alerts fail, confuse users, or are bypassed.
- Route domain and email authentication posture to FA3.SC2.C6, and mail-platform configuration, DNS changes, and infrastructure hardening to FA3 or the messaging-platform owner, while FA2 records the social-engineering detection and response evidence.
- Retest email controls after phishing incidents, executive impersonation campaigns, major platform changes, domain changes, or confirmed bypasses.

- The mail-platform owner's configuration and detection records satisfy this control's evidence expectation by reference.

Evidence core:

- Email-protection configuration record with owner and date, platform records by reference
- Quarantine decisions and reported-message samples with dates
- Retest or tuning record after incidents or confirmed bypasses

Applicability: from micro scale.

Related controls: FA3.SC2.C6.

FA2.SC3.C2: Phishing Web Protection Handoff

Connect browser, DNS, and malicious-site protections to social-engineering training, reporting, and incident response evidence.

Implementation guidance:

- Define how malicious-link blocks, lookalike-domain warnings, browser warnings, DNS filtering, cloud-email link protection, and web-proxy alerts are reported into the social-engineering response path.
- Treat OAuth and app-consent grant phishing as a reportable lure class: include unexpected third-party application consent prompts, permission escalations, and device-code prompts in detection and reporting paths, and route consent-grant inventory and revocation to FA3 or the identity owner.
- Record alert source, affected user or role, lure context, requested action, destination domain or URL, control action, user response, and escalation decision for high-risk phishing-web events.
- Use blocked or bypassed web lures to update employee warnings, verification scripts, phishing simulations, and incident-response playbooks.
- Route browser patching, endpoint security, DNS filtering, proxy configuration, browser-extension governance, and web-control deployment to FA3 or endpoint/platform owners.
- Retain evidence that technical web protections are tested against social-engineering scenarios, especially credential-harvesting pages, fake portals, QR-code lures (quishing), and executive or vendor impersonation paths.

Evidence core:

- Phishing-web event records with alert source, affected user, and control action
- Warning, simulation, or playbook update fed by blocked or bypassed lures
- Dated test evidence of web protections against credential-harvesting scenarios

Applicability: from small scale.

FA2.SC3.C3: Multi-Factor Authentication Everywhere

Require MFA coverage across organization-managed accounts with documented exceptions, prefer phishing-resistant methods for high-risk roles, and maintain the recovery-process evidence that limits credential theft from phishing and pretexting.

Implementation guidance:

- Require MFA on all organization-managed accounts; maintain an exception inventory recording owner, rationale, compensating control, and retirement date, and treat unmanaged or legacy authentication paths as findings.
- Prefer phishing-resistant authentication for executives, administrators, finance, HR, help desk, incident responders, and other high-risk roles, naming passkeys (FIDO2/WebAuthn) as the preferred class; align assurance decisions to NIST SP 800-63B-4, which requires a phishing-resistant option at AAL2, permits syncable passkeys at AAL2, and requires device-bound authenticators at AAL3.
- Govern enrollment and recovery for high-risk roles: review account recovery, MFA reset, device enrollment, backup-code, SMS, voice, and help desk procedures for public-data dependency and SIM-swap or impersonation risk, and require verified identity proofing before authenticator changes.
- Treat stolen session tokens and cookies as an MFA bypass: train personnel that infostealer malware harvests active sessions, require reporting of suspected stealer exposure, and trigger session revocation and credential reset through FA2.SC5.C2 containment.
- Train users that MFA prompts, one-time codes, recovery links, and approval fatigue can be social-engineering channels; require reporting and transaction holds for suspicious prompts or reset requests.
- Record MFA coverage by account population and high-risk role, exception owner, recovery-channel review, reset approvals, suspicious MFA events, user coaching, incident linkage, and residual-risk decisions.
- Route IAM architecture, authenticator selection, enrollment policy, conditional access, and technical enforcement to FA3 or the identity owner while FA2 owns phishing-resilience behavior, coverage evidence, and response linkage.

Evidence core:

- MFA coverage record by account population and high-risk role
- Exception inventory with owner, compensating control, and retirement date
- Recovery-channel review record with identity-proofing requirements and date

Applicability: from micro scale.

Related controls: FA2.SC5.C2.

FA2.SC3.C4: Credential Guessing and Recovery Exposure Handoff

Address how public personal or organizational information can weaken credential, password-reset, and account-recovery assumptions.

Implementation guidance:

- Teach personnel and help desk teams that birthdays, relatives, pets, schools, old employers, phone numbers, addresses, breached emails, usernames, and public profile details can be used in guessing, credential stuffing, and account recovery pretexts.
- Require credential-related training to reference approved password-management, breached-password, reset, and recovery procedures without duplicating IAM policy inside FA2.
- Record incidents or drills where public information supported credential guessing, recovery abuse, help desk impersonation, or approval fatigue, and link the finding to training, verification, and IAM remediation owners.
- Route password manager deployment, banned-password lists, breached-password checks, account lockout, recovery configuration, and shared-account elimination to FA3 or the identity owner.
- Use credential-exposure findings to update FA2 role training, FA2.SC2 verification rules, FA2.SC5 response playbooks, FA4 executive telecom/account controls, and FA5 monitoring where recurrence or evidence retention is required.

Evidence core:

- Training record covering public-information credential and recovery risks, with audience and date
- Incident or drill finding where public information enabled credential abuse, with remediation owner

Applicability: from small scale.

FA2.SC4: Remote Work Social Engineering Exposure

Objective. Reduce social-engineering and information-leakage risk in remote work, remote meetings, and distributed collaboration while routing technical access, endpoint, home-office, and executive-protection controls to their primary homes.

FA2.SC4.C1: Remote Work Visual and Audio Exposure Awareness

Train personnel to recognize visible, audible, and contextual remote-work exposures that can support social engineering.

Implementation guidance:

- Cover risks from screens, whiteboards, printed materials, calendars, family names, badges, delivery labels, smart speakers, background conversations, location cues, and personal social posts that reveal organizational context.

- Provide remote-work checklists that define what to hide, blur, move, mute, or avoid sharing before meetings, recordings, screenshots, livestreams, public posts, or customer-facing calls.
- Record training audience, scenario source, required behavior, exception path, reporting channel, and any role-specific requirement for executives, support staff, finance, HR, legal, administrators, or incident responders.
- Route home-office physical hardening, executive household exposure, travel routines, and private-life protection to FA4 or executive-protection material.
- Route endpoint controls, screen-capture prevention, collaboration-platform configuration, home-network security, and managed-device policy to FA3 while FA2 retains awareness, reporting, and meeting behavior.
- Use confirmed remote-work exposure findings to update FA1 public-content review, FA2 training, FA2.SC2 verification rules, and FA5 monitoring or metrics where recurring patterns appear.

Evidence core:

- Training completion record with audience, scenario source, and required behavior
- Issued remote-work checklist with date

Applicability: from small scale.

FA2.SC4.C2: Remote Meeting Security

Define meeting behaviors and evidence that prevent public-exposure-enabled impersonation, unauthorized attendance, and accidental disclosure.

Implementation guidance:

- Define requirements for attendee verification, meeting links, waiting rooms or admission controls, screen-share review, recording or transcript approval, chat/file handling, and post-meeting artifact cleanup for sensitive meetings.
- Require extra verification for meetings involving payment approval, vendor changes, incident response, executive instructions, legal matters, layoffs, M&A, unreleased product details, or privileged technical access.
- Record meeting owner, sensitivity, attendee verification, recording/transcript decision, shared artifact review, exception, incident trigger, and remediation or cleanup evidence.
- Route collaboration-platform configuration, access controls, retention settings, recording controls, and technical enforcement to FA3 or the platform owner.
- Route crisis-communications governance and enterprise incident-room procedures to FA5 while FA2 owns meeting-specific social-engineering and synthetic-media verification behavior.
- Retest remote meeting procedures through drills, deepfake scenarios, incident-response exercises, and post-incident reviews.

Evidence core:

- Defined sensitive-meeting requirements covering attendee verification and admission controls
- Sensitive-meeting record with owner, verification evidence, and recording decision
- Drill or post-incident retest evidence for meeting procedures

Applicability: from small scale.

FA2.SC4.C3: Remote Access Request Verification Handoff

Treat remote access requests, exceptions, and recovery actions as social-engineering targets that require verification evidence.

Implementation guidance:

- Define verification steps for VPN enrollment, remote-access exception requests, device replacement, MFA reset, emergency access, contractor access, support-session initiation, and privileged remote administration.
- Require request source, requester identity, business need, verifier, approved channel, expiration, compensating control, and closure evidence for remote-access exceptions.
- Train help desk, administrators, managers, and high-risk users to recognize public-source pretexts that claim travel, outage, urgent support, lost device, new phone, or executive pressure.
- Route VPN, endpoint, home-network, remote-desktop, conditional-access, DLP, and technical exposure assessment controls to FA3 or the primary access owner.
- Link suspected remote-access pretexting to FA2.SC5 incident response and to FA5 monitoring when patterns, indicators, or evidence-retention requirements recur.

Evidence core:

- Defined verification steps for remote-access, reset, and emergency-access requests
- Per-exception verification record with verifier, expiration, and closure evidence
- Help-desk and administrator training evidence on remote-access pretexts

Applicability: from small scale.

FA2.SC4.C4: Remote Document Pretext and Exposure Reporting

Train remote personnel to prevent and report document exposures that can support impersonation, fraud, or targeted pressure.

Implementation guidance:

- Define training for printed materials, shipment labels, whiteboard photos, screenshots, handwritten notes, customer files, legal packets, financial documents, and discarded drafts that reveal names, signatures, project context, approval paths, or account details.

- Require personnel to report lost, misdirected, photographed, publicly posted, or suspiciously requested documents that could enable social engineering or account recovery abuse.
- Record source, document type, exposed data elements, affected workflow, owner, action taken, notification or legal/privacy handoff, and residual-risk decision.
- Route document classification, secure disposal, retention policy, physical storage, DLP, asset inventory, and broad data-handling governance to FA1, FA3, FA5, or the organization's primary records owner as applicable.
- Use document-exposure reports to update remote-work training, publication review, verification rules, and incident-response scenarios.

Evidence core:

- Document-exposure training record with audience and date
- Exposure report record with document type, action taken, and residual-risk decision

Applicability: from small scale.

FA2.SC5: Incident Response for Social Engineering

Objective. Develop and implement specific incident response procedures for social engineering attempts and successful attacks, including rapid containment, investigation, and recovery steps.

FA2.SC5.C1: Incident Reporting Channels

Maintain accessible reporting channels for suspected phishing, impersonation, pretexting, canary contacts, and other social-engineering attempts.

Implementation guidance:

- Provide approved reporting paths for email, phone, SMS, chat, social media, support-ticket, vendor, in-person, physical-package, and canary-signal reports.
- Define channel owner, triage SLA, acknowledgement message, escalation criteria, evidence to preserve, employee feedback loop, and non-punitive handling requirements.
- Require reports to capture source, timestamp, channel, claimed identity, requested action, public information referenced, screenshots or headers where available, affected business process, and whether the employee clicked, replied, disclosed, or verified.
- Train employees that fast reporting is expected even if they clicked, replied, almost acted, or are unsure whether the event was malicious.
- Route recurring monitoring intake, trend analysis, and metrics to FA5 while FA2 owns social-engineering report quality and employee-facing response.

Evidence core:

- Published reporting channels with named owner and triage expectation

- Report records with source, timestamp, channel, and requested action
- Acknowledgement or feedback evidence to reporting employees

Applicability: from micro scale.

FA2.SC5.C2: Containment Actions

Define containment decisions for confirmed or suspected social-engineering incidents.

Implementation guidance:

- Maintain containment decision trees for credential disclosure, MFA prompt abuse, malicious-link interaction, malware execution, infostealer or session-token exposure, fraudulent payment or vendor change, data release, executive impersonation, deepfake request, physical pretext, and canary-signal trigger.
- Record incident type, initial report, affected person or workflow, public information used, containment authority, action taken, evidence preserved, customer/legal/privacy handoff, and residual-risk decision.
- Coordinate account disablement, credential reset, session revocation, endpoint isolation, message removal, domain or URL blocking, payment recall, vendor notification, and data-exposure review with FA3, FA5, finance, legal, privacy, and communications owners as appropriate; trigger session revocation and credential reset when stealer-log exposure or suspected session-token theft involves organizational accounts (FA5.SC1.C1).
- Issue targeted employee warnings when additional personnel may receive the same lure, pretext, fake profile, malicious link, or request pattern.
- Retest containment after closure by validating access state, payment or data handling outcome, employee warning coverage, and recurrence monitoring.

Evidence core:

- Containment decision tree covering credential, payment, and impersonation incident types
- Per-incident containment record with action taken, authority, and date
- Post-closure validation of access state and payment or data outcomes

Applicability: from micro scale.

Related controls: FA5.SC1.C1.

FA2.SC5.C3: Post-Incident Investigation and Learning

Investigate how public exposure, authority cues, technical controls, and verification behavior shaped a social-engineering event.

Implementation guidance:

- Identify the exposed condition or public-source cue that made the attempt credible, such as role authority, travel, project names, vendor relationships, org structure, personal contact data, executive media, or old documents.

- Gather indicators such as message headers, phone or chat metadata, call notes, fake profiles, domains, URLs, screenshots, attachment hashes, payment details, source artifacts, and user actions.
- Document timeline, affected workflow, weakened control assumption, containment action, business consequence, corrective owner, and evidence package.
- Determine whether the source exposure routes to FA1 content or PII remediation, FA3 technical exposure, FA4 executive or high-risk-person exposure, or FA5 monitoring, evidence, and reporting.
- Feed lessons into role training, verification thresholds, channel rules, technical protections, reporting paths, incident playbooks, and board/auditor summaries where the event reveals a Control Confidence Gap.

Evidence core:

- Investigation record naming the public-source cue that made the attempt credible
- Timeline with weakened control assumption, corrective owner, and evidence package
- Routing decision sending source exposure to its owning focus area

Applicability: from small scale.

FA2.SC5.C4: Support for Affected Users

Provide documented support, coaching, and remediation follow-up for people affected by social-engineering incidents.

Implementation guidance:

- Acknowledge reports and affected-user involvement in a non-punitive manner, preserving psychological safety and encouraging fast future reporting.
- Provide private coaching, refresher training, credential or account-recovery support, device or mailbox remediation coordination, and clear next steps based on the incident type.
- Record support owner, affected person or role, remediation action, coaching provided, privacy or HR handoff, completion date, retest need, and any retaliation or blame-prevention concern.
- For executive, assistant, family-adjacent, or public-profile incidents, route personal or household exposure handling to FA4 while FA2 preserves organizational verification, reporting, and training records.
- Use support outcomes to improve training, verification scripts, help desk procedures, and escalation paths without turning incident response into blame assignment.

Evidence core:

- Support record per affected person with owner, action, and completion date
- Coaching or refresher evidence with privacy or HR handoff where needed

Applicability: from small scale.

FA2.SC5.C5: Incident Response Plan Integration

Embed social-engineering scenarios into the broader incident response program with clear FA5 handoffs.

Implementation guidance:

- Maintain scenario playbooks for phishing, vishing, smishing, executive impersonation, payment diversion, account recovery abuse, help desk pretexting, fake profiles, brand impersonation, canary-signal triggers, deepfake requests, physical pretexts, and public document or PII abuse.
- Assign roles for intake, triage, technical analysis, containment, finance, HR, legal/privacy, communications, platform reporting, bank or law-enforcement contact, and closure approval.
- Preserve scenario source, exercise date, participants, decisions made, gaps found, corrective actions, retest date, communications approvals, and evidence package links.
- Route enterprise IR governance, crisis communications, evidence vaults, metrics, and lessons-learned reporting to FA5 while FA2 owns social-engineering scenario content and user-facing response behavior.
- Update playbooks after incidents, drills, new ODSF findings, material public-exposure changes, new executive media exposure, major vendor changes, or emerging synthetic-media tactics.

Evidence core:

- Scenario playbooks with assigned response roles
- Exercise record with participants, gaps found, and corrective actions
- Playbook update record after incidents, drills, or exposure changes

Applicability: from small scale.

FA2.SC5.C6: Emergency Verification and Communications Handoff

Define social-engineering-safe verification behavior for emergency communications while FA5 governs the broader crisis-communications architecture.

Implementation guidance:

- Define emergency verification rules for incident commanders, executives, finance, legal, communications, IT, external counsel, insurers, responders, and vendors when normal channels may be compromised or unavailable.
- Require approved emergency channels, verified participant records, fallback contact sources, authentication steps, permitted information types, expiration criteria, and evidence of periodic testing.

- Train participants to assume that an attacker may know names, titles, vendors, incident details, phone numbers, travel, or public event context, and to verify identity before acting on urgent requests.
- Record exercise results, failed contact attempts, channel changes, participant updates, exceptions, and post-incident improvements.
- Route channel architecture, crisis communications governance, retention, evidence vault records, and board/auditor reporting to FA5; route technical authenticators and device controls to FA3.

Evidence core:

- Defined emergency verification rules with approved channels and authentication steps
- Verified participant and fallback-contact records with dates
- Exercise results with failed contact attempts and resulting changes

Applicability: from mid scale.

FA2.SC6: Canary Signal Awareness and Reporting

Objective. Train personnel to recognize and report interactions with legal-approved canary identifiers, honeytokens, and monitored decoy artifacts governed through FA5.

FA2.SC6.C1: Canary Signal Awareness, Reporting, and Response Handoff

Where the organization operates governed canary signals or honeytokens under FA5.SC4, train personnel on approved signals within disclosure boundaries, maintain reporting behavior, and hand reports into incident response and monitoring; organizations without governed canary signals record this control as not applicable.

Implementation guidance:

- Train only on security-owned canary identifiers, honeytokens, decoy email aliases, decoy documents, source markers, or tokenized artifacts with a current FA5.SC4.C1 authorization record covering owner, purpose, approval basis, alert destination, and retirement criteria, and check training references against that register so content never references unapproved or retired signals. Governed honeytokens may also support detection of credential misuse and unauthorized collection; the artifacts, placement rules, logging, and technical isolation are owned by FA5.SC4, FA5.SC1.C5, and FA3.
- Explain the purpose of approved signals, the interactions that require reporting, and the difference between a canary trigger and ordinary business communication, with role-specific examples for frontline teams, help desk staff, finance, HR, executive assistants, and support teams; record which employee groups need awareness of each signal class and what details can be disclosed without reducing detection value or creating confusion with real people, customers, applicants, or vendors.

- Use internal examples, sanitized artifacts, and approved labels in training; limit distribution of materials that describe canary placement or trigger logic to audiences with a need to know, recording where such materials are stored and who can access them; and record any employee-facing disclosure decision that could affect signal usefulness, including audience, rationale, approval owner, and date. Public-profile, recruiting, metadata, code-repository, and social-platform placement decisions stay in FA5 deception governance with documented legal, communications, and platform review.
- Maintain the employee reporting path through FA2.SC5.C1's channels for messages, calls, support requests, vendor inquiries, or social-engineering attempts that mention an approved signal, capturing source, date, channel, referenced signal, requested action, screenshots or message headers where available, and affected business process; train frontline staff to acknowledge reports without revealing sensitive detection details, define acknowledgement and feedback expectations so reporters learn a report was received without learning detection specifics, and test the reporting path through periodic drills.
- Treat an external reference to a canary signal as a social-engineering indicator: escalate through FA2.SC5.C1 intake for triage and FA2.SC5.C2 for containment, agree severity, correlation, and escalation thresholds with FA5 monitoring owners so an isolated canary reference is distinguished from coordinated reconnaissance, and route signal-side response, tuning, and retirement to FA5.SC4.C4; preserve message content, source metadata, affected signal, triage decision, action owner, and closure outcome with the incident record.
- Review awareness modules after alerts, exercises, incidents, organizational changes, or FA5 signal changes; document training audience, date, learning objective, disclosure boundary, reporting path, and acknowledgement evidence for each module; track coverage, report quality, time to employee escalation, and false-positive trends, verifying through drills or spot checks that personnel recognize and report governed signals; use confirmed alerts to update social-engineering warnings and verification procedures; send evidence of confusing, stale, over-disclosed, or low-value signals to FA5 for governance review, tuning, or retirement; and record review owner, cadence, inputs, and resulting content or governance changes.

Evidence core:

- Training record per module with audience, date, and disclosure boundary
- Content check against the FA5.SC4 authorization register with date
- Canary-reference report and escalation record with triage decision and closure

Applicability: from mid scale; condition: governed canary signals under FA5.SC4.

Related controls: FA2.SC5.C1 · FA2.SC5.C2 · FA5.SC1.C5 · FA5.SC4.C1 · FA5.SC4.C4.

FA2.SC7: Deepfake and AI-Generated Content Defense

Objective. Prepare personnel and workflows to verify suspicious voice, video, text, and synthetic-media requests without relying on detector output alone.

FA2.SC7.C1: Voice Authentication Protocols

Define verification procedures for voice requests where synthetic audio, spoofed caller identity, or public-source context could create false trust.

Implementation guidance:

- Require approved callback paths, transaction holds, second approver review, or independent workflow confirmation for voice requests involving payments, account recovery, privileged access, data release, vendor changes, legal matters, or executive instructions.
- Avoid relying on personal knowledge questions, family details, recent travel, internal project names, or other facts that may be available through public sources or prior compromise.
- Record caller identity claim, channel, requested action, verification path, verifier, result, hold or escalation decision, and evidence preserved.
- Train high-risk roles to recognize voice-cloning risk, caller-ID spoofing, urgency pressure, and requests that reference public media, announcements, events, or personal context.
- Route voice biometric systems, telephony controls, identity-provider integrations, and technical authenticator selection to FA3 or the identity/communications owner.

Evidence core:

- Defined callback or transaction-hold procedure for sensitive voice requests
- Voice-verification record with caller claim, verifier, result, and date
- High-risk-role training evidence on voice-cloning and caller-ID spoofing

Applicability: from micro scale.

FA2.SC7.C2: Video Verification Measures

Define procedures for verifying sensitive video meetings, recordings, and live appearances that could be synthetic or impersonated.

Implementation guidance:

- Require attendee verification, meeting-source validation, live challenge procedures, out-of-band confirmation, or transaction holds before acting on sensitive video instructions.
- Record meeting owner, participant list, source link, sensitivity, verification method, recording or transcript handling, exception, escalation, and closure evidence.
- Train participants on synthetic-video risk, replayed recordings, compromised meeting links, avatar or voice substitution, and limitations of visual artifact spotting.

- Use provenance checks such as official calendar source, approved meeting room, prior verified contact, signed communication, or trusted workflow record where available.
- Route collaboration-platform configuration, meeting authentication, recording controls, and retention settings to FA3 or the platform owner while FA2 owns human verification behavior.
- Apply live verification to remote hiring interviews for sensitive roles, and verify candidate identity through documented checks before any access provisioning.

Evidence core:

- Defined verification and hold procedures for sensitive video instructions
- Per-meeting verification record with method, owner, and closure evidence
- Participant training evidence on synthetic-video and replay risk

Applicability: from small scale.

FA2.SC7.C3: AI-Personalized Lure Verification

Verify unusual text-based requests that may use AI-generated personalization, public business context, or prior communication style.

Implementation guidance:

- Train personnel that fluent writing, correct tone, recent business context, and familiar personal details do not prove legitimacy.
- Require verification for unusual requests involving money, credentials, access, legal documents, HR data, vendor changes, public statements, confidential attachments, or urgent executive instructions.
- Preserve reported lure text, source channel, claimed sender, public context referenced, requested action, verification result, technical telemetry where available, and employee response.
- Use AI-personalized lure reports to update phishing filters, role-based scenarios, verification rules, and monitoring criteria, without treating generic AI-text detector scores as sufficient control evidence.
- Route model-detection tooling, mail-security telemetry, and automated classification controls to FA2.SC3, FA3, or FA5 depending on ownership and evidence use.

Evidence core:

- Training record on AI-personalization risk with audience and date
- Preserved lure report with claimed sender, requested action, and verification result
- Filter, scenario, or verification-rule update fed by lure reports

Applicability: from small scale.

FA2.SC7.C4: Synthetic-Media Emergency Verification Handoff

Integrate suspected synthetic-media scenarios into FA2 verification and incident response while routing technical authenticators and crisis governance to their primary owners.

Implementation guidance:

- Define when suspected synthetic audio, video, text, or image content triggers transaction holds, alternate-channel verification, second approver review, incident escalation, or public communications review.
- Record suspected medium, source, claimed identity, requested action, verification steps, hold decision, technical evidence, escalation owner, and final disposition.
- Maintain scenario playbooks for deepfake executive instructions, fake vendor calls, synthetic incident updates, fraudulent public statements, manipulated meeting recordings, and AI-personalized phishing.
- Route shared emergency channel governance to FA2.SC5 and FA5, and route physical security keys, identity-provider configuration, device enrollment, and technical authenticators to FA3 or IAM owners.
- Use exercises and confirmed incidents to update FA2.SC2 verification rules, FA2.SC5 response playbooks, FA4 executive exposure controls, and FA5 monitoring and reporting.

Evidence core:

- Defined trigger rules for holds and alternate-channel verification
- Per-event record with suspected medium, verification steps, hold decision, and disposition
- Scenario playbook update evidence from exercises or confirmed incidents

Applicability: from mid scale.

Technology Exposure Management

Technology Exposure Management identifies, governs, and reduces externally observable technology assets, services, code artifacts, APIs, third-party technical surfaces, and automated collection paths. FA3 owns technical exposure evidence, remediation, retest, exception, and residual-risk records for systems and artifacts that attackers can discover or abuse from outside the organization. This focus area broadly orients to NIST CSF 2.0 asset management, risk assessment, platform security, infrastructure resilience, continuous monitoring, adverse event analysis, and supply chain governance categories.

Business rationale. Many breaches begin with attackers using internet-wide scan data, search engines, and automated scanning to find an organization's weak points: an open database, an unpatched server, a forgotten subdomain. Especially in a world of cloud and remote work, a company's internet-facing footprint can sprawl beyond headquarters' firewall. Technology exposure leads to incidents such as data leaks, ransomware (via exposed RDP or VPN), cryptojacking (via open cloud instances), etc. For a business, uncontrolled exposure means higher risk of compromise, service outages, and compliance violations (if, say, a database with customer data is left open). Managing this exposure keeps the organization's online systems known, tracked, and properly secured. It also feeds into customer trust - clients expect businesses to secure their systems, and a publicly discovered flaw can damage reputation. Furthermore, reducing exposure can lower the noise in security monitoring (fewer false alarms from unknown systems) and optimize resource focus on legitimate assets. In summary, systematic management of technical exposures deters opportunistic attacks and makes targeted attacks far more difficult.

Scope. This focus area covers external-facing technology assets and technical artifacts, including domains, subdomains, IPs, cloud services, SaaS tenants, remote access systems, public repositories, packages, containers, infrastructure-as-code, APIs, third-party hosted assets, shared technical workspaces, and automated collection controls. FA3 routes public-content approval to FA1, human verification and social-engineering behavior to FA2, executive/private-life device exposure to FA4, and monitoring governance, evidence vaults, metrics, and broad vendor governance to FA5.

NIST CSF 2.0 orientation: GV.SC · ID.AM · ID.RA · PR.PS · PR.IR · DE.CM · DE.AE

Focus-area alignment entries are broad orientation metadata indicating thematic overlap with NIST CSF 2.0 categories. They are not conformance mappings, control-level crosswalks, or claims of coverage. Control-level mappings to external standards are published separately as ODSF mapping packs.

FA3.SC1: External Asset Discovery and Inventory

Objective. Maintain an evidence-ready inventory of externally reachable or externally referenced technology assets, with owner, source, authorization, expected exposure, review cadence, closure, and residual-risk records.

FA3.SC1.C1: Domain and Subdomain Inventory

Maintain an authorized inventory of domains, subdomains, DNS records, certificates, and externally resolvable names.

Implementation guidance:

- Record domain or subdomain, registrar or DNS owner, business owner, technical owner, environment, purpose, expected exposure, data sensitivity, certificate source, registrar-lock status, DNSSEC posture, CAA policy, WHOIS privacy state, approval status, review cadence, and retirement criteria.
- Use approved discovery sources such as DNS zones, registrar records, certificate transparency, web crawls, cloud inventories, attack-surface tooling, and manual validation as evidence inputs.
- Validate DNS records against live, owned targets at each review cadence so records pointing at released or unclaimed resources are caught before takeover, covering CNAME, NS, MX, A/AAAA, and TXT service references.
- Classify unknown names as authorized, abandoned, shadow IT, vendor-hosted, fraudulent, or investigation pending, and record triage owner, decision, remediation action, retest, and closure evidence.
- Route website and campaign content disclosure to FA1 while FA3 records the technical asset, hosting, DNS, certificate, and service exposure evidence.
- Route brand lookalike, phishing, and recurring domain monitoring trends to FA5 when they become monitoring cases, metrics, or board/auditor reporting items.
- Preserve residual-risk approval for any externally resolvable name that remains exposed outside the expected baseline.
- Review certificate issuance practice so public certificate-transparency logs do not map internal hostnames; prefer wildcard or private-CA issuance for internal names.
- Reference cadence: quarterly review; organizations may substitute a documented equivalent cadence.

Evidence core:

- Domain and DNS inventory with owner and registrar-lock state
- Dated review result against live records
- Closure or exception record per drift or takeover-prone finding

Applicability: from small scale.

FA3.SC1.C2: Public IP and Cloud Asset Mapping

Map public IP addresses, cloud resources, and internet-reachable infrastructure to owners, business processes, and expected exposure.

Implementation guidance:

- Record public IP, cloud account or subscription, region, asset type, service owner, business process, exposure state, data sensitivity, expected access path, and change or deployment reference.
- Reconcile internet registry records, cloud provider inventories, load balancers, CDN endpoints, firewall rules, scanning results, and asset-management records.
- Distinguish organization-owned, subsidiary-owned, cloud-managed, vendor-hosted, and unknown public assets so remediation ownership is clear.
- Document whether each asset is intended to be public, restricted, temporary, retired, or under investigation, and preserve evidence for the decision.
- Route vendor-hosted public assets and shared infrastructure to FA3.SC4 while keeping the core public reachability record in the FA3 inventory.
- Track closure evidence, compensating controls, and residual-risk acceptance for any exposed asset that cannot be removed or restricted.

Evidence core:

- Public IP and cloud asset inventory with owner and exposure state
- Dated reconciliation result against provider and registry records
- Closure or residual-risk record per unknown or exposed asset

Applicability: from small scale; condition: organization-controlled public IPs or cloud resources.

FA3.SC1.C3: Service and Port Exposure Baseline

Define and validate the expected externally visible services, ports, banners, and management interfaces for each public asset.

Implementation guidance:

- Create an expected-service baseline for each public asset, including permitted ports, protocols, service names, management interfaces, authentication requirements, exposure rationale, and owner approval.
- Preserve scan timestamp, scan source, coverage, externally indexed evidence, banner or screenshot evidence where available, and comparison against the expected baseline.
- Triage unauthorized services, exposed databases, administrative consoles, remote access points, debug endpoints, default pages, and unexpected banners as findings with owner, severity, remediation, retest, and closure evidence.
- Route vulnerability and configuration remediation to FA3.SC2 while SC1 retains the inventory and expected-baseline record.

- Require exception approval, expiration, compensating controls, and residual-risk rationale for services that remain externally reachable outside the standard baseline.
- Validate that origins behind CDN or WAF services are not directly reachable at their network addresses, and treat recovered origin exposure as a finding.

Evidence core:

- Expected-service baseline per public asset with owner approval
- Dated scan result compared against the baseline
- Remediation or exception record per unexpected service or exposed origin

Applicability: from small scale; condition: organization-operated internet-facing services.

FA3.SC1.C4: Cloud, SaaS, and Vendor-Hosted Asset Inventory

Track externally reachable cloud services, SaaS tenants, public links, and vendor-hosted technical assets that represent the organization.

Implementation guidance:

- Record service name, tenant or workspace identifier, public URL, vendor or hosting owner, internal owner, data category, authentication model, sharing model, expected public exposure, and review cadence.
- Include public dashboards, support portals, collaboration spaces, file-sharing links, developer environments, analytics portals, customer portals, and vendor-operated systems that expose organizational data or technical context.
- Classify shadow IT and unapproved public services by business owner, data handled, public reachability, access model, remediation path, and closure evidence.
- Route procurement approval, contract terms, recurring vendor governance, and vendor risk policy to FA5 while FA3 owns the externally reachable technical asset record.
- Route mobile app store metadata and public app artifacts to FA1.SC7; route API authentication, authorization, traffic, storage, and binary technical remediation to FA3 controls.
- Retain residual-risk approval for vendor-hosted or SaaS exposure that cannot be directly remediated by the organization.

Evidence core:

- SaaS and vendor-hosted asset inventory with owner and expected exposure
- Triage record per shadow or unapproved service with closure evidence
- Residual-risk approval for exposure the organization cannot directly remediate

Applicability: from small scale.

FA3.SC1.C5: Continuous Asset Discovery

Operate recurring discovery and reconciliation workflows for new, changed, abandoned, or unauthorized external technology assets.

Implementation guidance:

- Define discovery cadence, source coverage, reconciliation method, owner, alert destination, false-positive handling, and coverage metric for domains, certificates, IPs, cloud resources, SaaS tenants, services, APIs, and repositories.
- Integrate deployment, change-management, cloud, DNS, certificate, and inventory workflows so new external assets receive owner approval and expected-exposure records before or at release.
- Investigate newly discovered or changed assets as authorized, unauthorized, shadow IT, abandoned, fraudulent, vendor-hosted, or false positive, and record evidence for the classification.
- Detect dangling DNS records and takeover-prone references during discovery, including CNAMEs to deprovisioned SaaS or storage targets, NS delegations to expired zones, MX hosts no longer under control, and addresses released back to cloud pools; triage each as an urgent finding, since a dangling record lets an attacker publish content or receive mail under an organizational name.
- Track remediation owner, due date, closure artifact, retest result, exception, residual-risk decision, and recurrence trigger for assets that deviate from the baseline.
- Route monitoring program metrics and board/auditor trend reporting to FA5 while FA3 retains technical discovery, validation, remediation, and retest evidence.
- Reference cadence: monthly discovery and reconciliation; organizations may substitute a documented equivalent cadence.

Evidence core:

- Dated discovery sweep result with source coverage and owner
- Disposition record per new or changed asset
- Remediation or residual-risk record per deviating or takeover-prone asset

Applicability: from mid scale.

FA3.SC2: Vulnerability and Configuration Management

Objective. Identify, prioritize, remediate, retest, and document vulnerabilities or misconfigurations in external-facing systems that attackers can discover or exploit.

FA3.SC2.C1: External Vulnerability Scan Coverage

Maintain evidence that externally reachable assets are scanned and assessed for public exploitability.

Implementation guidance:

- Define scan scope from the FA3.SC1 inventory, including domains, IPs, cloud resources, SaaS-exposed assets, web applications, APIs, remote access systems, and public storage or configuration surfaces.
- Record scan type, scan date, source, coverage, authenticated or unauthenticated status, vulnerability-signature currency, exclusions, false-positive handling, and owner for each scan cycle.
- Prioritize findings by external reachability, exploit availability, known-exploited status, business criticality, data sensitivity, exposure duration, and whether the weakness supports account recovery, fraud, lateral movement, or customer-impacting compromise.
- Create remediation records with asset owner, severity basis, due date, compensating control, exception approval, retest result, closure evidence, and residual-risk decision.
- Trigger out-of-cycle assessment after major deployments, internet-exposed configuration changes, credible exploit advisories, observed attack activity, incident findings, or monitoring alerts.
- Route recurring monitoring metrics and executive reporting to FA5 while FA3 retains scan evidence, remediation evidence, and technical closure records.
- An existing vulnerability-management program's records satisfy this control's evidence expectation by reference; FA3 adds external-reachability prioritization and the reconnaissance-value lens.
- Reference cadence: quarterly external scans; organizations may substitute a documented equivalent cadence.

Evidence core:

- Dated external scan result with coverage against the asset inventory
- Remediation record per finding with owner, due date, and retest
- Exception or residual-risk record for unremediated exposure

Applicability: from small scale.

FA3.SC2.C2: Exposure-Based Patch and Mitigation

Apply patching, mitigation, or compensating controls based on external exploitability and business impact.

Implementation guidance:

- Maintain software, platform, firmware, dependency, image, and service-version evidence for externally reachable assets where public version or fingerprint data can guide attackers.
- Use vulnerability advisories, scanner findings, known-exploited catalogs, exploit intelligence, vendor guidance, and incident findings to determine affected assets and remediation urgency.
- Define patch or mitigation SLAs by external exposure, known exploitation, asset criticality, data sensitivity, attack path, and customer or business impact.

- Record patch decision, maintenance window, emergency mitigation, configuration workaround, disabled feature, compensating control, owner, approval, retest evidence, and residual-risk approval.
- Review delayed remediation through a documented exception path with expiration date, monitoring requirement, customer or legal/privacy impact review where relevant, and escalation criteria.
- Summarize unresolved high-risk exposure in board/auditor language that identifies the exposed condition, weakened control assumption, business consequence, mitigation status, and residual-risk owner.
- An existing patch-management program's records satisfy this control's evidence expectation by reference.

Evidence core:

- Patch or mitigation record per affected asset with owner and date
- Retest or validation evidence after patch or mitigation
- Exception record with expiration and residual-risk approval for delayed remediation

Applicability: from small scale.

FA3.SC2.C3: External Configuration Baselines

Define and validate secure baselines for externally visible services, management interfaces, storage, APIs, and error responses.

Implementation guidance:

- Define external baselines for allowed services, management exposure, authentication, network restrictions, TLS, default accounts, public storage, directory listing, verbose errors, API response detail, headers, and software-version disclosure.
- Preserve baseline source, asset owner, configuration evidence, validation method, test date, deviation, exception, remediation action, and retest result.
- Treat exposed administrative interfaces, open databases, default credentials, unauthenticated storage, debug modes, verbose stack traces, and unsafe TLS as findings with tracked remediation and residual-risk decisions.
- Limit externally visible banners, filenames, stack traces, environment names, internal hostnames, user identifiers, and dependency details where disclosure would materially improve reconnaissance or exploit selection.
- Route publication content leakage to FA1 and recurring monitoring or evidence-vault reporting to FA5 while FA3 owns technical configuration evidence and closure.

Evidence core:

- Documented external baseline with source and asset owner
- Dated validation result with deviations identified

- Remediation or exception record per deviation with retest

Applicability: from small scale; condition: organization-operated internet-facing services.

FA3.SC2.C4: External Attack-Path Testing

Perform authorized testing that validates whether external technical exposure can be chained into material compromise or control bypass.

Implementation guidance:

- Define scope, authorization, rules of engagement, testing window, data-handling restrictions, production-safety limits, contact paths, and evidence expectations before testing.
- Include external asset discovery, service enumeration, web and API testing, cloud exposure, repository exposure, remote access exposure, and chained paths from public clues to technical compromise.
- Record findings with exposed condition, exploit or abuse path, affected asset, weakened control assumption, business consequence, evidence artifact, remediation owner, retest requirement, and closure result.
- Route social-engineering test content to FA2 and enterprise exercise governance to FA5, while FA3 retains external technical testing scope, findings, remediation, and retest evidence.
- Use testing results to update FA3.SC1 inventory coverage, FA3.SC2 baselines, FA3.SC3 repository controls, FA3.SC4 third-party technical exposure, and FA5 metrics.

Evidence core:

- Dated test report with authorized scope and rules of engagement
- Finding record with abuse path, business consequence, and remediation owner
- Retest or closure result per finding

Applicability: from mid scale.

FA3.SC2.C5: Remote Access and Management Interface Hardening

Control external exposure of remote access, administrative, cloud-management, IoT, OT, and support interfaces.

Implementation guidance:

- Inventory externally reachable VPN, remote desktop, SSH, administrative web interfaces, cloud consoles, remote support tools, network appliances, IoT, OT, and building or facility systems.
- Require secure access paths such as managed gateways, segmentation, allowlists, phishing-resistant MFA where feasible, recovery-channel review, session logging, alerting, and rapid disablement procedures.

- Prohibit or formally except direct internet exposure of high-risk management interfaces, with documented business need, compensating controls, expiration date, monitoring, and residual-risk approval.
- Preserve exposure scan evidence, patch/configuration evidence, access-control evidence, login or session telemetry, unusual-activity alerts, remediation tickets, and retest results.
- Route user verification behavior, help desk reset training, and deepfake-safe remote-access requests to FA2; route recurring monitoring trends, crisis escalation, and board/auditor reporting to FA5.

Evidence core:

- Inventory of externally reachable remote-access and management interfaces with access-control state
- Dated exposure scan or validation evidence
- Exception record with compensating controls, expiration, and residual-risk approval

Applicability: from micro scale.

FA3.SC2.C6: Outbound Email and Domain Authentication Posture

Enforce and evidence outbound email authentication for all owned domains so organizational mail cannot be credibly spoofed, treating published authentication posture as externally enumerable exposure.

Implementation guidance:

- Publish and maintain SPF, DKIM, and DMARC for every owned domain and subdomain that sends mail, and bring DMARC to an enforcement policy (quarantine or reject) on a documented timeline; align records to RFC 9989 (DMARC, obsoletes RFC 7489 and RFC 9091) with aggregate and failure reporting per RFC 9990 and RFC 9991.
- Treat authentication posture as public exposure: a missing or unenforced DMARC policy is enumerable by anyone through DNS and signals that impersonation mail will deliver; check posture for all registered domains, and publish restrictive records for non-sending and parked domains (SPF that fails all sources and DMARC reject).
- Deploy MTA-STS and TLS-RPT to protect mail transport, and evaluate BIMI where brand-impersonation risk justifies it; record owner, decision, and rationale where these are not deployed.
- Monitor DMARC aggregate and failure reports for unauthorized senders, spoofing attempts, vendor senders missing authentication, and forwarding breakage; route confirmed impersonation campaigns to FA2.SC5 response and FA5 monitoring.
- Record per-domain posture evidence: policy state, enforcement level, alignment mode, authorized senders, reporting destinations, change owner, review cadence, exception rationale, and residual-risk decision for any domain below enforcement.

- Route mail-platform configuration and DNS change execution to the messaging or DNS platform owner; FA3 retains the posture baseline, validation evidence, and remediation records that FA2.SC3.C1 consumes for social-engineering response.

Evidence core:

- Per-domain SPF, DKIM, and DMARC state with enforcement level
- Dated validation result against live DNS records
- Exception and residual-risk record per domain below enforcement

Applicability: from micro scale.

Related controls: FA2.SC3.C1.

FA3.SC3: Managing Data Exposure in Code and Repositories

Objective. Prevent, detect, remediate, and document exposure of secrets, internal architecture, credentials, source code, packages, containers, infrastructure-as-code, and technical artifacts through repositories or developer workflows.

FA3.SC3.C1: Public Repository Release Review

Review public repositories and release artifacts before publication and after material changes.

Implementation guidance:

- Require pre-publication review for secrets, credentials, tokens, internal hostnames, environment names, private IPs, customer data, stack traces, debug output, architecture diagrams, support paths, and exploit-enabling configuration details.
- Preserve review owner, repository owner, release purpose, secret-scan result, dependency or package manifest review, commit-history check, exception, approval, and publication date.
- Review issue trackers, pull requests, wiki pages, examples, test fixtures, screenshots, build logs, release notes, and discussions for accidental technical exposure.
- If sensitive material is published, record exposed artifact, affected secret or system, credential rotation, revocation, takedown or history-removal action, fork or clone impact, retest, and residual-risk decision.
- Route official public-content approval and marketing release language to FA1 while FA3 owns code, repository, package, and technical artifact exposure evidence.

Evidence core:

- Pre-publication review record with secret-scan result, reviewer, and date
- Rotation and takedown record per published secret or sensitive artifact

Applicability: from small scale; condition: public code repositories.

FA3.SC3.C2: Private Repository Exposure Prevention

Control private repository access, visibility, and egress paths that could turn source code or secrets into public exposure.

Implementation guidance:

- Maintain repository owner, visibility, access group, privileged maintainer list, third-party access, branch protection or review requirement, backup location, and offboarding review evidence.
- Require MFA or equivalent account protection for repository administrators and high-risk contributors, and route identity architecture to FA3 IAM owners or the primary identity program.
- Track visibility changes, fork permissions, clone or export activity, service-token access, CI/CD secret access, and unusual repository access where available.
- Use approved secret scanning, commit hooks, pre-receive checks, or equivalent controls to reduce the chance that credentials enter private repositories and later become public exposure.
- Record access reviews, exceptions, departed-user removal, secret findings, credential rotation, incident linkage, and residual-risk decisions.
- Route general SDLC policy to the primary engineering governance home while FA3 retains exposure-prevention evidence for source code, secrets, and repository artifacts.

Evidence core:

- Repository access record with owner, visibility, and protection state
- Dated access review with departed-user removal evidence
- Secret finding record with rotation outcome

Applicability: from small scale; condition: private code repositories.

FA3.SC3.C3: Public Package, Container, and IaC Review

Review packages, containers, infrastructure-as-code, build artifacts, and shared code before public or third-party distribution.

Implementation guidance:

- Review package manifests, source distributions, compiled artifacts, containers, build contexts, environment files, sample configs, logs, infrastructure-as-code templates, deployment examples, and documentation before publication.
- Preserve artifact owner, registry or distribution channel, intended audience, scan result, secret or credential check, internal-reference review, approval, exception, and release date.
- Check public registries and shared vendor channels for accidental publication of private packages, images, templates, environment files, or build artifacts.

- If exposure occurs, record registry action, artifact removal, credential rotation, dependent system impact, third-party or customer notification need, retest, and closure evidence.
- Route supply-chain governance and external consumer communication policy to FA5 while FA3 owns technical artifact review and remediation evidence.

Evidence core:

- Pre-release artifact review record with scan result and approver
- Registry check result for accidental private-artifact publication
- Removal and rotation record per exposed artifact

Applicability: from small scale; condition: public package, container, or artifact distribution.

FA3.SC3.C4: Code and Secret Leak Monitoring

Monitor public code, paste, package, and repository sources for exposed secrets, internal identifiers, and technical artifacts.

Implementation guidance:

- Define monitored terms, domains, email patterns, repository names, project names, package names, internal hostnames, credential formats, token patterns, cloud identifiers, and unique technical strings.
- Monitor approved public sources such as code hosts, package registries, paste sites, container registries, search indexes, issue trackers, public forks, and third-party development workspaces.
- Record alert source, timestamp, artifact URL or identifier, source owner where known, affected secret or system, verification result, severity, triage owner, and false-positive decision.
- For confirmed leaks, execute rotation, revocation, takedown, access review, fork or clone assessment, affected-system review, retest, and residual-risk approval.
- Route monitoring governance, lawful collection boundaries, metrics, and evidence-vault records to FA5 while FA3 owns technical validation and remediation of code or secret exposure.
- Reference cadence: weekly alert review; organizations may substitute a documented equivalent cadence.

Evidence core:

- Monitored-term and source coverage list with owner
- Triage record per alert with verification result and disposition
- Rotation, revocation, or takedown evidence per confirmed leak

Applicability: from small scale; condition: in-house software development.

FA3.SC3.C5: Developer Exposure-Prevention Process

Embed measurable developer workflow controls that prevent secrets, internal details, and sensitive technical artifacts from becoming public exposure.

Implementation guidance:

- Define developer workflow requirements for secret management, local configuration, sample data, debug output, public examples, issue comments, screenshots, build logs, public forum posts, and open-source releases.
- Require review checklists or automated controls for secrets, internal endpoints, customer data, credentials, tokens, package contents, container contents, and infrastructure-as-code before external sharing.
- Preserve adoption evidence such as enabled repository checks, scan coverage, code-review checklist use, exception records, training completion where required, and recurring findings by team or workflow.
- Route enterprise training governance to FA5 and general social-engineering awareness to FA2; FA3 owns developer process evidence tied to technical public exposure prevention.
- Use incidents, leak monitoring, external testing, and package review failures to update developer workflows, tool configuration, review checklists, and retest expectations.

Evidence core:

- Enabled repository check and secret-scan coverage evidence
- Recurring-finding record by workflow with corrective action and owner

Applicability: from mid scale; condition: in-house software development.

FA3.SC4: Exposure via Third Parties and Supply Chain

Objective. Govern technical exposure created by vendors, partners, shared infrastructure, third-party scripts, partner-accessible workspaces, technical disclosures, and third-party access paths.

FA3.SC4.C1: Third-Party Technical Exposure Assessment

Assess vendors and partners that host, integrate with, administer, or publicly disclose technical assets connected to the organization.

Implementation guidance:

- Identify vendors and partners that operate public portals, support systems, managed infrastructure, APIs, scripts, integrations, authentication paths, customer-facing pages, or technical workspaces on the organization's behalf.
- Record vendor name, service, technical asset, hosting model, owner, data category, integration type, public exposure, access path, review cadence, and remediation contact.

- Assess public technical disclosures such as case-study architecture claims, support documentation, implementation screenshots, integration guides, exposed portals, leaked configuration, or vendor breach statements that change the organization's exposure assumptions.
- Route broad vendor due diligence, contract language, vendor risk scoring, procurement approval, and regulatory vendor governance to FA5 while FA3 owns technical exposure facts and remediation evidence.
- Route vendor personnel personal-data or executive/private-life exposure to FA4-facing material; FA3 records only organization-relevant technical access, support, and integration exposure.
- Preserve remediation request, vendor response, retest, compensating control, exception, and residual-risk approval where vendor-controlled exposure remains.

Evidence core:

- Vendor technical-exposure record with asset, hosting model, and owner
- Dated assessment result per connected vendor
- Remediation request with vendor response and residual-risk disposition

Applicability: from mid scale.

FA3.SC4.C2: Shared Infrastructure Mapping

Map shared services, hosted portals, third-party scripts, integrations, and dependencies that can alter the organization's external technical exposure.

Implementation guidance:

- Maintain an inventory of shared infrastructure and third-party components such as hosted portals, tenant configurations, embedded scripts, analytics tags, chat widgets, payment pages, CDNs, identity integrations, support portals, and customer-facing vendor pages.
- Record owner, vendor contact, dependency purpose, public URL or asset identifier, data handled, script or integration permissions, authentication model, configuration owner, and expected exposure.
- Preserve evidence for script integrity controls, content security policy, tenant settings, access restrictions, patch or configuration status, dependency review, vendor remediation handoff, and residual-risk decision.
- Review whether a third-party outage, compromise, disclosure, or configuration change weakens assumptions about customer trust, payment integrity, authentication, data exposure, or incident response.
- Route recurring vendor governance and executive reporting to FA5 while FA3 keeps shared technical dependency evidence and retest records.

Evidence core:

- Shared infrastructure and third-party script inventory with owner and purpose
- Dated control-state evidence per shared dependency (integrity, policy, configuration)
- Remediation handoff or residual-risk record per weakened dependency

Applicability: from small scale.

FA3.SC4.C3: Partner-Accessible Technical Workspace Controls

Control technical data exposed through partner-accessible repositories, issue trackers, support portals, shared workspaces, and collaboration channels.

Implementation guidance:

- Inventory partner-accessible workspaces that contain technical information, including shared repositories, tickets, support cases, chat channels, data rooms, documentation portals, file shares, logs, screenshots, and implementation notes.
- Define permitted data types, prohibited content, access owner, external participants, expiration, review cadence, logging, and offboarding process for each workspace.
- Prohibit or formally except sharing of secrets, credentials, production data, unredacted logs, private keys, internal-only architecture, and unsupported recovery paths in partner-accessible spaces.
- Preserve access review evidence, external participant list, workspace owner, sensitive-content review, expiration or closure record, incident handoff, and residual-risk decision.
- Route broad data-sharing policy and records governance to FA5, social-engineering channel behavior to FA2, and public release approval to FA1.

Evidence core:

- Partner-accessible workspace inventory with owner and external participants
- Dated access and sensitive-content review result
- Exception or closure record with residual-risk decision

Applicability: from small scale; condition: partner-accessible technical workspaces.

FA3.SC4.C4: Third-Party Technical Disclosure Monitoring

Monitor vendor, partner, and public ecosystem disclosures that reveal technical architecture, integrations, support paths, or exposure changes.

Implementation guidance:

- Track vendor case studies, implementation guides, screenshots, support articles, conference material, status pages, breach notices, public roadmaps, customer references, and partner documentation for technical details about the organization.
- Record disclosure source, URL or artifact, retrieval date, vendor or partner owner, technical detail exposed, affected asset or control assumption, business consequence, and remediation owner.

- Classify disclosures as public-content approval issue, technical exposure issue, vendor governance issue, incident indicator, or residual-risk item, and route accordingly.
- Retain FA3 ownership for disclosures that reveal technical stack, architecture, integration paths, admin surfaces, APIs, remote access, data flows, or vendor-hosted exposure.
- Route partner-publication approval and customer-story content to FA1 and FA5, while FA3 records technical mitigation, retest, and residual-risk evidence.

Evidence core:

- Disclosure record with source, retrieval date, and technical detail exposed
- Classification and routing decision per disclosure
- Mitigation or residual-risk record per affected asset or control assumption

Applicability: from mid scale.

FA3.SC4.C5: Third-Party Technical Access Controls

Limit, monitor, review, and retire third-party technical access paths that could become externally enabled compromise routes.

Implementation guidance:

- Maintain an inventory of third-party accounts, service accounts, API keys, remote access paths, integration scopes, privileged roles, support sessions, and vendor-managed identities.
- Require least privilege, segmentation, scope limits, MFA or equivalent controls, recovery-channel review, logging, owner approval, expiration, and offboarding evidence for third-party technical access.
- Monitor third-party activity for unusual access time, source location, data volume, administrative action, token use, configuration change, or support-session behavior.
- Record access review date, reviewer, owner, scope, justification, exception, unusual-activity triage, remediation action, and closure evidence.
- Route business verification procedures to FA2 and broad vendor governance to FA5 while FA3 owns technical access controls, logs, exceptions, and retest records.

Evidence core:

- Third-party access inventory with owner, scope, and expiration
- Dated access review with reviewer and offboarding evidence
- Unusual-activity triage or exception record with closure

Applicability: from small scale.

FA3.SC5: Defense Against Automated OSINT Collection

Objective. Limit, detect, and respond to automated collection of externally exposed organizational data, technical metadata, APIs, and public-facing content.

FA3.SC5.C1: Automated and AI-Driven Collection Abuse Controls

Apply layered controls that reduce bulk harvesting and AI-assisted collection from public websites, portals, directories, search interfaces, and high-value public pages.

Implementation guidance:

- Identify protected data classes such as employee names, titles, contact paths, support workflows, customer references, account recovery hints, document metadata, pricing or procurement signals, and technical identifiers.
- Inventory public surfaces where automated agents, crawlers, scrapers, and AI-assisted collection workflows can collect or correlate high-risk data, including websites, APIs, documents, schema metadata, structured data, directories, search endpoints, developer docs, and support artifacts.
- Define rate limits, query limits, pagination limits, download limits, bot detection, anomaly thresholds, allowlist or denylist logic, and abuse-response actions for high-value public endpoints, with data and response minimization, crawler directives where applicable, tokenized artifacts, and source-specific alerting for agent and scraper traffic.
- Use human-verification, friction, or challenge mechanisms only where they fit accessibility, privacy, user experience, and business requirements; record the rationale and impact review.
- Record model/crawler access policy decisions, protected data classes, technical controls, observed agent or scraper behavior, alert thresholds, response actions, and residual-risk decisions.
- Preserve bot telemetry, source indicators, request patterns, endpoint affected, data class targeted, control action, false-positive handling, escalation, and closure evidence.
- Avoid treating speculative AI-detection claims as control evidence; preserve observable telemetry, source artifacts, endpoint behavior, and remediation records.
- Route public-content minimization to FA1, synthetic-media social-engineering readiness to FA2, deception or canary approvals to FA5, and legal terms, data-use policy, recurring monitoring metrics, and evidence-vault handling to FA5; FA3 owns technical anti-collection controls, telemetry, and remediation evidence.
- Document residual risk where public business requirements make bulk collection technically possible despite controls.

Evidence core:

- Inventory of high-value public endpoints with protected data classes
- Deployed anti-collection control record per endpoint with owner
- Abuse-event triage record with response action and closure evidence

Applicability: from mid scale; condition: data-rich public sites or search endpoints.

FA3.SC5.C3: API Data Harvesting Controls

Secure APIs against unauthorized enumeration, bulk extraction, object-level access abuse, and excessive response disclosure.

Implementation guidance:

- Maintain an API inventory with owner, endpoint, data class, authentication requirement, authorization model, object-level access pattern, rate limit, scope model, logging source, and public documentation status.
- Test API authorization, object-level access, pagination, search, export, enumeration, token scope, error handling, and response minimization for externally reachable APIs.
- Record abuse thresholds, rate-limit policy, token or key owner, suspicious usage telemetry, triage owner, remediation action, retest result, and exception approval.
- Minimize API responses so unauthenticated or low-privilege callers cannot collect unnecessary identifiers, metadata, relationship graphs, recovery hints, or internal implementation details.
- Route mobile app public clues to FA1.SC7 until technical API remediation is required; FA3 owns API authentication, authorization, rate limiting, logging, abuse triage, and retest evidence.

Evidence core:

- API inventory with owner, authentication, and rate-limit state
- Dated authorization and enumeration test result per externally reachable API
- Abuse-triage or remediation record with retest outcome

Applicability: from small scale; condition: externally reachable APIs.

FA3.SC5.C4: Externally Exposed Data-Flow Limits

Limit data flows from public or partner-accessible systems that allow automated collection, correlation, or bulk export.

Implementation guidance:

- Identify public or partner-accessible data flows such as search results, exports, directories, federated identity metadata, support portals, public dashboards, analytics endpoints, document repositories, and integration feeds.
- Define data minimization, field suppression, query limits, export limits, authentication requirements, scope limits, retention, logging, and review cadence for externally exposed data flows.
- Record data-flow owner, source system, destination, public or partner accessibility, data elements exposed, business purpose, control evidence, exception, and residual-risk decision.

- Route internal DLP, segmentation, encryption, and least-privilege architecture baselines to the primary security governance or platform-control homes; FA3 retains externally exposed data-flow limits tied to automated collection risk.
- Use findings from scraping, API abuse, third-party disclosure, and repository leaks to update data-flow limits, publication reviews, and monitoring rules.

Evidence core:

- Externally exposed data-flow record with owner, elements exposed, and purpose
- Dated control evidence per flow (field suppression, query and export limits)
- Exception or residual-risk record per flow exceeding limits

Applicability: from mid scale.

Executive Exposure Protection

Executive Exposure Protection governs public and semi-public information about executives, board members, founders, public spokespeople, executive assistants, and other high-risk personnel where that information can weaken organizational controls. FA4 covers executive personal data, household and family-adjacent exposure, account recovery dependencies, mobile and telecom exposure, public appearances, impersonation, doxing, coercion, fraud, and reputation attacks when those conditions can affect business authority, continuity, incident response, board confidence, or customer trust. This focus area broadly orients to NIST CSF 2.0 roles, risk management, risk assessment, identity and access assumptions, awareness, monitoring, incident management, and response communication categories.

Business rationale. Executives and other high-risk personnel carry unusual public-exposure risk because attackers can combine personal data, authority cues, public media, travel context, financial signals, family associations, assistants, and delegated workflows into fraud, account recovery abuse, social engineering, coercion, or public-trust attacks. Executive compromise can bypass ordinary control assumptions because the executive may approve payments, direct staff, influence incident communications, authorize exceptions, or become a pressure point during extortion. FA4 turns executive exposure into governed evidence: authorized scope, consent, source records, abuse paths, remediation actions, compensating controls, residual-risk decisions, and board/auditor-ready summaries.

Scope. This focus area applies to organization-relevant exposure involving executives, board members, founders, public spokespeople, executive assistants, and similarly high-risk personnel. It includes consent-based exposure audits, data broker and public-record suppression, personal-account and telecom recovery risk, executive device and BYOD bridge risk, executive-targeted monitoring and response, public appearance exposure, household contact paths, family-adjacent exposure, financial-authority abuse, disinformation, likeness abuse, and executive identity monitoring. FA4 routes general public-content governance to FA1, social-engineering verification and training behavior to FA2, durable technical controls to FA3, and recurring monitoring governance, evidence vaults, metrics, and enterprise incident records to FA5.

NIST CSF 2.0 orientation: GV.RR · GV.RM · ID.RA · PR.AA · PR.AT · DE.CM · RS.MA · RS.CO

Focus-area alignment entries are broad orientation metadata indicating thematic overlap with NIST CSF 2.0 categories. They are not conformance mappings, control-level crosswalks, or claims of coverage. Control-level mappings to external standards are published separately as ODSF mapping packs.

FA4.SC1: Executive Digital Footprint Management

Objective. Maintain a consent-based inventory of executive and high-risk-person public exposure, with owner, source, abuse path, remediation evidence, recurrence monitoring, and residual-risk records.

FA4.SC1.C1: Executive Exposure Audit

Assess public and semi-public exposure for executives and high-risk personnel where the exposure can affect organizational authority, fraud risk, account recovery, coercion, or incident response.

Implementation guidance:

- Define the authorized scope for each executive or high-risk person, including role, business authority, public profile, approved identifiers, consent basis, data categories, excluded areas, reviewer, and review cadence.
- Inventory public names, aliases, personal emails, phone numbers, addresses, relatives, public records, social profiles, media appearances, biographies, domains, leaked credentials, public documents, and business-used personal accounts where they can create organization-relevant risk.
- Record source URL or identifier, retrieval date, collection method, affected role or workflow, exposed condition, abuse path, severity basis, remediation owner, and confidence level.
- Classify findings by weakened assumption, such as identity verification, account recovery, payment approval, emergency communication, executive authority, board communications, incident response, or customer trust.
- Route workforce or customer PII exposure to FA1.SC4, social-engineering verification behavior to FA2, technical account and device controls to FA3, and recurring monitoring governance to FA5 while FA4 retains the executive exposure record.
- Preserve remediation action, retest result, recurrence trigger, compensating control, residual-risk approval, and board/auditor summary for unresolved exposure.
- Record residual-risk acceptance on an executive's own exposure one level up from the affected executive, with board risk or audit committee sign-off for chief-executive subjects.
- Reference cadence: annual audit per covered person; organizations may substitute a documented equivalent cadence.

Evidence core:

- Authorized scope record per executive with consent basis and excluded areas
- Dated exposure findings with source, abuse path, and remediation owner
- Remediation or residual-risk record per finding with one-level-up acceptance

Applicability: from small scale; condition: executives or other high-risk public-profile personnel.

FA4.SC1.C2: High-Risk Person Data Broker Suppression

Suppress brokered and people-search exposure for executives and other high-risk personnel through documented requests, verification, recurrence monitoring, and residual-risk treatment.

Implementation guidance:

- Maintain an approved source list for data brokers, people-search sites, public-record aggregators, breach-data sources, and managed removal providers, including coverage, owner, consent basis, cadence, and lawful-use boundary.
- For each affected person, record exposed identifiers such as personal phone numbers, personal emails, home addresses, relatives, property links, employer links, role titles, age, or location signals that could support impersonation, SIM swap preparation, harassment, or account recovery abuse.
- Submit removal, suppression, correction, or delisting requests through approved channels and preserve request date, requester, source response, denial reason, follow-up date, and verification result.
- Use generic service categories such as data broker removal services or managed privacy providers in normative text; keep named vendors only in non-normative internal references where needed.
- If a source cannot remove or suppress the data, record compensating controls such as stronger help desk verification, phishing-resistant authentication, recovery-factor changes, monitoring, or formal residual-risk acceptance.
- Feed recurrence findings into FA5 monitoring records and update FA4 exposure severity when public data reappears or becomes linked to a sensitive workflow.
- Reference cadence: quarterly suppression sweeps; organizations may substitute a documented equivalent cadence.

Evidence core:

- Per-person exposed-identifier list from approved sources with consent basis
- Suppression request log with request date, source response, and verification result
- Compensating-control or residual-risk record where removal fails or exposure recurs

Applicability: from small scale; condition: executives or other high-risk public-profile personnel.

FA4.SC1.C3: Executive Online Presence Cleanup

Reduce executive online presence risk through account inventory, business-use classification, privacy-setting evidence, abandoned-account closure, and impersonation escalation.

Implementation guidance:

- Inventory executive social profiles, public bios, personal websites, old forums, professional directories, public comments, newsletter profiles, public contact pages, and business-used personal accounts.

- Classify each account as official, business-used personal, personal private, dormant, abandoned, impersonating, or investigation pending, and record owner, expected visibility, recovery path, and business use.
- Review profile fields, connection visibility, contact data, birthdays, family details, travel context, hobbies, public photos, public replies, and third-party tags for account recovery, pretexting, or authority-abuse risk.
- Preserve cleanup evidence such as privacy setting screenshots, profile edits, abandoned-account closure, contact-data removal, recovery-factor changes, impersonation report, exception rationale, and retest result.
- Route official public-content standards to FA1.SC3, verification behavior to FA2, account recovery and platform technical controls to FA3, and recurring impersonation monitoring to FA5 or FA4.SC7 as applicable.
- Record residual risk for public figures whose role requires visibility, including approved exposure rationale, compensating controls, and next review date.

Evidence core:

- Executive account inventory with classification, owner, and business use
- Cleanup evidence per account: privacy-setting screenshots, closures, or recovery-factor changes
- Residual-risk record with rationale where role requires public visibility

Applicability: from small scale; condition: executives or other high-risk public-profile personnel.

FA4.SC1.C4: Executive Detail Minimization in Corporate Communications

Control executive personal details in company-controlled communications, media assets, biographies, events, and leadership pages.

Implementation guidance:

- Define approved executive biography and public-detail standards for leadership pages, press releases, investor materials, annual reports, event profiles, podcasts, webinars, social posts, and media kits.
- Review company-controlled materials for unnecessary home city, family status, precise age indicators, school or graduation year, routines, personal contact paths, travel patterns, hobbies, assistants, private affiliations, or location-specific anecdotes.
- Require media asset checks for metadata, background identifiers, visible documents, facility cues, location cues, calendar details, badge information, device screens, and other visual artifacts before publication.
- Preserve publication checklist, communications owner, approved detail standard, exception rationale, metadata verification, image or transcript review, approval date, and post-publication verification.
- Route general publication workflow, public website governance, and media sanitization to FA1 while FA4 retains the executive exposure rationale and exception evidence.

- Trigger review after executive changes, public incidents, major events, crisis communications, board changes, M&A activity, or public exposure findings involving leadership.

Evidence core:

- Pre-publication review record per material with communications owner and approval date
- Metadata and visual-artifact check evidence for executive media assets
- Exception rationale and post-publication verification for retained details

Applicability: from small scale; condition: executives or other high-risk public-profile personnel.

FA4.SC1.C5: Family and Household Exposure Governance

Govern family-adjacent and household exposure only where it can become organizational leverage, fraud, account recovery abuse, coercion, incident-response pressure, or business-continuity risk.

Implementation guidance:

- Define a consent-based review boundary for household contact paths, family associations, public directories, home addresses, shared phone numbers, public photos, school or community listings, delivery records, and reachable devices connected to executive risk.
- Record why the exposure is organization-relevant, such as extortion pressure, doxing, executive impersonation, emergency escalation abuse, SIM swap preparation, account recovery questions, business continuity disruption, or incident-response pressure.
- Preserve source evidence, affected person category, consent or approval basis, exposure type, affected business workflow, remediation request, verification result, and residual-risk decision.
- Use minimization, suppression, alternative contact channels, private mailing arrangements, stronger identity proofing, executive support procedures, and recurrence monitoring as treatment options where appropriate.
- Route family device monitoring, school-directory operations, residential security design, and general personal safety advice to executive-protection extensions or non-normative guidance unless they produce an ODSF evidence/remediation artifact tied to organizational risk.
- Coordinate confirmed household targeting or coercion concerns with FA4.SC3 incident response and FA5 evidence, legal/privacy, communications, and board-reporting records.
- Household-member identifiers require that member's own documented consent; consent on an adult family member's behalf is out of scope.

Evidence core:

- Documented consent record from each reviewed household member
- Exposure finding with organization-relevant abuse path and source evidence

- Remediation request with verification result or residual-risk decision

Applicability: from mid scale; condition: household members of protected executives.

FA4.SC2: Secure Executive Communications and Devices

Objective. Govern executive accounts, telecom dependencies, devices, secure channels, BYOD bridges, and testing where compromise or recovery abuse can weaken organizational authority, access, or incident-response assumptions.

FA4.SC2.C1: Executive Account and Recovery Hardening

Protect executive corporate and business-relevant personal accounts from account recovery abuse, credential misuse, delegated-access abuse, and impersonation.

Implementation guidance:

- Inventory executive accounts that can affect business authority, communications, approvals, public statements, incident response, or account recovery, including corporate email, personal email used for business, collaboration accounts, public social accounts, cloud accounts, delegated-access relationships, and third-party OAuth or app-consent grants attached to executive accounts.
- Require phishing-resistant MFA where the platform supports it, naming passkeys (FIDO2/WebAuthn) as the preferred class (NIST SP 800-63B-4; FA2.SC3.C3), with verified identity proofing before authenticator enrollment or reset, strong recovery-factor governance, recovery email and phone review, login and forwarding alerts, delegated-access records, session review, and unusual login escalation for high-risk accounts.
- Record account owner, business use, recovery factors, delegated users, privileged roles, monitoring source, exception owner, and last review date.
- Replace shared passwords with auditable delegation, role accounts, approved assistant workflows, or other access methods that preserve accountability and revocation evidence.
- Route identity-provider architecture, mail-system configuration, password management, conditional access, and platform technical controls to FA3 or the identity owner while FA4 retains executive exposure and authority-risk evidence.
- Preserve remediation records for recovery-factor changes, revoked sessions, revoked OAuth or app-consent grants, delegated-access corrections, unauthorized forwarding removal, account recovery tests, and residual-risk acceptance.
- Distinguish authority by account class: corporate accounts carry required postures; personal accounts operate under documented agreement with the executive, recorded in the FA4.SC1.C1 scope.

Evidence core:

- Executive account inventory with recovery factors and delegated or app-consent grants
- Phishing-resistant MFA enrollment evidence, with documented executive agreement for personal accounts

- Remediation records for recovery-factor changes, revoked grants, and residual-risk acceptance

Applicability: from micro scale; condition: executives or other high-risk public-profile personnel.

Related controls: FA2.SC3.C3 · FA4.SC1.C1.

FA4.SC2.C2: Executive Telecom and Mobile Number Protection

Govern executive phone numbers, SIM swap exposure, mobile-account recovery paths, and telecom dependencies that can support account takeover or business impersonation.

Implementation guidance:

- Inventory personal and business phone numbers used by executives for MFA, account recovery, vendor escalation, payment approval, emergency communications, public contact, assistant routing, or customer-facing workflows.
- Assess whether each number is discoverable through public records, data brokers, breach data, social media, business directories, resumes, contact-sync leaks, or third-party publications.
- Apply approved controls such as carrier account PINs, port-out locks or freezes where available, number-use restrictions, enterprise-managed numbers for business workflows, removal of SMS recovery for privileged accounts, and stronger help desk verification.
- Record number owner, use case, public exposure source, carrier protection evidence, recovery dependency, replacement path, exception rationale, retest, and residual-risk decision.
- Route mobile device management, endpoint security, telephony platform administration, cloud account configuration, and general device hardening to FA3 while FA4 retains telecom exposure and executive account-recovery risk.
- Use SIM swap attempts, unexpected service loss, number re-exposure, or related phishing attempts to trigger FA4.SC3 response and FA5 monitoring/evidence records.

Evidence core:

- Executive phone-number inventory with use case and recovery dependency
- Carrier protection evidence: account PIN, port-out lock, or SMS-recovery removal
- Exception rationale, retest, or residual-risk decision per unprotected number

Applicability: from micro scale; condition: executives or other high-risk public-profile personnel.

FA4.SC2.C3: Sensitive Executive Communication Channels

Define approved channels and evidence requirements for sensitive executive discussions, instructions, board matters, M&A, legal matters, and incident communications.

Implementation guidance:

- Maintain an approved channel inventory for executive instructions, board communication, legal and financial discussions, M&A, incident response, customer commitments, and external advisor communications.
- Define channel criteria such as authentication, participant verification, audit trail, access owner, retention rule, attachment handling, fallback path, and emergency override handling.
- Require evidence for sensitive requests, including channel used, participant verification, meeting or message source, approval owner, exception, fallback contact, and closure decision.
- Route general out-of-band verification rules to FA2.SC2 and collaboration-platform configuration, encryption settings, meeting controls, and retention implementation to FA3 or the platform owner.
- Prohibit unsanctioned personal or consumer channels for sensitive business workflows unless an approved exception records owner, duration, business need, compensating controls, and retirement date.
- Review channel rules after executive travel, incidents, synthetic-media attempts, board changes, M&A activity, platform changes, or communication outages.

Evidence core:

- Approved channel inventory for sensitive executive workflows with access owner
- Per-request evidence: channel used, participant verification, approval owner
- Exception record for unsanctioned channels with compensating controls and retirement date

Applicability: from small scale; condition: executives or other high-risk public-profile personnel.

FA4.SC2.C4: Executive BYOD and Personal-Work Bridge Governance

Control executive personal devices and accounts that bridge personal life and corporate data, access, communications, or approval workflows.

Implementation guidance:

- Identify executive personal devices, home devices, personal accounts, browsers, messaging tools, cloud storage, printers, and remote environments used to access corporate data or conduct business workflows.
- Record consent boundary, enrolled or unenrolled status, data categories, access path, business justification, compensating controls, monitoring boundary, support owner, and revocation criteria.
- Require managed containers, approved apps, remote-access scope limits, device posture checks, backup controls, account recovery review, and offboarding or revocation procedures where personal devices access corporate resources.
- Preserve enrollment evidence, exception approvals, support records, remote wipe or data removal authority, access reviews, incident handoffs, and residual-risk decisions.

- Route MDM configuration, endpoint security, VPN or ZTNA setup, browser separation, home network hardening, and cloud security controls to FA3 while FA4 retains executive-specific bridge risk and consent evidence.
- Review bridges after role changes, device loss, executive departure, family or household targeting, high-risk travel, incident response, and public exposure findings.

Evidence core:

- Personal-device and bridge inventory with consent boundary and access path
- Enrollment, compensating-control, or exception evidence per bridge
- Revocation or offboarding record with data-removal authority and residual-risk decision

Applicability: from small scale; condition: executives or other high-risk public-profile personnel.

FA4.SC2.C5: Executive Exposure Testing and Coaching

Include executives in authorized exposure-driven testing and private coaching that validates protection of authority, communications, and recovery workflows.

Implementation guidance:

- Define testing scope, authorization, privacy and ethics boundaries, scenario source, affected executives, support staff, communication channels, data handling, and stop conditions before executive testing begins.
- Use scenarios tied to public exposure, such as payment approval pressure, assistant pretexts, executive impersonation, SIM swap recovery abuse, deepfake instructions, public event lures, or doxing response.
- Record scenario, participants, public-source cues used, expected verification behavior, actual response, coaching provided, remediation owner, retest date, and residual-risk decision.
- Provide private feedback that supports behavior change and compensating controls without creating blame records unrelated to security governance.
- Route enterprise drill governance and metrics to FA5, social-engineering scenario content to FA2, and technical test remediation to FA3 while FA4 retains executive-specific exposure and coaching evidence.
- Use repeated failures or new exposure findings to update executive channel rules, account recovery protections, assistant procedures, and board/auditor reporting language.

Evidence core:

- Pre-test authorization record with scope, ethics boundaries, and stop conditions
- Scenario result record: expected versus actual response, coaching provided
- Remediation owner with retest date or residual-risk decision per failure

Applicability: from mid scale; condition: executives or other high-risk public-profile personnel.

FA4.SC3: Threat Monitoring and Incident Response for Executives

Objective. Respond to executive-targeted exposure, impersonation, doxing, harassment, coercion, account compromise, and authority-abuse scenarios with evidence, escalation, remediation, and residual-risk records.

FA4.SC3.C1: Executive Threat Signal Intake

Collect and triage executive-targeted threat signals through approved sources, consent boundaries, severity criteria, and remediation records.

Implementation guidance:

- Define monitored executive identifiers such as names, aliases, personal emails, business emails, phone numbers, images, public handles, domains, high-risk family or household identifiers where authorized, and role-based authority terms.
- Maintain source categories, collection method, lawful basis or approval, platform terms, retention period, alert destination, triage SLA, and false-positive handling for executive monitoring.
- Record alert source, timestamp, match confidence, source artifact, exposed condition, affected executive or workflow, severity, triage owner, action taken, and closure result.
- Route recurring monitoring program governance, lawful collection rules, and evidence vault records to FA5 while FA4 retains executive-specific context, consent, severity, and treatment evidence.
- Route credential rotation, account containment, device response, and technical remediation to FA3, and route employee-facing warnings or social-engineering procedures to FA2.
- Use confirmed signals to update executive exposure audits, data broker suppression, communication channel rules, doxing response plans, and board/auditor summaries.

Evidence core:

- Monitored-identifier list per executive with lawful basis or consent approval
- Triage record per alert with source artifact, severity, owner, and timestamp
- Action and closure result per confirmed signal

Applicability: from mid scale; condition: executives or other high-risk public-profile personnel.

FA4.SC3.C2: Executive Impersonation and Fraud Triage

Triage executive impersonation, fake profiles, fraudulent instructions, and authority-abuse attempts with source evidence and response ownership.

Implementation guidance:

- Capture fake profiles, spoofed messages, fake executive domains, fraudulent payment requests, customer or investor scams, malicious job or vendor outreach, synthetic content, and unauthorized use of executive identity.

- Record claimed identity, source platform, URL or artifact, requested action, affected audience, public information referenced, business process targeted, verification result, and severity.
- Define response paths for platform reports, domain or registrar action, employee/customer warning, payment hold, law-enforcement referral, legal review, and public correction where appropriate.
- Route broad brand/domain monitoring to FA5 and technical domain controls to FA3; FA4 owns executive identity context, authority-abuse risk, and executive-specific remediation evidence.
- Route employee reporting, verification behavior, and fraudulent request handling to FA2 while preserving the FA4 impersonation case record.
- Update official-channel registries, executive bios, communication rules, and assistant procedures after confirmed impersonation or fraud attempts.

Evidence core:

- Impersonation case record with source artifact, claimed identity, and targeted process
- Response action evidence: platform report, takedown, warning, or payment hold
- Closure result with registry or procedure updates after confirmed incidents

Applicability: from small scale; condition: executives or other high-risk public-profile personnel.

FA4.SC3.C3: Doxing, Harassment, and Coercion Response

Respond to exposed executive personal information, harassment, threats, or coercion with severity criteria, evidence preservation, safety escalation, and residual-risk follow-up.

Implementation guidance:

- Define triggers for doxing, household contact exposure, family-adjacent targeting, threats, harassment, coercive extortion, unwanted public attention, swatting risk, or publication of private contact channels.
- Preserve evidence such as URLs, screenshots, timestamps, account identifiers, message headers, call logs, platform reports, public-source origin, threat language, and affected workflow or business event.
- Record severity, legal/privacy review, HR or people-support owner, communications owner, physical security or safety escalation, law-enforcement threshold, platform request, and closure decision.
- Coordinate removal, suppression, account hardening, temporary communication changes, employee warnings, executive support, and residual-risk decisions through approved response owners.
- Route enterprise communications, evidence vault, notification analysis, and board/auditor records to FA5 while FA4 retains executive harm, leverage, and exposure-remediation context.

- Use after-action findings to update data broker suppression, household exposure governance, public appearance controls, and incident simulations.

Evidence core:

- Preserved source evidence with URLs, timestamps, and affected workflow
- Severity and escalation record with response owners and law-enforcement threshold
- Closure decision with removal, hardening, or residual-risk follow-up actions

Applicability: from small scale; condition: executives or other high-risk public-profile personnel.

FA4.SC3.C4: Executive Incident Simulations and Drills

Exercise executive-targeted scenarios with role rosters, decision logs, after-action records, remediation ownership, and retest cadence.

Implementation guidance:

- Run scenarios such as executive email compromise, synthetic executive instructions, public doxing, household contact targeting, fake press statements, payment diversion, travel exposure, event disruption, or executive device loss.
- Define exercise scope, participants, scenario source, legal/privacy boundary, decision authority, evidence to produce, expected communication approvals, and stop conditions.
- Record timeline, decisions, failed assumptions, missing contacts, executive availability assumptions, containment choices, public messaging decisions, and business-continuity impacts.
- Assign after-action items with owner, due date, affected control, remediation evidence, retest requirement, and residual-risk decision.
- Route enterprise exercise governance and reporting to FA5 while FA4 preserves executive scenario content and exposure-specific improvement evidence.
- Use exercises to validate assistant procedures, temporary authority delegation, emergency communication channels, takedown paths, law-enforcement contact paths, and board/customer communication thresholds.
- Reference cadence: annual exercises; organizations may substitute a documented equivalent cadence.

Evidence core:

- Exercise record with scenario, participants, decision timeline, and failed assumptions
- After-action items with owner, due date, and affected control
- Retest or residual-risk evidence per after-action item

Applicability: from mid scale; condition: executives or other high-risk public-profile personnel.

FA4.SC3.C5: Executive Recovery and Continuity Plan

Prepare recovery and continuity steps for executive account, device, identity, communication, and public-trust incidents.

Implementation guidance:

- Define recovery authority for executive account compromise, device loss, unauthorized public statements, impersonation, doxing, household targeting, and temporary executive unavailability.
- Maintain steps for account containment, session revocation, credential and recovery-factor reset, delegated access change, device isolation, public correction, internal verification notice, and customer or partner clarification where needed.
- Define temporary approval delegation, alternate spokespersons, emergency communication channels, board contact paths, advisor access, and business-continuity thresholds when an executive cannot safely act.
- Record incident source, recovery owner, action timestamps, legal or law-enforcement records, communication approvals, systems restored, residual-risk items, and post-incident review.
- Route technical containment and recovery implementation to FA3, social-engineering warnings to FA2, and enterprise crisis communication/evidence governance to FA5.
- Retest recovery procedures after incidents, exercises, executive transitions, channel changes, and material public-exposure findings.

Evidence core:

- Recovery and delegation procedure with named recovery authority
- Activation or retest record with action timestamps and systems restored
- Post-incident or post-test review with residual-risk items

Applicability: from small scale; condition: executives or other high-risk public-profile personnel.

FA4.SC4: Executive Authority and Support Safeguards

Objective. Govern executive authority, assistant workflows, official identity, public instructions, and public-engagement boundaries where public exposure can enable fraud, impersonation, or control bypass.

FA4.SC4.C1: Executive Exposure Coaching

Provide executive-specific coaching tied to public exposure, authority abuse, account recovery, deepfake risk, and incident-response expectations.

Implementation guidance:

- Define coaching modules for executives and board-facing personnel based on role authority, public profile, approval power, media exposure, account recovery dependencies, public events, and family-adjacent exposure where organization-relevant.
- Use sanitized findings to show how public data can weaken verification, payment approval, help desk recovery, public communications, or incident-response assumptions.
- Record audience, module, public exposure examples, learning objective, completion evidence, exception path, refresher trigger, and follow-up coaching need.
- Route enterprise training governance and completion metrics to FA5, broad social-engineering training to FA2, and detailed technical controls to FA3 while FA4 retains executive coaching evidence.
- Update coaching after incidents, public appearances, executive transitions, major media exposure, synthetic-media developments, or exposure audit findings.

Evidence core:

- Coaching completion record per executive with module and exposure examples used
- Refresher trigger or follow-up record with exception path where coaching lapses

Applicability: from small scale; condition: executives or other high-risk public-profile personnel.

FA4.SC4.C2: Executive Authority and Instruction Boundaries

Define how executives issue critical instructions and how staff verify authority when public exposure or synthetic media can create false trust.

Implementation guidance:

- Define critical instruction classes such as payments, vendor changes, HR actions, public statements, legal approvals, privileged access, incident commands, customer commitments, and exception approvals.
- For each class, record permitted channel, required verifier, second approver threshold, emergency fallback, assistant role, travel or outage exception, and evidence artifact.
- Require staff to verify executive instructions through approved records or independent channels when urgency, secrecy, public context, voice/video media, or unusual requested action increases risk.
- Route general verification behavior and request-class rules to FA2.SC2 while FA4 records executive authority limits, assistant workflow dependencies, and exposure-driven exception evidence.
- Review boundaries after executive role changes, travel, M&A activity, public incidents, deepfake attempts, or audit findings that show authority paths are discoverable.

Evidence core:

- Per-class instruction rules with permitted channel, verifier, and evidence artifact
- Verification or exception record per critical instruction with approver and date

Applicability: from micro scale; condition: executives or other high-risk public-profile personnel.

FA4.SC4.C3: Official Executive Identity Registry

Maintain authoritative records of official executive channels, public profiles, reserved handles, and verification references.

Implementation guidance:

- Inventory official executive domains, social profiles, public contact paths, media pages, investor relations references, board communication channels, assistant contacts, and reserved handles.
- Record owner, platform, purpose, expected visibility, recovery path, renewal or review date, verification marker, inactive account handling, and takedown contact path.
- Publish official-channel references where doing so reduces fraud and confusion, while applying FA1 minimization rules to avoid unnecessary personal detail exposure.
- Route recurring monitoring for fake profiles, lookalike domains, and unauthorized channel use to FA5 or FA4.SC7; route technical domain controls and renewals to FA3.
- Preserve takedown requests, platform responses, account recovery changes, reserved-handle records, residual-risk decisions, and public correction evidence.

Evidence core:

- Official executive channel registry with owner, recovery path, and verification status
- Dated registry review with renewal or retirement decisions
- Takedown request and platform response evidence for unauthorized channels

Applicability: from small scale; condition: executives or other high-risk public-profile personnel.

FA4.SC4.C4: Executive Assistants and Support Staff Process Controls

Protect executive assistants and support staff from public-source pretexts that exploit access, scheduling, communication, and delegated authority.

Implementation guidance:

- Maintain a roster of assistants, chiefs of staff, executive support, travel coordinators, communications staff, board liaisons, and other personnel who can affect executive access or authority.
- Define request classes, verification steps, escalation paths, delegation authority, travel and calendar disclosure limits, unusual-request criteria, and override approval for support workflows.
- Train support personnel on pretexts that use public events, family references, vendor names, travel context, press cycles, board meetings, or personal contact data to create false urgency.

- Record request source, claimed identity, public information referenced, verification result, escalation owner, action taken, exception, and closure evidence for unusual or sensitive support requests.
- Route broad social-engineering training and reporting to FA2 while FA4 owns executive-support workflow risk and assistant-specific evidence.
- Use incidents and drills to update assistant scripts, verified directories, calendar-sharing rules, public contact exposure, and temporary authority procedures.

Evidence core:

- Support-staff roster with delegation authority and verification procedures
- Unusual-request record with claimed identity, verification result, and escalation owner
- Training or drill evidence for support personnel on public-source pretexts

Applicability: from small scale; condition: executives supported by assistants or dedicated support staff.

FA4.SC5: Executive Location Exposure Management

Objective. Reduce exposure of executive addresses, location metadata, routines, travel context, public appearances, and residential technology signals where those exposures can support coercion, targeting, account recovery abuse, or business disruption.

FA4.SC5.C1: Address and Residential Exposure Governance

Reduce public exposure of executive home addresses, mailing paths, property links, and residential contact points where they create organizational leverage or account recovery risk.

Implementation guidance:

- Inventory home address sources, property records, voter or licensing records, corporate filings, court records, data brokers, delivery records, public photos, shared household identifiers, and mailing addresses where legally and ethically reviewable.
- Record source, jurisdiction, legal constraint, exposed identifier, affected executive, organizational abuse path, remediation option, legal/privacy review, and residual-risk decision.
- Use appropriate address alternatives such as business mailing addresses, private mailbox services, registered-agent paths, suppression requests, or other legally reviewed arrangements where they reduce public exposure.
- Preserve request records, provider responses, verification results, denied-request rationale, compensating controls, and recurrence monitoring.
- Route generic residential security operations to executive-protection extensions; FA4 core keeps public-exposure, evidence, and remediation records tied to organizational risk.
- Escalate doxing, threats, coercion, or household contact targeting to FA4.SC3 and FA5 incident/evidence governance.

- Operate within the authorized scope, consent, and excluded-areas record FA4.SC1.C1 establishes before collecting in this domain.

Evidence core:

- Collection authorization under the FA4.SC1.C1 scope and consent record
- Address exposure findings with source, jurisdiction, and abuse path
- Suppression or alternative-address evidence with provider response and residual-risk decision

Applicability: from small scale; condition: executives or other high-risk public-profile personnel.

Related controls: FA4.SC1.C1.

FA4.SC5.C2: Travel and Routine Exposure Controls

Control public travel, commute, and routine disclosures that can create executive targeting, fraud, coercion, or incident-response risk.

Implementation guidance:

- Identify travel and routine exposures from public calendars, event pages, flight or venue posts, assistant communications, social media, vendor materials, hotel or transport records, public photos, and recurring schedule disclosures.
- Monitor registration-based movement tracking for organization-linked aircraft and vessels, such as public tail-number and transponder trackers, and enroll eligible aircraft in registry privacy and blocking programs, recording verification evidence.
- Define rules for pre-announcement timing, calendar sharing, assistant disclosures, travel contact paths, public attendee lists, social posts, and high-risk travel communications.
- Record travel exposure source, affected event or route, business need, approved audience, risk rationale, mitigation, exception owner, and review date.
- Use delayed posting, minimized location detail, controlled contact paths, approved travel aliases where lawful, temporary communication procedures, and post-event review as treatment options.
- Route secure travel equipment, endpoint preparation, remote-access technical controls, and network hardening to FA3; route crisis escalation and temporary communications governance to FA5.
- Trigger review after travel-related phishing, event disruption, unwanted contact, public controversy, high-risk geography, or executive exposure findings.
- Operate within the authorized scope, consent, and excluded-areas record FA4.SC1.C1 establishes before collecting in this domain.

Evidence core:

- Collection authorization under the FA4.SC1.C1 scope and consent record
- Travel exposure findings with source, affected event, and risk rationale

- Mitigation or exception record with owner and review date

Applicability: from mid scale; condition: executives or other high-risk public-profile personnel.

Related controls: FA4.SC1.C1.

FA4.SC5.C3: Location Metadata and Visual Cue Controls

Reduce location disclosure through metadata, background artifacts, visual cues, check-ins, and public media involving executives.

Implementation guidance:

- Review executive photos, videos, livestreams, podcasts, document shares, social posts, calendar screenshots, public interviews, and event media for location metadata and visual cues.
- Control geotags, EXIF data, background landmarks, home or office interiors, device screens, badges, documents, street views, routines, and live-location features before publication or sharing.
- Preserve review checklist, media owner, metadata verification, visual cue finding, remediation action, exception rationale, approval, and post-publication verification.
- Route media sanitization tooling and publication review to FA1.SC5 and FA1.SC3; FA4 retains executive location risk and residual-risk rationale.
- Update executive coaching, event briefing, and communication standards when media exposure reveals location, routine, household, or travel patterns.

Evidence core:

- Pre-publication media review record with metadata verification and visual-cue findings
- Remediation or exception record per finding with post-publication verification

Applicability: from small scale; condition: executives or other high-risk public-profile personnel.

FA4.SC5.C4: Residential Technology Exposure Handoff

Identify home IoT, smart-device, and residential technology signals that create executive location, occupancy, account recovery, or corporate-access risk, then route durable technical remediation to the right owner.

Implementation guidance:

- Assess residential technology only where it creates organization-relevant exposure, such as public cameras, smart-doorbell sharing, voice assistant leakage, smart-home account takeover risk, occupancy signals, shared networks used for corporate access, or devices linked to executive identity.
- Record device or service category, exposure signal, public source, account owner, business dependency, corporate access relationship, consent boundary, remediation owner, and residual-risk decision.

- Use treatment options such as account recovery review, public sharing reduction, device visibility reduction, network separation, corporate-access limits, and monitoring for public exposure where appropriate.
- Route device configuration, network segmentation, endpoint security, cloud account hardening, and vulnerability remediation to FA3 or the designated technical owner.
- Route family device monitoring, household operations, and personal safety procedures to executive-protection extensions unless they produce ODSF evidence tied to fraud, coercion, account recovery, or business continuity.
- Escalate confirmed residential technology abuse, location leakage, or coercion attempts to FA4.SC3 and FA5 incident/evidence governance.

Evidence core:

- Residential exposure finding with device category, public source, and consent boundary
- Handoff record to the technical owner with remediation ownership
- Residual-risk decision or escalation record for confirmed abuse

Applicability: from mid scale; condition: residential technology linked to protected executives.

FA4.SC5.C5: Public Engagement and Appearance Exposure Management

Govern executive public engagements and appearances, including pre-event exposure briefing, so event details, media, recordings, and attendee interactions do not create avoidable exposure or incident-response pressure.

Implementation guidance:

- Review planned engagements and appearances for announcement timing, location specificity, published agenda, attendee access and lists, media access and rules, recording policy, photography boundaries, public Q&A, badge display, travel cues, staff contact exposure, and personal-detail disclosure risks.
- Define the pre-event briefing: approved topics and disclosure boundaries, prohibited personal details, sensitive business boundaries, support staff roles, assistant or communications contact, emergency contacts, incident triggers, evidence preservation, post-event monitoring criteria, and escalation path for unexpected questions or targeting.
- Record event owner, briefing record, public materials reviewed, approved disclosures, exception rationale, monitoring triggers, incidents, takedown requests, and post-event remediation, cleanup, correction, or residual-risk decisions.
- Route public-content approval and media sanitization to FA1, social-engineering training and suspicious-contact reporting to FA2, and recurring monitoring or crisis-communications governance to FA5.
- Update exposure audits, executive coaching, executive biographies, travel disclosure rules, assistant procedures, social media guidance, image and likeness controls, and public appearance rules after major events, hostile attention, impersonation attempts, or new public media artifacts.

Evidence core:

- Pre-event briefing record with approved disclosures and escalation path
- Event exposure review covering public materials, recording rules, and attendee access
- Post-event record with incidents, takedowns, cleanup, or residual-risk decisions

Applicability: from mid scale; condition: executives or other high-risk public-profile personnel.

FA4.SC5.C6: Calendar and Scheduling Exposure Governance

Govern calendar visibility, free/busy sharing, scheduling-link exposure, and meeting-detail disclosure where they reveal executive routines, relationships, or business context.

Implementation guidance:

- Inventory calendar surfaces that expose executive context, including tenant default calendar sharing and free/busy visibility, delegated calendar access, published booking or scheduling links, embedded availability widgets, shared meeting links, and assistant-managed scheduling workflows.
- Set tenant and account defaults so calendar detail, free/busy state, and meeting subjects are not visible beyond approved audiences; review external-sharing settings, federation defaults, and conference-room or resource calendars that leak attendee or location detail.
- Govern booking and scheduling links: record owner, audience, exposure rationale, and whether the link reveals availability patterns, meeting titles, attendee names, or locations; replace open-ended public links with audience-limited or expiring links where the business purpose allows.
- Treat exposed availability as targeting data: free/busy patterns reveal travel, routines, meeting cadence, and likely response windows that support impersonation timing, pretext credibility, and physical targeting; record that abuse path in exposure findings.
- Record surface, owner, sharing state, approved audience, mitigation, exception rationale, review cadence, and residual-risk decision; trigger review after assistant changes, platform migrations, travel-pattern incidents, or new exposure findings.
- Route tenant configuration and collaboration-platform hardening to FA3 or the platform owner, and org-wide calendar minimization to FA1.SC2.C1; FA4 retains executive-specific exposure rationale and evidence.

Evidence core:

- Calendar surface inventory with owner, sharing state, and approved audience
- Tenant default and scheduling-link configuration evidence
- Exception rationale or residual-risk decision per exposed surface

Applicability: from small scale; condition: executives or other high-risk public-profile personnel.

Related controls: FA1.SC2.C1.

FA4.SC6: Executive Financial Authority Exposure

Objective. Govern public financial, ownership, payment, and advisor-context exposure where it can enable BEC, payment diversion, account recovery abuse, coercion, or executive authority fraud.

FA4.SC6.C1: Financial Authority Abuse Controls

Protect executive financial authority and payment approval paths from public-source impersonation, coercion, account recovery abuse, and business email compromise.

Implementation guidance:

- Identify executives and delegates who can approve payments, investments, vendor changes, payroll actions, wire transfers, banking changes, customer credits, or emergency finance actions.
- Record approval thresholds, channel rules, verification requirements, backup approvers, public authority cues, assistant involvement, exception path, and evidence artifact for high-risk financial actions.
- Review whether public financial context, wealth indicators, board roles, investment activity, charitable affiliations, business registrations, or family associations could support payment diversion or coercion.
- Require transaction holds, second approver review, verified callback paths, or finance workflow evidence for unusual executive financial instructions.
- Route general payment workflow controls and social-engineering verification to FA2, financial-system access controls to FA3, and evidence/reporting governance to FA5 while FA4 retains executive authority exposure records.
- Preserve incident, drill, or exception records showing requested action, claimed authority, verification result, decision owner, remediation, and residual-risk decision.

Evidence core:

- Financial-authority roster with approval thresholds and verification requirements
- Verification evidence per unusual instruction: hold, callback, or second approval
- Incident, drill, or exception record with decision owner and residual-risk decision

Applicability: from small scale; condition: executives or other high-risk public-profile personnel.

FA4.SC6.C2: Public Financial and Ownership Record Exposure

Review public financial, ownership, filing, and registration records for executive-linked exposure that can support coercion, impersonation, fraud, or account recovery abuse.

Implementation guidance:

- Inventory public financial and ownership sources such as business registrations, licensing records, property records, political or charitable filings, litigation records, public compensation context, investment disclosures, and beneficial ownership references where legally reviewable.
- Record source, jurisdiction, exposed data element, linked executive, business relevance, abuse path, legal constraint, remediation option, and residual-risk decision.
- Use lawful minimization, correction, alternative mailing addresses, registered-agent paths, suppression requests, or compensating controls where exposure is unnecessary or can be reduced.
- Document when records must remain public and define compensating controls such as strengthened verification, limited public detail elsewhere, monitoring, and response playbooks.
- Route broad privacy compliance, legal interpretation, and mapping-pack evidence to FA5; FA4 preserves public financial exposure and executive authority risk evidence.
- Review after executive role changes, new entities, acquisitions, divestitures, public controversies, financing events, or exposure findings.

Evidence core:

- Public-record exposure findings with source, jurisdiction, and abuse path
- Minimization or correction request evidence with outcomes
- Compensating-control record where records must remain public

Applicability: from mid scale; condition: executives or other high-risk public-profile personnel.

FA4.SC6.C3: Financial Correspondence and Advisor Verification

Control executive financial correspondence, advisor interactions, and document exchange where public context can enable fraud or unauthorized disclosure.

Implementation guidance:

- Inventory financial advisors, banks, accountants, attorneys, family office contacts, board finance contacts, payment processors, and internal finance staff who may receive executive-linked requests.
- Define approved channels, identity verification, document exchange rules, escalation thresholds, callback sources, retention limits, and exception handling for sensitive financial correspondence.
- Record request source, claimed identity, public context referenced, verification path, documents exchanged, approval owner, exception, and closure evidence for unusual or sensitive requests.
- Use secure document exchange, redaction, approved contact directories, transaction holds, and second-person approval for sensitive financial communications where public exposure creates plausible pretexts.

- Route general secure-channel architecture and platform configuration to FA3, social-engineering verification behavior to FA2, and evidence retention to FA5 while FA4 keeps executive financial-context risk.
- Update procedures after BEC attempts, advisor impersonation, public financial-record exposure, executive travel, or major transactions.
- Operate within the authorized scope, consent, and excluded-areas record FA4.SC1.C1 establishes before collecting in this domain.

Evidence core:

- Collection authorization under the FA4.SC1.C1 scope and consent record
- Advisor and contact directory with approved channels and callback sources
- Verification record per unusual request with claimed identity and closure evidence

Applicability: from mid scale; condition: executives or other high-risk public-profile personnel.

Related controls: FA4.SC1.C1.

FA4.SC6.C4: Digital Payment and Subscription Exposure Review

Review public digital payment handles, subscriptions, receipts, personal commerce artifacts, and financial app exposure only where they can affect organizational fraud, authority, coercion, or account recovery risk.

Implementation guidance:

- Identify public payment handles, donation pages, storefronts, subscriptions, receipts, personal commerce profiles, app usernames, phone-number links, or transaction references that connect executives to business authority or sensitive personal identifiers.
- Assess whether the exposure supports impersonation, payment diversion, account recovery, SIM swap preparation, coercion, public controversy, or fraudulent vendor/customer contact.
- Record source, affected account or handle, linked identifier, business relevance, remediation action, verification result, and residual-risk decision.
- Use minimization, privacy settings, contact separation, public handle changes, removal requests, or stronger account recovery controls as treatment options where the exposure is relevant to ODSF risk.
- Route generic personal banking hygiene, browser privacy, and consumer payment advice to non-normative executive-protection guidance; FA4 core keeps exposure that affects organizational control confidence.
- Feed confirmed payment impersonation or coercion findings into FA2 verification procedures, FA4.SC3 response records, and FA5 monitoring/evidence governance.
- Operate within the authorized scope, consent, and excluded-areas record FA4.SC1.C1 establishes before collecting in this domain.

Evidence core:

- Collection authorization under the FA4.SC1.C1 scope and consent record
- Payment-exposure findings with linked identifier and business relevance
- Remediation action with verification result or residual-risk decision

Applicability: from mid scale; condition: executives or other high-risk public-profile personnel.

Related controls: FA4.SC1.C1.

FA4.SC7: Executive Disinformation and Likeness Protection

Objective. Govern executive identity, likeness, official-channel, deepfake, and disinformation exposure where public manipulation can harm trust, fraud prevention, incident response, investor confidence, or customer communications.

FA4.SC7.C1: Executive Identity and Likeness Monitoring

Monitor unauthorized executive identity, image, voice, quote, and likeness use through approved sources, provenance checks, triage criteria, and remediation records.

Implementation guidance:

- Define monitored identifiers such as executive names, images, headshots, voice samples, public quotes, videos, social handles, official titles, domains, and high-risk alternate spellings.
- Maintain source categories, collection method, lawful basis or approval, platform constraints, retention period, alert thresholds, and false-positive handling for identity and likeness monitoring.
- Record source artifact, timestamp, platform, media type, match confidence, suspected manipulation, affected audience, business consequence, triage owner, and action taken.
- Route broad monitoring governance, evidence vault records, and reporting metrics to FA5 while FA4 retains executive context, likeness risk, and treatment evidence.
- Route technical domain controls or platform configuration to FA3 and social-engineering verification updates to FA2 as needed.
- Use confirmed unauthorized identity or likeness use to update official channel registries, communication templates, public corrections, takedown paths, and residual-risk records.

Evidence core:

- Monitored-identifier and source list with lawful basis or approval
- Triage record per alert with source artifact, match confidence, and owner
- Action and closure evidence per confirmed unauthorized use

Applicability: from mid scale; condition: executives or other high-risk public-profile personnel.

FA4.SC7.C2: Official Executive Channel Reservation

Reserve and govern executive social handles, official profiles, and limited executive-name domains where reservation reduces impersonation or public confusion.

Implementation guidance:

- Inventory reserved social handles, official profiles, executive-name domains, common variants, inactive accounts, and platform verification markers with owner, purpose, review date, and renewal or retirement criteria.
- Prioritize channels where executive impersonation could affect customers, investors, vendors, employees, incident communications, recruiting, or fraud prevention.
- Record account owner, credential owner, recovery path, public visibility, verification status, content approval boundary, monitoring path, and exception rationale.
- Route brand-wide domain monitoring, typosquat detection, and registrar governance to FA5 and FA3; FA4 keeps executive-specific reservation rationale and official-channel evidence.
- Avoid speculative bulk registration that creates unnecessary operational burden; document risk basis, protected audience, renewal owner, and residual-risk decision for reserved assets.
- Review channel reservations after executive changes, board changes, public campaigns, impersonation incidents, mergers, product launches, and public controversies.

Evidence core:

- Reserved-handle and domain inventory with owner, risk basis, and renewal date
- Credential and recovery-path record per reserved asset
- Dated reservation review with retirement or residual-risk decisions

Applicability: from small scale; condition: executives or other high-risk public-profile personnel.

FA4.SC7.C3: Executive Disinformation Response Planning

Plan response to false, manipulated, or synthetic executive content with provenance assessment, approval chains, platform action, correction workflow, and notification criteria.

Implementation guidance:

- Define scenarios for fake executive statements, synthetic audio or video, manipulated images, false resignation or financial claims, fake incident updates, investor misinformation, customer-impacting rumors, and harassment-driven narratives.
- Record source, provenance assessment, media type, claimed identity, affected audience, potential business consequence, response owner, legal/privacy review, communications approval, and escalation threshold.
- Maintain correction workflows, platform reporting paths, employee/customer warning templates, spokesperson authority, law-enforcement referral criteria, and board or regulator notification criteria where applicable.

- Coordinate with FA2 deepfake verification procedures, FA5 crisis communications and evidence vaults, and FA3 technical takedown or domain controls as needed.
- Exercise disinformation scenarios and preserve participants, decisions, gaps, corrective actions, retest date, and residual-risk decisions.
- Use confirmed events to update executive media guidance, official-channel registries, likeness monitoring, and public appearance controls.

Evidence core:

- Correction workflow and notification-criteria record with spokesperson authority
- Exercise or incident record with provenance assessment, decisions, and corrective actions
- Retest and residual-risk decision per identified gap

Applicability: from mid scale; condition: executives or other high-risk public-profile personnel.

FA4.SC7.C4: Executive Image Rights and Provenance Governance

Govern approved executive media assets, likeness usage, provenance markers, and takedown/legal handoffs for unauthorized manipulation or reuse.

Implementation guidance:

- Maintain an approved executive media repository with asset owner, source, usage permission, allowed contexts, expiration, provenance marker or watermark decision, and public-distribution history.
- Define release rules for headshots, videos, voice clips, event recordings, investor materials, social clips, podcast media, and generated or edited executive imagery.
- Record approval, publication location, usage terms, metadata review, takedown contact, legal/IP owner, and monitoring trigger for each high-value asset class.
- Preserve evidence for unauthorized use, manipulated media, deepfake training concerns, takedown or legal request, platform response, correction action, and residual-risk decision.
- Route media sanitization and publication workflow to FA1, synthetic-media verification behavior to FA2, and broad incident evidence/reporting to FA5 while FA4 owns executive likeness risk.
- Review image and likeness governance after new campaigns, executive transitions, public incidents, major media appearances, or confirmed manipulation events.

Evidence core:

- Approved media repository with asset owner, usage permission, and expiration
- Release approval and metadata-review record per published asset class
- Takedown or legal-request evidence with platform response and residual-risk decision

Applicability: from large scale; condition: executives or other high-risk public-profile personnel.

Continuous Monitoring and Response

Continuous Monitoring and Response governs how public-exposure signals are collected, triaged, evidenced, remediated, reported, and fed back into the ODSF program. This focus area broadly orients to NIST CSF 2.0 oversight, policy, risk assessment, improvement, continuous monitoring, adverse event analysis, incident response, and recovery communication categories. It turns new exposures, attacker signals, impersonation attempts, breach indicators, canary alerts, and monitoring results into accountable response records and Control Confidence Gap evidence.

Business rationale. Public exposure changes after the initial assessment. New breach data appears, employees and vendors publish new material, platforms change visibility rules, impersonation campaigns emerge, and attackers reuse public information in new ways. FA5 gives the organization a governed intake and response backbone so public-exposure findings become accountable cases with evidence, owners, legal and privacy boundaries, remediation tracking, residual-risk decisions, program metrics, and board/auditor-ready reporting. The business value is defensibility: leadership can show that foreseeable public-exposure attack paths are monitored, evaluated, reduced, compensated, or formally accepted.

Scope. This includes monitoring source governance, lawful collection boundaries, alert triage, false-positive handling, incident-response playbooks, takedown and mitigation workflows, evidence retention, exposure scoring, operational and board reporting, compliance evidence, training cadence, and program improvement. Technical remediation routes to FA3, public-content and data minimization routes to FA1, social-engineering response content routes to FA2, and executive/private-life exposure handling routes to FA4. FA5 owns the governance records that connect those actions into a continuous exposure-governance program.

NIST CSF 2.0 orientation: GV.OV · GV.PO · ID.RA · ID.IM · DE.CM · DE.AE · RS.MA · RS.AN · RS.CO · RS.MI · RC.CO

Focus-area alignment entries are broad orientation metadata indicating thematic overlap with NIST CSF 2.0 categories. They are not conformance mappings, control-level crosswalks, or claims of coverage. Control-level mappings to external standards are published separately as ODSF mapping packs.

FA5.SC1: OSINT Threat Intelligence and Monitoring

Objective. Govern recurring public-exposure monitoring through approved sources, lawful collection boundaries, triage criteria, evidence capture, incident linkage, and closure records.

FA5.SC1.C1: Breach and Credential Exposure Monitoring

Monitor breach, credential, and dark-web exposure through approved sources with lawful handling, triage ownership, and closure evidence.

Implementation guidance:

- Maintain an approved source inventory for breach-notification feeds, credential-exposure services, dark-web monitoring providers, stealer-log and infostealer-marketplace monitoring services, and internal reports; record owner, coverage, collection method, retention period, and lawful-use boundary.
- Define monitored identifiers such as company domains, product names, privileged roles, executive identifiers, support channels, and approved high-risk personal identifiers where consent or another approved basis exists.
- Set triage criteria for credential exposure, stealer-log records (prioritizing entries containing active session tokens or cookies, which bypass MFA), initial-access offers, data-set claims, executive or customer references, and high-confidence matches; include false-positive handling and escalation thresholds.
- Route credential and account findings to identity, access, and incident-response owners, triggering session revocation and credential reset for stealer-exposed accounts (FA2.SC5.C2); route technical leakage to FA3 and executive/private-life exposure to FA4 while preserving the FA5 monitoring record.
- Preserve source reference, timestamp, collection method, screenshot or hash where appropriate, affected role or asset, severity, action owner, remediation action, retest result, residual-risk decision, and closure date.
- Reference cadence where none is defined yet: review breach-notification alerts weekly, triage stealer or marketplace findings within one business day of receipt, and review the approved-source inventory quarterly.

Evidence core:

- Monitored-source or breach-notification subscription list
- Triage record per alert with owner and disposition (one business day for stealer hits)
- Revocation or closure evidence for confirmed exposures

Applicability: from micro scale.

Related controls: FA2.SC5.C2.

FA5.SC1.C2: Public Web, Social, Brand, and Repository Monitoring

Monitor public web, social, paste, repository, brand, and impersonation signals through governed alert criteria and evidence records.

Implementation guidance:

- Maintain monitored terms, domains, handles, product names, project names, public repositories, paste sources, file-sharing indicators, departed-personnel references, acquisition or divestiture terms, subsidiary or brand transitions, and brand-impersonation patterns with an assigned owner and review cadence.

- Document platform terms, privacy constraints, scraping restrictions, collection method, data minimization rule, retention period, and legal-review triggers before automated collection is used.
- Define alert criteria for leaked documents, exposed credentials, sensitive code or snippets, fake profiles, lookalike domains, malicious apps, stale public personnel references, M&A or divestiture footprint drift, public harassment, and unusual brand or executive mentions.
- Route publication cleanup to FA1, technical repository or secret remediation to FA3, social-engineering response to FA2, and executive-specific monitoring to FA4 while retaining a single FA5 intake and closure record.
- Track source quality, match confidence, false-positive disposition, affected business process, action owner, notification decision, remediation evidence, retest result, and residual-risk acceptance.
- Watch certificate-transparency logs and newly registered domain feeds for permutations of organization domains and brands, covering typosquats, combosquats, and homoglyph variants.

Evidence core:

- Monitored terms, domains, and handles list with assigned owner
- Triage record per alert with disposition and routing destination
- Takedown, remediation, or residual-risk evidence per confirmed finding

Applicability: from small scale.

FA5.SC1.C3: External Asset Change Monitoring

Monitor externally visible asset changes as public-exposure signals and route technical remediation to the owning control program.

Implementation guidance:

- Define the monitored asset baseline for domains, subdomains, certificates, public cloud endpoints, exposed storage, public APIs, public repositories, and externally visible service changes.
- Record discovery source, asset owner, approved state, alert threshold, severity rule, and routing path for unapproved assets, configuration drift, exposed interfaces, certificate changes, and public storage changes.
- Treat FA5 as the monitoring and case-management home; route vulnerability validation, configuration hardening, key rotation, secret revocation, and application remediation to FA3.
- Preserve change evidence, asset-owner decision, remediation ticket, exception or risk acceptance, retest result, and closure summary so external-asset drift can support reporting and trend analysis.

Evidence core:

- External-asset baseline with owner and approved state
- Change or drift alert record with routing decision and date
- Remediation ticket, exception, or risk acceptance with closure evidence

Applicability: from small scale.

FA5.SC1.C4: Threat Intelligence Intake and Sharing

Use trusted threat-intelligence sources and sharing communities through documented relevance, handling, and actionability criteria.

Implementation guidance:

- Maintain approved sources such as sector sharing groups, government advisories, law-enforcement notifications, platform abuse notices, brand-protection feeds, domain-watch feeds, vendor intelligence, and peer reports.
- For each source, document owner, subscription scope, handling restrictions, redistribution limits, confidence rating, applicability criteria, and expected action path.
- Translate relevant intelligence into monitored indicators, scenario updates, playbook changes, training updates, or technical-control handoffs; record when intelligence is reviewed and declined as not applicable.
- Use approved information-sharing protocols when contributing indicators or incident details, and sanitize sensitive evidence before sharing outside the organization.
- Preserve source reference, retrieval date, analysis note, affected ODSF areas, decision owner, action taken, and follow-up review date.
- An existing threat-intelligence program satisfies this control by reference; ODSF adds the OSINT-specific sources and routing above.

Evidence core:

- Approved intelligence-source list with owner and handling restrictions
- Dated intake record with action taken or not-applicable decision

Applicability: from mid scale.

FA5.SC1.C5: Logging and Analytics for OSINT Signals

Integrate public-exposure and canary signal data with security monitoring tools through governed log sources, alert rules, and response records.

Implementation guidance:

- Define a signal taxonomy for breach indicators, public-source scraper behavior, suspicious support requests, impersonation reports, governed canary or honeytoken alerts, and personalized phishing patterns.

- Record the log source, owner, lawful collection boundary, jurisdiction or platform constraint, retention period, correlation rule, alert destination, and triage SLA before routing OSINT signals into SIEM, SOC, or case-management workflows.
- Integrate legal-approved honeytoken or canary alerts only when the source has documented purpose, expected trigger, false-positive handling, incident-response linkage, and retirement criteria.
- Analyze inbound traffic to public web services, disclosure channels, support forms, and public repositories for scraping, probing, or targeted-reconnaissance patterns while distinguishing legitimate search engines, partners, and authorized testers.
- Preserve tuning records, alert evidence, action owner, closure outcome, and lessons learned so OSINT-driven detections can support Control Confidence Gap analysis and later board/auditor reporting.

Evidence core:

- OSINT signal-source register with owner, alert destination, and triage SLA
- Alert record with action owner, disposition, and closure outcome

Applicability: from mid scale.

FA5.SC2: Incident Response and Adaptation

Objective. Convert monitoring discoveries into governed response actions with playbooks, takedown paths, communication approvals, evidence preservation, lessons learned, and continuity records.

FA5.SC2.C1: OSINT Incident Playbooks

Maintain public-exposure incident playbooks with triggers, roles, evidence steps, severity criteria, and remediation handoffs.

Implementation guidance:

- Define playbooks for public data leaks, credential exposure, phishing or impersonation campaigns, lookalike domains or apps, executive doxing or threats, employee doxing or harassment (with an HR or people-support owner), deepfake or disinformation events, third-party public disclosures, departed-personnel residual exposure, M&A or divestiture footprint drift, and governed canary alerts.
- For each playbook, record trigger conditions, severity criteria, response owner, legal/privacy review point, communications owner, evidence-preservation steps, affected control assumptions, and handoffs to FA1, FA2, FA3, or FA4.
- Include source verification, containment, takedown, credential or secret rotation, employee/customer notification decision, platform or law-enforcement referral, retest, and residual-risk acceptance steps where applicable.
- Maintain current contact paths for security, legal, privacy, communications, HR, executive protection, third parties, platforms, registrars, hosting providers, and law enforcement.

- Exercise playbooks on a defined cadence and after material program changes; preserve scenario, participants, decisions, gaps, corrective actions, owner, due date, and closure evidence.

Evidence core:

- Playbook per priority exposure scenario with trigger, owner, and handoffs
- Current escalation and platform contact list
- Exercise record with date, gaps, and corrective-action owner

Applicability: from small scale.

FA5.SC2.C2: Rapid Takedown and Mitigation Actions

Operate approved takedown, containment, and mitigation paths with request evidence, response tracking, and retest records.

Implementation guidance:

- Maintain a takedown and mitigation channel inventory for platforms, search engines, app stores, social networks, registrars, hosting providers, code repositories, paste sites, data brokers, and unsafe-site reporting services.
- For each action, record source URL or identifier, request type, submission path, requester, legal or trademark basis where relevant, timestamp, platform response, follow-up date, and final disposition.
- Route leaked credentials, secrets, code, infrastructure exposure, and configuration issues to the technical owner for revocation, rotation, patching, or hardening while FA5 tracks intake, urgency, evidence, and closure.
- Define mitigation paths for content that cannot be removed, including warning blocks, search-result handling, user/customer notification, strengthened verification controls, monitoring, and residual-risk acceptance.
- Test priority takedown and containment workflows periodically and preserve elapsed time, blockers, lessons learned, and corrective actions.
- Reference cadence where none is defined yet: test priority takedown workflows twice yearly and review the platform contact sheet quarterly.

Evidence core:

- Takedown and reporting channel inventory with platform contact sheet
- Per-request record with submission date, requester, and platform response
- Final disposition with retest evidence or residual-risk acceptance where removal fails

Applicability: from micro scale.

FA5.SC2.C3: Communication and Notification Plans

Govern internal, customer, board, regulator, platform, and public communications for public-exposure incidents.

Implementation guidance:

- Define notification thresholds, approval chains, message owners, audience types, and timing expectations for employees, executives, customers, partners, boards, regulators, platforms, law enforcement, and the public.
- Maintain templates for phishing warnings, impersonation alerts, takedown notices, customer trust updates, executive-targeted events, and board-level exposure summaries.
- Require legal, privacy, communications, and incident-command review when communications could affect breach notification, employment matters, public markets, customer contracts, or law-enforcement coordination.
- Preserve drafts, approvals, distribution lists, timestamps, final messages, decision rationale, and follow-up obligations as part of the incident evidence package.
- Use verified facts, source provenance, uncertainty labels, and correction procedures so communications reduce attacker leverage without overstating attribution or compliance impact.

Evidence core:

- Notification thresholds and approval chain with named message owners
- Template set for priority warning and notification scenarios
- Per-event communication record with approvals, timestamps, and final message

Applicability: from mid scale.

FA5.SC2.C4: Continuous Improvement

Convert monitoring and incident outcomes into control updates, training updates, metrics changes, and residual-risk decisions.

Implementation guidance:

- Run an after-action review for material monitoring misses, confirmed incidents, major false positives, failed takedowns, delayed remediations, exercises, departed-personnel exposure events, and M&A or divestiture footprint events.
- Record the exposed condition, weakened control assumption, detection source, missed detection path, response timeline, business consequence, remediation decision, residual risk, and owner of each improvement item.
- Update monitoring sources, alert rules, playbooks, public-content controls, social-engineering training, technical safeguards, executive-protection handoffs, and compliance evidence requirements based on lessons learned.
- Track corrective actions through owner, due date, validation method, closure evidence, and recurring-review date.

- Share sanitized lessons with affected teams or approved information-sharing communities when it improves resilience and does not expose sensitive evidence.

Evidence core:

- After-action record per material incident, miss, or exercise
- Corrective-action log with owner, due date, and closure evidence
- Dated update to the affected rule, playbook, or training artifact

Applicability: from small scale.

FA5.SC2.C5: Temporary Communications and Escalation Continuity

Maintain approved temporary communication, escalation, and authority-verification paths for public-exposure incidents and high-risk events.

Implementation guidance:

- Define temporary communication channels and escalation paths for incidents, public events, executive travel, platform outages, doxing events, deepfake scenarios, and suspected compromise of ordinary channels.
- Record channel owner, authorized users, verification method, activation criteria, expiration date, logging expectation, privacy constraints, and fallback path before use.
- Require out-of-band authority verification for payment, account recovery, customer notification, legal, executive, and public-statement decisions made through temporary channels.
- Route executive travel preparation, personal-location privacy, and secure travel equipment guidance to FA4 while FA5 retains crisis escalation, incident communication, and post-event closure records.
- Preserve activation evidence, decision log, users notified, deactivation confirmation, post-use cleanup, and lessons learned.

Evidence core:

- Approved temporary-channel record with owner, authorized users, and expiration
- Out-of-band verification rule for payment, recovery, and public-statement decisions
- Activation evidence with decision log and deactivation confirmation per use

Applicability: from small scale.

FA5.SC2.C6: External Vulnerability Disclosure Intake

Operate a public vulnerability disclosure intake with a published security.txt, monitored contact, triage commitments, and intake-to-closure evidence.

Implementation guidance:

- Publish /.well-known/security.txt per RFC 9116 on primary public domains, with Contact and Expires fields kept current; treat an expired, missing, or unreachable security.txt as a finding.
- Publish a disclosure policy covering scope, legal safe-harbor language reviewed by counsel, expected acknowledgement time, and what reporters can expect; link it from the security.txt Policy field.
- Monitor the disclosure contact path with a named owner, acknowledgement SLA, triage severity criteria, spam and out-of-scope handling, and escalation into incident response when a report indicates active exploitation or material public exposure.
- Record intake-to-closure evidence per report: receipt timestamp, acknowledgement, triage decision, affected asset owner, remediation handoff to FA3 for technical findings, reporter communication, disposition, and closure date.
- Treat researcher reports as public-exposure signals: feed confirmed findings into FA5.SC1 monitoring records and FA5.SC2.C4 improvement, and acknowledge or credit reporters per policy where appropriate.
- Review the published files and contact path on a defined cadence and after domain, mail-routing, or ownership changes so the public intake never goes stale.
- Reference cadence: annual review of the published files and contact path; organizations may substitute a documented equivalent cadence.

Evidence core:

- Published security.txt with current Expires field and monitored contact
- Per-report record with receipt, acknowledgement, triage decision, and closure date

Applicability: from small scale.

Related controls: FA5.SC2.C4.

FA5.SC3: Measurement and Metrics

Objective. Define the ODSF exposure-scoring, measurement, threshold, reporting, and review cadence needed to turn findings into defensible program evidence.

FA5.SC3.C1: ODSF Exposure Scoring Method

Maintain a documented scoring method for public-exposure findings, control confidence gaps, and residual risk; every recorded finding names at least one abuse path.

Implementation guidance:

- Define scoring inputs such as exposure category, source reliability, freshness, persistence, replication, affected role or asset sensitivity, exploitability, abuse-path clarity, weakened control assumption, business consequence, and existing compensating controls.

- Adopt the framework's finding-scoring reference (assessment section) as the documented method where no method exists yet, then tailor inputs and thresholds to organizational context.
- Record data provenance, scorer, review date, confidence level, severity rationale, and any evidence limitations for each scored finding.
- Use consistent thresholds for the informational, monitored, remediation-required, and critical tiers, with incident linkage and executive review handled as escalation flags; define who can override a score and what evidence is required.
- Track baseline, current score, remediation target, retest result, residual-risk score, and acceptance owner so scoring measures verified risk reduction alongside discovery volume.
- Review the scoring method on a defined cadence and after major incidents, new exposure categories, platform changes, or changes in threat actor behavior.
- Reference cadence where none is defined yet: review the scoring method annually.

Evidence core:

- Documented scoring method or adopted framework reference with tier thresholds
- Per-finding score record with scorer, date, and named abuse path
- Residual-risk disposition with acceptance owner and retest result

Applicability: from micro scale.

FA5.SC3.C2: Program Effectiveness Metrics

Measure whether public-exposure monitoring, triage, remediation, retesting, and residual-risk handling are operating effectively.

Implementation guidance:

- Track time from discovery to triage, owner assignment, containment, remediation, retest, closure, and residual-risk acceptance by exposure category and severity.
- Measure source quality, duplicate rate, false-positive rate, missed-detection learnings, reopened findings, recurrence after remediation, and findings closed without source-backed verification.
- For approved canary identifiers, honeytokens, or decoy artifacts, track trigger volume, false positives, triage time, response linkage, tuning decisions, and retirement decisions.
- Track incident-linked findings, near misses, social-engineering attempts that reused public exposure, and business consequences such as fraud exposure, customer-trust impact, response cost, or operational disruption where evidence supports the measure.
- Use metrics to identify stale owners, weak takedown channels, incomplete evidence, untested playbooks, training gaps, and controls that remain in accepted-risk status.

Evidence core:

- Dated metrics report covering triage, remediation, and closure timeliness

- False-positive and recurrence measures by source or category
- Tuning or improvement decision traced to a metric result

Applicability: from mid scale.

FA5.SC3.C3: Metric Ownership and Thresholds

Assign each ODSF metric a business owner, data source, formula, threshold, audience, and review cadence.

Implementation guidance:

- Define each metric's purpose, source system, calculation method, reporting owner, accountable business owner, target threshold, exception rule, and review frequency.
- Separate governance metrics such as triage timeliness, closure evidence, residual-risk age, and report readiness from control-specific metrics owned by FA1, FA2, FA3, or FA4.
- Avoid vanity counts by pairing discovery volume with severity, verified impact, remediation status, recurrence, and residual-risk decisions.
- Document thresholds that trigger escalation to security leadership, legal/privacy review, executive protection, customer communications, or board reporting.
- Review metric usefulness periodically and retire measures that do not drive decisions, remediation, reporting, or evidence quality.

Evidence core:

- Metric register with business owner, data source, formula, threshold, and audience
- Dated usefulness review with retired or revised metrics

Applicability: from mid scale.

FA5.SC3.C4: Board, Auditor, and Operational Reporting

Produce audience-specific public-exposure reports with evidence-backed findings, trends, residual risk, and action status.

Implementation guidance:

- Maintain operational dashboards for open findings, triage status, owner, severity, source, remediation age, retest status, and evidence completeness.
- Prepare board-ready reporting that summarizes top exposure themes, material control confidence gaps, remediation progress, accepted residual risks, incident linkage, and management decisions.
- Prepare auditor-ready evidence packets that link findings to source evidence, decision logs, remediation records, retest artifacts, retention rules, and summary language without implying final control-level framework mappings before those mappings are reviewed.
- Use trend reporting to show exposure reduction, recurring categories, stale actions, monitoring coverage gaps, and changes after incidents or program updates.

- Apply access controls and redaction rules to reports containing credentials, personal data, executive details, sensitive investigation facts, or legal-privileged material.

Evidence core:

- Operational findings report with status, owner, and remediation age
- Dated board-level exposure summary with accepted residual risks
- Evidence packet linking findings to sources, decisions, and retest artifacts

Applicability: from mid scale.

FA5.SC4: Governed Deception and Canary Infrastructure

Objective. Govern legal-approved honeytokens, canary identifiers, monitored decoy artifacts, and isolated deception infrastructure used to detect reconnaissance, with documented owner, approval, monitoring, safety, response, and retirement records.

FA5.SC4.C1: Honeytoken and Canary Artifact Authorization

Authorize canary artifacts before deployment and record the purpose, ownership, monitoring path, and retirement criteria.

Implementation guidance:

- Approve each honeytoken, canary identifier, decoy email address, document marker, credential-like token, or source marker before deployment; record owner, purpose, scope, lawful basis, platform or contract constraints, alert destination, and retirement date.
- Use unique identifiers and non-sensitive artifacts that cannot grant access, misrepresent real people, or create obligations for customers, applicants, vendors, or the public.
- Place canary artifacts only in approved internal or controlled external locations. Public placement requires legal, communications, and platform review with a documented business-risk rationale.
- Preserve deployment evidence, alert configuration, expected trigger, false-positive handling, review cadence, and closure records for each active canary artifact.

Evidence core:

- Per-artifact authorization record with owner, purpose, alert destination, and retirement date
- Deployment evidence with alert configuration and expected trigger
- Closure or retirement record per retired artifact

Applicability: from mid scale; condition: governed canary signals or deception artifacts.

FA5.SC4.C2: Public Deception Boundary

Control any public-facing deception or ambiguity so it does not undermine publication governance, audit evidence, brand trust, or platform obligations.

Implementation guidance:

- Require legal, ethics or communications, security, and business-owner approval before any public-facing decoy, ambiguity, or signal-to-noise measure is considered.
- Document target risk, expected detection value, affected audiences, platform obligations, customer or vendor impact, measurement plan, rollback criteria, and residual-risk owner.
- Use accurate public-content governance from FA1 as the default standard for public materials, with routine deception programs kept inside controlled artifacts and approved monitoring channels.
- Treat contradictory public statements, fake employees, fake jobs, fake code, and planted misinformation as advanced-practices exceptions that require separate rules of engagement and executive approval.

Evidence core:

- Pre-approval record with legal, communications, security, and business-owner sign-off
- Documented detection value, rollback criteria, and residual-risk owner per measure

Applicability: from mid scale; condition: governed canary signals or deception artifacts.

FA5.SC4.C3: Deception Infrastructure Governance

Govern isolated decoy systems and monitored infrastructure through explicit authorization, technical safeguards, logging, and decommissioning records.

Implementation guidance:

- Authorize honeypot systems, decoy subdomains, monitored API endpoints, sinkholes, or similar infrastructure through a documented security program before deployment.
- Record the FA5 program owner and FA3 technical owner, asset inventory status, isolation boundary, network segmentation, logging design, data-handling restrictions, safety controls, and decommissioning plan.
- Ensure decoy infrastructure cannot be mistaken for unsupported production assets, expose real organizational data, collect unnecessary personal data, or create unsafe interaction paths.
- Test alert delivery, incident-response routing, false-positive handling, and shutdown procedures before activation and during periodic review.

Evidence core:

- Authorization record per decoy system with program and technical owners
- Documented isolation boundary, logging design, and decommissioning plan

- Dated alert-delivery and shutdown test result

Applicability: from mid scale; condition: governed canary signals or deception artifacts.

FA5.SC4.C4: Canary Alert Response and Engagement Boundaries

Define response actions for canary and deception alerts while constraining active interaction with suspected adversaries.

Implementation guidance:

- Route canary and deception alerts through incident-response triage with evidence preservation, severity assignment, action ownership, legal review triggers, and closure records.
- Define approved response options such as observe, block, preserve, notify, takedown, retest, report to a platform, refer to law enforcement, or share indicators with an approved information-sharing community.
- Require written executive and legal authorization, safety review, rules of engagement, and incident-command ownership before any active interaction with suspected adversaries.
- Use detection outcomes to update monitoring rules, employee awareness, public-content controls, technical safeguards, and residual-risk decisions.

Evidence core:

- Triage record per canary alert with severity, action owner, and closure
- Approved response-option list with engagement constraints
- Written executive and legal authorization preceding any active adversary interaction

Applicability: from mid scale; condition: governed canary signals or deception artifacts.

FA5.SC5: Internal OSINT Defense

Objective. Govern internal information patterns that can become externally useful reconnaissance, while routing generic IAM, DLP, directory, and insider-risk implementation to their primary control homes.

FA5.SC5.C1: Internal Reconnaissance Exposure Boundaries

Define internal information boundaries for details that could become public-exposure fuel if leaked, scraped, overshared, or reused in social engineering.

Implementation guidance:

- Identify internal details that carry ODSF relevance, including unreleased project names, privileged team structures, support workflows, approval chains, vendor relationships, departed-personnel references, acquisition or divestiture workstreams, internal URLs, emergency contacts, and recovery procedures.

- Define approved disclosure level, owner, business purpose, sharing boundary, exception path, and review cadence for those details.
- Route ordinary data classification, access control, DLP, and directory permission implementation to the organization's primary security governance and FA3 technical-control homes.
- Preserve boundary decisions, exceptions, approved disclosures, detected leakage, remediation owner, and residual-risk acceptance as FA5 governance evidence.
- Use monitoring and incident outcomes to update internal sharing rules when exposed internal detail weakens identity verification, fraud prevention, vendor management, or incident-response assumptions.

Evidence core:

- Sensitive internal-detail inventory with approved disclosure level and owner
- Exception or approved-disclosure record with owner and date
- Detected-leakage record with remediation owner and residual-risk disposition

Applicability: from mid scale.

FA5.SC5.C2: Internal Reconnaissance Signal Monitoring

Monitor for internal collection patterns that could indicate preparation for public leakage, impersonation, coercion, or unauthorized aggregation.

Implementation guidance:

- Define monitored signals such as unusual directory enumeration, sensitive roster exports, bulk profile access, repeated searches for executives or approval chains, project-name harvesting, and access to public-release repositories or evidence archives.
- Record legal, privacy, HR, labor, and acceptable-use boundaries before monitoring employee activity; collect the minimum evidence needed for triage and response.
- Use approved honeytokens or canary artifacts only through FA5.SC4 authorization with documented owner, purpose, alert path, and retirement criteria.
- Set alert thresholds, false-positive handling, investigation roles, escalation paths, and closure records for internal reconnaissance signals.
- Route insider-risk, HR, IAM, endpoint, and logging implementation to the appropriate owners while FA5 retains exposure-governance rationale, evidence, and lessons learned.

Evidence core:

- Monitored signal definitions with alert thresholds and investigation roles
- Dated legal, privacy, and HR boundary review preceding employee monitoring
- Alert investigation record with escalation and closure outcome

Applicability: from mid scale; condition: in-house internal telemetry or UEBA.

FA5.SC5.C3: Project and Codename Exposure Governance

Govern project names, codenames, launch plans, and internal labels that can reveal business strategy, technical direction, or attack paths when exposed.

Implementation guidance:

- Define naming guidance for sensitive initiatives, acquisitions, divestitures, integrations, launches, incident workstreams, security projects, and customer programs where descriptive names could create reconnaissance value.
- Require owner, sensitivity, approved disclosure level, expiration or declassification trigger, and exception approval for project names and codenames used outside controlled internal channels.
- Monitor public content, recruiting posts, repositories, documents, vendor materials, conference talks, and support artifacts for unexpected project or codename exposure.
- Route current publication cleanup to FA1 and repository or technical leakage remediation to FA3 while FA5 tracks source, owner, severity, action, retest, and residual risk.
- Update naming rules, release checklists, and training triggers when exposed project language weakens confidentiality, vendor management, acquisition, incident-response, or fraud-prevention assumptions.

Evidence core:

- Sensitive project-name register with owner, disclosure level, and declassification trigger
- Exposure finding record with source, severity, and action owner
- Retest or residual-risk record per confirmed exposure

Applicability: from mid scale.

FA5.SC5.C4: Organizational Structure Exposure Governance

Govern exposure of roles, reporting lines, approval authority, support paths, and team structure that can enable impersonation or targeted pressure.

Implementation guidance:

- Define which organizational details may be public, limited, or restricted for executives, finance, HR, legal, IT administrators, incident responders, support teams, and other high-risk roles.
- Review public bios, job postings, org charts, conference materials, vendor case studies, support documentation, partner portals, departed-employee public profiles, archived leadership pages, acquisition pages, and divestiture materials for role hierarchy, approval authority, escalation paths, or recovery workflows.
- Route public-content correction to FA1, directory and access-control implementation to FA3 or the primary IAM program, and executive/private-life exposure to FA4.
- Track exposure source, affected role or process, abuse path, owner, approval or exception, mitigation, retest, and residual-risk decision.

- Use findings to strengthen transaction verification, account recovery, vendor onboarding, escalation procedures, and incident communications.

Evidence core:

- Disclosure classification for executive, finance, support, and other high-risk roles
- Dated review result covering bios, job postings, and org-chart exposure
- Exposure finding with abuse path, mitigation, and residual-risk decision

Applicability: from small scale.

FA5.SC6: Regulatory and Compliance Alignment

Objective. Govern legal review, jurisdiction-aware monitoring rules, evidence records, and mapping-pack readiness without creating unreviewed compliance claims.

FA5.SC6.C1: Privacy and Legal Basis Governance

Review public-exposure monitoring and evidence handling for privacy, lawful basis, data minimization, and legal-review requirements.

Implementation guidance:

- Classify monitored data categories, affected people, source type, collection method, business purpose, lawful basis or approval rationale, retention period, and access restrictions.
- Define legal-review triggers for employee or executive monitoring, leaked personal data, credential or breach data, dark-web collection, scraping, cross-border processing, platform terms, and law-enforcement or regulator contact.
- Maintain procedures for data subject, employee, executive, customer, or third-party requests connected to OSINT-collected evidence, including verification, response owner, and preservation limits.
- Require data minimization, redaction, need-to-know access, legal hold handling, and deletion or retention decisions for evidence that contains personal data or sensitive investigation material.
- Preserve legal/privacy review records, approval decisions, restrictions, retention decisions, incident notification analysis, and residual-risk rationale.

Evidence core:

- Monitored-data classification with lawful basis, purpose, and retention period
- Dated legal or privacy review record with approval and restrictions
- Deletion, redaction, or retention decision record for sensitive evidence

Applicability: from mid scale.

FA5.SC6.C2: Mapping-Pack Applicability Governance

Control when ODSF findings may be connected to external frameworks, regulations, or assurance regimes through reviewed mapping packs.

Implementation guidance:

- Record the applicable framework, regulation, sector, geography, version, retrieval date, source URL, reviewer, review status, and applicability rationale before using an external mapping in customer or audit-facing material.
- Treat broad focus-area alignment as orientation metadata and maintain detailed control-level mappings in a reviewed mapping pack or other approved evidence layer.
- Document the ODSF exposure, weakened control assumption, business consequence, required evidence, remediation record, residual-risk path, and mapping rationale for each reviewed mapping.
- Treat non-NIST, sector-specific, and jurisdiction-specific control-level mappings as unsupported until a published mapping pack or the organization's own documented crosswalk provides source-backed rationale and review status.
- Preserve change history, reviewer notes, source updates, superseded mappings, and customer-facing language approvals so mapping evidence remains defensible.

Evidence core:

- Mapping record with framework version, source, retrieval date, and reviewer
- Documented applicability rationale per customer-facing or audit-facing mapping
- Change history with superseded mappings and approved language

Applicability: from mid scale; condition: external framework mappings used in audit or customer material.

FA5.SC6.C3: Jurisdiction and Cross-Border Monitoring Rules

Define jurisdiction-aware rules for monitoring operations, evidence retention, data handling, and cross-border review.

Implementation guidance:

- Maintain a monitoring-rules register for countries, regions, data sources, data categories, platform terms, employee-monitoring constraints, breach-data handling, dark-web access, scraping, and cross-border transfer review.
- Require legal/privacy review before collecting, storing, or sharing leaked personal data, credential material, sensitive executive information, protected employee data, or data sourced from restricted forums or markets.
- Document permitted collection methods, prohibited methods, retention limits, access controls, redaction requirements, transfer restrictions, and escalation paths for each jurisdiction-sensitive monitoring activity.

- Coordinate cross-border incidents through legal, privacy, security, communications, and local business owners; record notification analysis and local remediation constraints.
- Review jurisdiction rules when entering new markets, changing monitoring providers, adding new data sources, processing new personal-data categories, or producing customer/auditor evidence in a new region.

Evidence core:

- Jurisdiction monitoring-rules register covering sources, methods, and retention limits
- Dated legal review preceding sensitive collection, storage, or cross-border transfer

Applicability: from mid scale.

FA5.SC6.C4: Evidence Vault and Audit Packet Records

Maintain defensible evidence records for monitoring, findings, decisions, remediation, retesting, reporting, and audit packets; residual risk is recorded with an owner and review date.

Implementation guidance:

- Capture source URL or identifier, screenshot or export, timestamp, collector or system, collection method, source reliability, hash or integrity marker where appropriate, affected person or asset, and related control or finding ID.
- Record decision logs for severity, owner assignment, legal/privacy review, notification analysis, remediation option, exception, residual-risk acceptance, and closure approval.
- Link remediation tickets, takedown requests, platform responses, credential or secret rotation evidence, configuration changes, retest results, recurrence monitoring, and after-action items to the evidence record.
- Define retention, legal hold, redaction, access control, segregation of sensitive personal data, and deletion procedures for evidence records and audit packets.
- Produce auditor-ready and board-ready summaries that explain the exposed condition, weakened control assumption, business consequence, evidence status, remediation status, and residual-risk path without overclaiming unreviewed framework mappings.

Evidence core:

- Per-finding evidence record with source, timestamp, collection method, and integrity marker
- Decision log covering severity, remediation choice, exception, and closure approval
- Residual-risk record with acceptance owner and review date

Applicability: from small scale.

FA5.SC7: Cross-Platform Identity Linkage Prevention

Objective. Govern approved organizational identity separation, public identity-pattern review, and linkage monitoring where public correlations can enable impersonation, account recovery abuse, privileged targeting, or fraud.

FA5.SC7.C1: Approved Role and Identity Separation

Define approved identity types and separation rules for role accounts, privileged accounts, public spokespeople, support channels, and sensitive workflows.

Implementation guidance:

- Maintain an inventory of approved identity types, business purpose, owner, platform, expected public linkage, recovery channel, approval date, and retirement criteria.
- Use legitimate role accounts, team mailboxes, official support identities, spokesperson profiles, and privileged-administration identities where separation reduces impersonation, recovery, or fraud risk.
- Document platform rules, legal/privacy boundaries, naming standards, access ownership, recovery procedures, and customer or vendor impact before creating or changing organizational identities.
- Route technical account controls, MFA, browser or endpoint separation, and IAM implementation to FA3; route executive/private-life identity protection to FA4.
- Preserve approval records, exceptions, unauthorized-linkage findings, remediation actions, and residual-risk decisions.

Evidence core:

- Approved identity inventory with owner, platform, purpose, and recovery channel
- Approval or exception record per identity change with date
- Unauthorized-linkage finding with remediation action and residual-risk decision

Applicability: from small scale.

FA5.SC7.C2: Public Identity Pattern Review

Review public usernames, profile details, contact metadata, recovery hints, and communication patterns that can link sensitive identities or workflows.

Implementation guidance:

- Assess reused usernames, emails, phone numbers, profile images, bios, titles, recovery contacts, domains, handles, posting patterns, signature blocks, and metadata for linkage risk.
- Prioritize identities tied to executives, privileged users, finance and HR approvers, incident responders, administrators, support desks, public spokespeople, and high-risk business workflows.

- Define approved pattern standards and exceptions for official public identities where consistency is required for trust, customer support, or brand authenticity.
- Route public-profile and publication updates to FA1 or FA4 and technical account changes to FA3 while FA5 retains linkage rationale, monitoring evidence, and residual-risk records.
- Retest after remediation and record remaining linkages, compensating controls, owner approval, and review cadence.

Evidence core:

- Dated linkage-review result covering prioritized high-risk identities
- Remediation or approved-exception record per linkage finding
- Retest record with remaining linkages and compensating controls

Applicability: from small scale.

FA5.SC7.C3: Sensitive Workflow Anti-Correlation Governance

Govern when technical or operational anti-correlation measures are appropriate for sensitive organizational workflows.

Implementation guidance:

- Identify workflows where correlation would create organizational risk, such as incident response, fraud investigation, abuse reporting, executive support, sensitive procurement, legal matters, and privileged administration.
- Require business purpose, owner, legal/privacy review, platform-rule review, data-handling requirements, and expected evidence before approving anti-correlation measures.
- Route browser, endpoint, network, account, and access-control implementation to FA3, and route personal privacy tooling or executive household use to FA4.
- Document approved tools or procedures, authorized users, logging expectations, failure handling, retention, and review cadence.
- Retire anti-correlation measures when the sensitive workflow ends, and preserve closure, exception, and residual-risk records.

Evidence core:

- Approval record per measure with business purpose, owner, and legal review
- Documented procedure with authorized users and logging expectations
- Retirement or closure record when the sensitive workflow ends

Applicability: from mid scale; condition: anti-correlation measures in use or under evaluation for sensitive workflows.

FA5.SC7.C4: Identity Linkage Monitoring

Detect public correlations between approved organizational identities, role accounts, privileged users, executive identities, and personal or professional accounts.

Implementation guidance:

- Monitor concrete linkage indicators such as reused usernames, emails, phone numbers, profile images, recovery contacts, metadata, biographies, domains, shared handles, and cross-posted content.
- Consume the approved-identity inventory maintained under FA5.SC7.C1 as the monitoring scope baseline, covering identity types, account owners, platform constraints, legal/privacy boundaries, business purpose, and expected public linkage for role accounts, privileged accounts, public spokespeople, and support channels, recorded once and referenced here.
- Route canary identity concepts to FA5.SC4 approval and FA2 awareness before use; routine identity-linkage monitoring should focus on real approved identities and unauthorized correlations.
- Develop alerting, triage ownership, evidence capture, false-positive handling, response procedures, and closure records for unexpected or risky identity links.
- Use findings to update role-account separation, public profile guidance, recovery metadata, executive-protection handoffs to FA4, and technical account controls in FA3.

Evidence core:

- Monitoring scope record referencing the approved-identity inventory
- Linkage alert record with triage owner and disposition
- Closure evidence with remediation or accepted residual linkage

Applicability: from mid scale.

Related controls: FA5.SC7.C1.

FA5.SC8: OSINT Training Program

Objective. Govern ODSF training cadence, role coverage, completion evidence, refresher triggers, competency checks, and program metrics while routing detailed training content to the owning focus areas.

FA5.SC8.C1: Training Governance and Role Coverage

Maintain the enterprise ODSF training plan, required role coverage, cadence, completion evidence, exceptions, and refresher triggers.

Implementation guidance:

- Define training populations by role, exposure level, authority, privileged access, public visibility, approval responsibility, and incident-response responsibility.
- Assign required modules, owner, delivery cadence, completion deadline, assessment method, exception path, and refresher triggers for each population.

- Route social-engineering content to FA2, technical exposure content to FA3, executive/private-life content to FA4, and public-content/data-minimization content to FA1 while FA5 owns program governance evidence.
- Trigger refreshers after incidents, monitoring trends, role changes, departures, acquisitions, divestitures, policy changes, exposure-scoring updates, new public-exposure categories, or material control failures.
- Preserve rosters, completions, exceptions, assessment results, reminders, overdue actions, refreshers, and program-metric reports.
- Reference cadence: annual refresher per covered population; organizations may substitute a documented equivalent cadence.

Evidence core:

- Role-based training assignments with modules, owner, and completion deadline
- Completion roster with dates and approved exceptions per population
- Refresher record tied to incident, role-change, or policy triggers

Applicability: from mid scale.

FA5.SC8.C2: Technical Training Governance

Govern curriculum coverage and evidence for technical teams whose work can create public-exposure findings.

Implementation guidance:

- Define training requirements for developers, DevOps, cloud, IT, security operations, support engineering, product security, and administrators based on public-exposure risk.
- Cover learning objectives such as repository exposure, secret handling, public asset changes, metadata leakage, API documentation, support artifacts, logging evidence, and handoffs to FA3 controls.
- Require practical exercises, scenario review, or workflow checks where a role can create or remediate high-risk public exposure.
- Use FA3 incidents, monitoring findings, code leaks, exposed infrastructure, and technical takedown outcomes as triggers for curriculum updates.
- Preserve role roster, objectives, completion, exercise artifacts, exception records, improvement items, and evidence that technical findings changed training content.

Evidence core:

- Technical-role training roster with objectives and completion dates
- Practical exercise or workflow-check artifact for high-risk roles
- Curriculum-update record traced to technical findings or incidents

Applicability: from mid scale.

FA5.SC8.C3: Executive and High-Risk Role Training Governance

Govern training coverage for executives and other high-risk roles where public exposure can enable fraud, coercion, impersonation, or account recovery abuse.

Implementation guidance:

- Identify high-risk roles such as executives, board-facing staff, assistants, finance approvers, HR, legal, procurement, incident commanders, administrators, and public spokespeople.
- Define training objectives for authority verification, account recovery risk, telecom exposure, deepfake and vishing scenarios, payment or vendor fraud, public appearance exposure, and incident communication discipline.
- Keep personal, household, family, and executive-private-life material consent-based and routed to FA4; FA5 records role coverage, cadence, completion, exceptions, and refresher triggers.
- Use executive-targeted incidents, monitoring changes, public media events, new impersonation patterns, or major role changes to trigger updates or one-on-one briefings.
- Preserve attendance, coaching records where appropriate, accepted exceptions, compensating controls, and residual-risk decisions for high-risk personnel who cannot complete or fully follow the guidance.

Evidence core:

- High-risk role roster with assigned objectives and cadence
- Completion or briefing record with date per covered person
- Accepted-exception record with compensating controls and residual-risk decision

Applicability: from mid scale.

FA5.SC8.C4: Competency Evidence for Critical Roles

Verify practical ODSF competency for roles that collect evidence, triage findings, approve exceptions, communicate incidents, or remediate exposures.

Implementation guidance:

- Define critical roles that require competency evidence, such as exposure analysts, incident responders, evidence reviewers, legal/privacy approvers, communications approvers, technical remediators, and training owners.
- Use practical exercises, case reviews, tabletop participation, evidence-quality checks, or supervised findings to verify competency before relying on formal certification claims.
- Record assessor, scenario, performance criteria, result, remediation coaching, retest requirement, expiration or refresh date, and approved scope of responsibility.
- Trigger renewed competency evidence after major framework changes, tooling changes, incidents, repeated evidence-quality failures, or long gaps in role performance.

- Treat formal certification tracks as optional program maturity evidence; a formal track requires defined curriculum, assessor qualifications, and review cadence before the organization treats it as required.

Evidence core:

- Critical-role list requiring practical competency evidence
- Assessment record with assessor, scenario, result, and refresh date

Applicability: from large scale.

Assessment and Scoring

ODSF defines controls, evidence expectations, a reference rubric for scoring control implementation, and a reference method for scoring exposure findings. It does not define a maturity model, implementation tiers, conformance profiles, or a certification scheme; those are planned for the 1.0 release. Conformance claims against this version are self-assessments and must state the framework version, the scope of controls assessed, and the scoring method used; FA5.SC6.C2 governs public claims.

Scoring control implementation

A reference rubric for assessing control implementation. Organizations may substitute an equivalent method; whichever method is used must be documented and applied consistently.

- **Level 0 · Not implemented**: No owner, no operating process, no evidence.
- **Level 1 · Planned**: Named owner and a documented plan or schedule; the control is not yet operating.
- **Level 2 · Partially implemented**: Operating for part of the in-scope population, operating without the control's evidence core captured, or operating without a material element of the described outcome.
- **Level 3 · Implemented**: Operating across the in-scope population with the control's evidence core captured and current; documented organization-defined equivalents satisfy the core per the conventions.
- **Level 4 · Implemented and verified**: Evidence retested, exercised, or independently reviewed within the stated review cadence; exceptions and residual-risk records current. The control's full guidance field set is the depth target where the organization needs that depth.

Two dispositions sit outside the scale:

- **Not applicable**: The control's subject does not exist in the organization, for example FA1.SC7 where no public mobile app exists; the rationale is recorded and reviewed when circumstances change.
- **Risk accepted**: A documented decision not to implement, with owner, rationale, compensating controls where relevant, and a review date. Counted as not implemented in coverage metrics and distinguished in reporting.

Report scores per subcategory and focus area as distributions or averages alongside coverage, defined as the percentage of applicable controls at level 3 or above. All controls carry equal weight in this version; weighting, tiers, and profiles are deferred to the planned assessment

model. Applicability is decided by each control's applicability tags together with the not-applicable disposition.

Scoring exposure findings

A reference severity method for exposure findings, usable as the documented scoring method FA5.SC3.C1 requires when the organization has no existing method.

Inputs. Exploitability and abuse-path clarity; sensitivity of the affected role, asset, or workflow; freshness, persistence, and replication of the exposure; the control assumption it weakens (the Control Confidence Gap); and business consequence if abused. Compensating controls reduce the result by at most one tier.

- **Informational**: Exposure with no clear abuse path or negligible consequence; recorded for trend visibility.
- **Monitored**: Plausible abuse path with limited consequence or strong compensating controls; recurrence monitoring assigned.
- **Remediation required**: Clear abuse path against a sensitive role, asset, or workflow; owner, due date, and retest assigned. Abuse paths against executive authority, payment workflows, or regulated data carry an escalation flag.
- **Critical**: Active exploitation or incident linkage; immediate escalation per FA5.SC2 and executive review.

The baseline subset

The recommended starting point for small organizations and first-year programs: the controls that interrupt the most common public-information attack paths (phishing and payment fraud, account-recovery abuse and SIM swap, breached-credential reuse, impersonation, and data-broker-fed targeting) using procedures and built-in platform features rather than dedicated security tooling.

Each baseline control either blocks a common high-consequence abuse path on its own or supplies the inventory and reporting backbone the other baseline controls depend on. Controls requiring dedicated tooling, specialist staffing, or conditional subjects (public mobile apps, software development, deception infrastructure) are excluded. At baseline scale, domain-level breach-notification monitoring with triage records satisfies FA5.SC1.C1; dedicated stealer-log, marketplace, and dark-web monitoring services extend the same control as the program grows. Outbound brand-impersonation monitoring (FA5.SC1.C2) is deliberately post-baseline; the baseline covers inbound impersonation defense and response. At baseline scale one broker-suppression program suffices: FA1.SC4.C1's workforce-wide regime covers executives and other high-risk persons, and the consent-scoped executive program (FA4.SC1.C2) enters when household members or personal-agreement authority require it.

FA1 · Digital Footprint Reduction

- **FA1.SC1.C1**: Identify Public Assets and Data

- **FA1.SC1.C2**: OSINT Footprint Assessment
- **FA1.SC1.C4**: Risk Analysis of Exposed Information
- **FA1.SC2.C1**: Current Public Data Remediation and Minimization
- **FA1.SC3.C2**: Controlled Sharing on Social Media
- **FA1.SC4.C1**: Data Broker and People-Search Exposure Suppression
- **FA1.SC5.C2**: Document and PDF Sanitization

FA2 · Social Engineering Defense

- **FA2.SC1.C1**: OSINT Awareness in Training Programs
- **FA2.SC1.C2**: Recurring Training Delivery and Reinforcement
- **FA2.SC1.C4**: Verification Culture and Non-Punitive Reporting
- **FA2.SC1.C5**: Risk-Tiered Training for High-Risk Roles
- **FA2.SC2.C1**: Out-of-Band Verification for Sensitive Requests
- **FA2.SC2.C2**: Multi-person Approval
- **FA2.SC3.C1**: Email Security Gateway and Phishing Filters
- **FA2.SC3.C3**: Multi-Factor Authentication Everywhere
- **FA2.SC5.C1**: Incident Reporting Channels
- **FA2.SC5.C2**: Containment Actions
- **FA2.SC7.C1**: Voice Authentication Protocols

FA3 · Technology Exposure Management

- **FA3.SC1.C1**: Domain and Subdomain Inventory
- **FA3.SC2.C5**: Remote Access and Management Interface Hardening
- **FA3.SC2.C6**: Outbound Email and Domain Authentication Posture

FA4 · Executive Exposure Protection

- **FA4.SC2.C1**: Executive Account and Recovery Hardening
- **FA4.SC2.C2**: Executive Telecom and Mobile Number Protection
- **FA4.SC4.C2**: Executive Authority and Instruction Boundaries

FA5 · Continuous Monitoring and Response

- **FA5.SC1.C1**: Breach and Credential Exposure Monitoring
- **FA5.SC2.C2**: Rapid Takedown and Mitigation Actions
- **FA5.SC3.C1**: ODSF Exposure Scoring Method

Adoption paths

Self-assessment is the scope for all organizations. For micro organizations with no security function, the recorded path is consultancy-delivered adoption: an advisor runs the baseline controls and the assessment and delivers a fixed readout, a named owner at the organization accepts residual-risk decisions, and the evidence core may live in ordinary business records such as mail folders, shared drives, and ticket or invoice trails rather than dedicated registers.

Implementing the Framework

ODSF builds resilience through a structured lifecycle: identify exposures, protect and reduce them, detect new ones, respond to incidents, and adapt as the threat picture changes. Organizations that already run NIST CSF will recognize the rhythm; ODSF applies it to the public-information attack surface specifically.

Tailoring by organization size

A 50-person company can start with the baseline subset in the assessment section: perform a footprint audit, train staff on phishing and pretext calls, enforce MFA everywhere including executive accounts, lock down the handful of public-facing systems, and set alerts on the company name and key personnel. A designated IT security contact can own monitoring and response without a dedicated security operations center.

A large enterprise can formalize each focus area: a digital risk protection service for footprint reduction, a security awareness program with verification drills, an attack surface management function, an executive protection unit working with corporate security, and a security operations center consuming OSINT intelligence feeds. Connecting ODSF controls to the organization's existing standards program unifies the compliance work.

Executive sponsorship decides how far the program goes. The framework protects executives directly, which makes the case easier to carry, and the program belongs inside existing governance: risk committees, security steering groups, and the policy cycle.

Working alongside existing standards

Each focus area carries category-level orientation to NIST CSF 2.0, marked explicitly as orientation metadata; control-level crosswalks ship separately as ODSF mapping packs, so the framework's claims stay reviewable and the mappings stay versioned. The verification disciplines reflect zero-trust principles: verify requests out of band, expose the minimum, treat familiarity as a claim to verify. The data-minimization core supports privacy obligations, including GDPR-style minimization and erasure duties, because removing unnecessary public personal data is the shared mechanism.

From controls to policy

The framework feeds corporate policy directly. An acceptable use policy can absorb the social media and information-sharing controls, an incident response plan can absorb the OSINT-specific playbooks, and the control catalog doubles as an audit checklist with evidence-backed questions. The controls also justify budget: monitoring services, removal services, and training programs map to named controls and the abuse paths they close.

What rigorous application produces

- A reduced attack surface: less leaked material means attackers work harder for a foothold.
- Early warning: monitoring catches credential leaks and impersonation campaigns at the start, while response is cheap.
- Resilience against social engineering: trained people and verified processes contain even well-researched approaches.
- Protection for leaders and brand: impersonation and reputation attacks are prevented or countered quickly.
- A proactive posture: the organization hunts and fixes weaknesses in the open-source domain on its own schedule, ahead of the attacker's.

A Note from the Author

I developed this framework because the frameworks defenders rely on have to evolve with the threats. After almost 30 years in IT and cybersecurity, and as an OSINT practitioner, I kept seeing the same failure: enterprises spending millions on tooling and staffing, then losing to attacks that began with public information. In a May 2023 BlackCloak study, 42% of organizations surveyed had already had a senior executive or an executive's family member attacked by a cybercriminal. By 2025, Semperis was reporting physical threats against staff in 40% of ransomware attacks. The MGM Resorts intrusion of 2023 succeeded in part because staff profiles and technology details were publicly exposed and readily weaponized. As a community of defenders, we were watching one side of the map. We needed to start thinking differently.

Adopting ODSF is an ongoing commitment, and it changes culture as much as tooling. It requires cross-functional collaboration across IT, HR, legal, communications, and the executive suite, regular revisiting of assumptions, and staying informed about how OSINT is collected and used. Organizations that cultivate that awareness, where everyone understands the value and the risk of information, turn the adversary's tradecraft into a defensive instrument and fare far better than those that rely on conventional cybersecurity frameworks alone.

Use this document as a blueprint. It can anchor a digital risk management initiative, justify enhanced awareness training, and turn each subcategory into an actionable project with an owner and a quarter attached. Maturity builds over time, and the assessment section's rubric tracks it. The framework is comprehensive, and risk assessment should still guide prioritization: start with the high-impact, feasible steps such as critical asset scanning and executive data-broker opt-outs, then expand.

Organizations large and small can use ODSF to close off one of the most fundamental sources of risk: publicly accessible information, freely available to anyone who looks. I wrote this framework so defenders can stay a step ahead in the continuous contest of intelligence and counterintelligence.

Ray Heffer, CISSP

Author, OSINT Defense & Security Framework

Acknowledgements

The author thanks the reviewers who contributed editorial feedback to the framework's draft versions.

- **Paul Mander** (Optery): Review and editorial suggestions, v0.1.x drafts.
- **Sara Trammell** (Optery): Review and editorial suggestions, v0.1.x drafts.

Both listed contributors were affiliated with Optery, a personal data removal vendor, at the time of their review contributions to the v0.1.x drafts. The framework recommends no commercial products or services; vendor and tool names appearing in guidance are illustrative examples, not endorsements.

Glossary

abuse path

The route from publicly available information to attacker action, such as an exposed staff directory enabling a credible payroll-change pretext. Exposure findings record at least one abuse path so remediation priority reflects attacker use rather than data sensitivity alone.

adversary archetype

A generic adversary capability class described in the threat model: objectives, OSINT tradecraft, and the controls that counter it. Archetypes orient reading and calibration; they never name specific groups or vendors.

baseline subset

The designated set of controls recommended as the starting point for small organizations and first-year programs, listed in the assessment section. The baseline is a starting order, not a conformance ceiling.

canary signal

A monitored marker, such as a decoy email alias or tagged document, placed so that any external reference to it indicates reconnaissance or data misuse. Canary signals are governed through FA5.SC4 and trained through FA2.SC6.

Control Confidence Gap

The loss of justified confidence in a security control when publicly available information weakens an assumption the control relies on. Example: help desk identity verification assumes a caller cannot easily know an employee's manager, start date, and phone number; public profiles exposing those details create a Control Confidence Gap in that verification control. ODSF prioritizes exposures by the gaps they create or widen.

evidence artifact

A preserved record demonstrating that a control operated: screenshots, exports, tickets, approval records, logs, attestations, or equivalent. Controls name the fields their evidence artifacts should capture.

evidence core

The two or three evidence fields carried in a control's evidence_core: the reference evidence set scoring levels 2-3 require, satisfiable by documented organization-defined equivalents per the conventions. The fuller field lists in implementation guidance inform level-4 verification depth.

executive-protection extension

A planned companion artifact covering personal, household, and physical-safety practices that sit outside organizational evidence governance. Routes to executive-protection extensions mark that boundary; until the extensions are published, FA4 retains ownership of the organization-relevant remainder.

exposed condition

The factual public state a finding describes, such as a reachable administrative interface or a published personal phone number, recorded separately from the abuse paths it enables.

high-risk role

A role whose authority, access, visibility, or support function makes its compromise disproportionately damaging: executives, executive assistants, finance approvers, HR, legal, help desk, administrators, and incident responders are common examples. Organizations maintain their own roster (FA2.SC1.C5).

honeytoken

A credential-like or data-like artifact with no real access or value, placed so that any use of it raises an alert. A honeytoken is one kind of canary signal; authorization is governed by FA5.SC4.C1.

mapping pack

A planned sidecar artifact publishing curated control-level mappings between ODSF and one external standard, versioned and source-pinned independently of the framework. The framework itself carries only category-level orientation alignment (see alignment_note). Applicability of mappings is governed by FA5.SC6.C2.

out-of-band verification

Confirming a request through a channel independent of the one the request arrived on, using contact details from an approved directory rather than details supplied in the request (FA2.SC2.C1).

reference cadence

A default frequency named in guidance for an inherently periodic control. Organizations may substitute a documented equivalent cadence.

residual risk

The risk remaining after remediation, compensating controls, or a documented decision not to act. ODSF requires residual risk to be recorded with an owner and review date, and surfaced in board or auditor reporting where material.

satisfied by reference

The routing convention by which the owning program's records satisfy a routed control's evidence expectation; the routed control records the pointer rather than a duplicate ledger.

PsySecure

OPEN FRAMEWORK

BUILT TO BE ADOPTED, ADAPTED, AND SHARED.

The OSINT Defense & Security Framework is published under Creative Commons Attribution 4.0. The canonical JSON, the current edition, and the changelog live at the framework home.

01	**Digital Footprint Reduction**
02	**Social Engineering Defense**
03	**Technology Exposure Management**
04	**Executive Exposure Protection**
05	**Continuous Monitoring and Response**

Download the canonical JSON and the current edition at **psysecure.com/odsf.**

Version 0.3.0 · Public Draft