

Shadow IT: the silent threat inside your ISMS

Finding, assessing, and governing the tools and services your people adopt without approval

ISO/IEC 27001:2022 · NIST CSF 2.0 · CIS CONTROLS v8.1 · WHITEPAPER

General educational guidance for building your own approach, not affiliated with or endorsed by any standards body or vendor named, and not legal or compliance advice. Adapt it to your context and obligations. Published 2026-09-10.

3 frameworks it maps to

Controls in ISO/IEC 27001:2022 and CIS Controls v8.1, and the matching NIST CSF 2.0 outcomes

14 items on the adoption checklist

from the asset inventory to a standing risk entry

01 What Shadow IT is

Shadow IT is any system, tool, or service that people use for work without going through approval or a security review. It usually starts with someone trying to get the job done, and it leaves a set of systems the Information Security Management System (ISMS) does not cover.

Common forms

- A team signs up for a cloud storage or collaboration app to share files, sometimes with customer data.
- A developer or engineer spins up a virtual machine, database, or service in a cloud account, outside the normal build and configuration process.
- A department adopts a SaaS platform (software the organization rents and reaches over the internet) or external vendor that never went through supplier or security assessment.
- An employee uses an unsanctioned AI assistant or chatbot for work and pastes confidential data into it, where it may be retained or used to train the provider's models.
- A user grants a third-party app or browser extension broad access to corporate accounts.
- An employee keeps work files in a personal account on a service the organization otherwise approves.

02 Why it undermines an ISMS

Blind spots in risk management

A system nobody has recorded is never risk-assessed, so its vulnerabilities and misconfigurations go unnoticed. People also put sensitive information into those tools, which breaks the classification and handling rules the ISMS sets.

No support and no tested recovery

A system the business comes to depend on has no backup anyone has checked, no support the organization has contracted for, and no recovery route anyone has written down. The organization finds that out when the system fails.

Fragmented controls

Tools used outside approved environments often lack the access management, encryption, and logging the organization relies on, which leaves gaps in monitoring and incident response.

An inventory and scope that fall behind

Every unrecorded system is one more thing the asset inventory and the ISMS scope leave out. Risk assessment and audit evidence both rest on that inventory being accurate.

03 The risks that are easy to overlook

Each of these outlives the sign-up that created it.

Data residency and cross-border transfer

CHECK WHERE THE DATA IS STORED AND WHO CAN REACH IT

An unsanctioned SaaS tool may store personal data outside the EEA. Under the GDPR, Chapter V allows that only where the destination has an adequacy decision, the transfer carries appropriate safeguards such as standard contractual clauses, or a derogation applies. Someone has to pick one of those routes and record it, and nobody does that for a tool the organization does not know about.

A tool the organization never contracted with also has no processing contract, which Article 28(3) requires and Article 28(9) requires to be in writing, and sits outside the record of processing Article 30 requires of most organizations. A breach in it is notifiable unless it is unlikely to risk anyone's rights and freedoms, and the 72 hours in Article 33 run from the controller becoming aware, so on a shadow tool the clock starts when someone finds out.

Storage region is one half of the question. Where the provider's staff outside the EEA can open the data to give support or fix a fault, that access is itself a transfer, so a tool hosted in an EU region can still need one of those routes. Whether the GDPR reaches you depends on your data and markets, and other regimes set their own rules. Check where a tool stores data, and who can reach it from where, before it holds anything sensitive.

OAuth grants and third-party app access

A PASSWORD RESET DOES NOT REVOKE IT

When a user grants OAuth permissions to an external app such as an AI assistant or meeting bot, the app gains persistent, token-based access to corporate data. Where the app calls the cloud provider's API from its own servers, the traffic never crosses your network, so network monitoring does not see it. Resetting the user's password does not remove the grant, and whether it revokes the app's existing tokens depends on the platform, on what kind of app it is, and on how the reset was done; even where they are revoked, the app regains access at the user's next sign-in.

Withdraw the grant itself. Where an administrator consented for the whole organization, no password reset touches the consent itself, and an administrator has to remove it.

Browser extensions work differently: the browser grants their permissions when the extension is installed, or later if the extension asks for more, and removing the extension takes them away. Where the extension also signed in to a cloud account, it holds a grant on that account that the uninstall does not touch, so check the account's

connected apps as well. A meeting bot also records the meeting, which several US states allow only with every participant's consent, so the organization's rules on recording apply to it before the access question does.

Orphaned access at offboarding

THE LEAVER PROCESS DOES NOT REACH THEM

When someone leaves, their access to shadow systems can outlive their last day, because those systems were never part of the joiner-mover-leaver process, which grants, changes, and removes access as people arrive, move roles, and leave. The leaver checklist has to work from the discovery inventory as well as the asset register.

License, cost, and contract exposure

DUPLICATE SPEND AND UNREVIEWED TERMS

Duplicate or unmanaged subscriptions waste budget, and a click-through sign-up can commit the organization to terms no one reviewed. Where people add seats under a volume license agreement that reconciles once a year, such as a Microsoft Enterprise Agreement, those seats are counted and invoiced at that annual reconciliation (the true-up), which can fall up to a year after the seats were added.

04 Framework alignment

Managing Shadow IT draws on several controls at once, which is useful when you need to justify the work or show it to an auditor.

WHAT YOU ARE DOING	ISO/IEC 27001:2022 ANNEX A	NIST CSF 2.0	CIS CONTROLS v8.1
Inventory every asset, including the unmanaged ones	5.9 Inventory of information and other associated assets	ID.AM-02, ID.AM-04	1.1, 1.2, 2.1, 15.1
Classify and protect the data that lands in them	5.12 Classification of information	ID.AM-05, ID.AM-07, PR.DS-01, PR.DS-02	3.2, 3.3, 3.7
Check where the data goes and which law applies	5.31 Legal, statutory, regulatory and contractual requirements; 5.34 Privacy and protection of personal identifiable information (PII)	GV.OC-03, ID.AM-03	3.1, 3.8
Assess, contract, monitor, and exit external providers	5.19 Information security in supplier relationships; also 5.20, 5.21, and 5.22	GV.SC-04, GV.SC-05, GV.SC-06, GV.SC-07, GV.SC-10	15.2, 15.4, 15.5, 15.6, 15.7
Govern how cloud services are adopted	5.23 Information security for use of cloud services	GV.SC-06, ID.AM-04	2.3, 15.1, 15.2

WHAT YOU ARE DOING	ISO/IEC 27001:2022 ANNEX A	NIST CSF 2.0	CIS CONTROLS v8.1
Restrict who can deploy, configure, or grant app access	5.15 Access control; 5.18 Access rights; 8.2 Privileged access rights; 8.3 Information access restriction	PR.AA-05	5.4, 6.1, 6.2, 6.8
Set the policy and train people to it	5.1 Policies for information security; 6.3 Information security awareness, education and training	GV.PO-01, PR.AT-01	14.1
Detect unmanaged systems and act on them	8.16 Monitoring activities	DE.CM-01, DE.CM-03, DE.CM-06, DE.CM-09, ID.RA-07	1.2, 1.3, 1.5, 2.3, 2.4, 15.1

ISO/IEC 27001 reaches Shadow IT through its own requirements. Clause 8.1 requires the organization to control externally provided processes, products, and services that are relevant to the management system, which covers a tool nobody sanctioned. Clauses 6.1.2 and 6.1.3 set the risk assessment and treatment process, and clause 8.2 (Information security risk assessment) has that assessment repeated at planned intervals and whenever a significant change is proposed or occurs. Clauses 9.3 and 10 carry the result into management review and improvement.

NIST CSF 2.0 covers the same ground in ID.RA-07 (changes and exceptions are managed, assessed for risk impact, recorded, and tracked). CIS Controls v8.1 scopes its discovery safeguards to assets on the network and to installed software, so Section 06 pairs them with the identity provider's inventory.

Control numbers and titles reflect the published standards; confirm the exact wording against the source before quoting it in a certification document.

05 Managing Shadow IT within an ISMS

The aim is to bring tools into view and under governance without taking away the ones people rely on.

Start with visibility

Identify the systems in use and pull them into your risk assessment. Section 06 covers where to look, because no single tool sees all of it.

Assign ownership

Give every system and service a named owner who is accountable for it, so nothing sits in a gap between teams.

Enforce least privilege

Under the principle of least privilege, people get the access their work needs and no more. Limit who can deploy or configure new services, especially in cloud accounts, so a new system cannot appear without someone entitled to create it. Limit who can grant a third-party app access to company accounts as well, and route those requests through the same approval route new tools go through.

Set a clear policy, and train to it

State how new tools are introduced and approved, and back it with awareness training so people understand both the process and why it exists.

Track it as an ongoing risk

Record Shadow IT in the risk register with a named risk owner, who approves the treatment plan and accepts whatever risk is left, and review it in management meetings. Fold it into the continual-improvement cycle so it stays a managed item rather than a one-off cleanup.

Make the sanctioned path the easy path

PEOPLE GO AROUND A SLOW APPROVAL ROUTE

NIST SP 800-124r2 records three causes: staff turn to Shadow IT when the systems and processes they are given are seen as cumbersome or as impeding work, when the organization does not provide a system they need, or when the way the organization administers its systems looks to them like an intrusion on their privacy.

A fast, simple way to request and approve a new tool answers the first, hearing what people asked for answers the second, and telling people plainly what the discovery in Section 06 collects answers the third. Combine that with discovery and assessment, and new tools get recorded and assessed as they appear.

06 Finding what is in use

Network monitoring finds most SaaS reached from your network, and four things stay outside what it shows.

Where network monitoring falls short

Firewall and proxy logs show which cloud service a request went to, and CASB discovery reads exactly those logs, so finding the app takes no TLS inspection. What stays hidden is what was sent into it, cloud-to-cloud OAuth grants that never touch your network, SaaS reached from an employee's home or phone, and a resource created inside a cloud account you already sanction, which looks like traffic to a destination you allow.

The combined approach

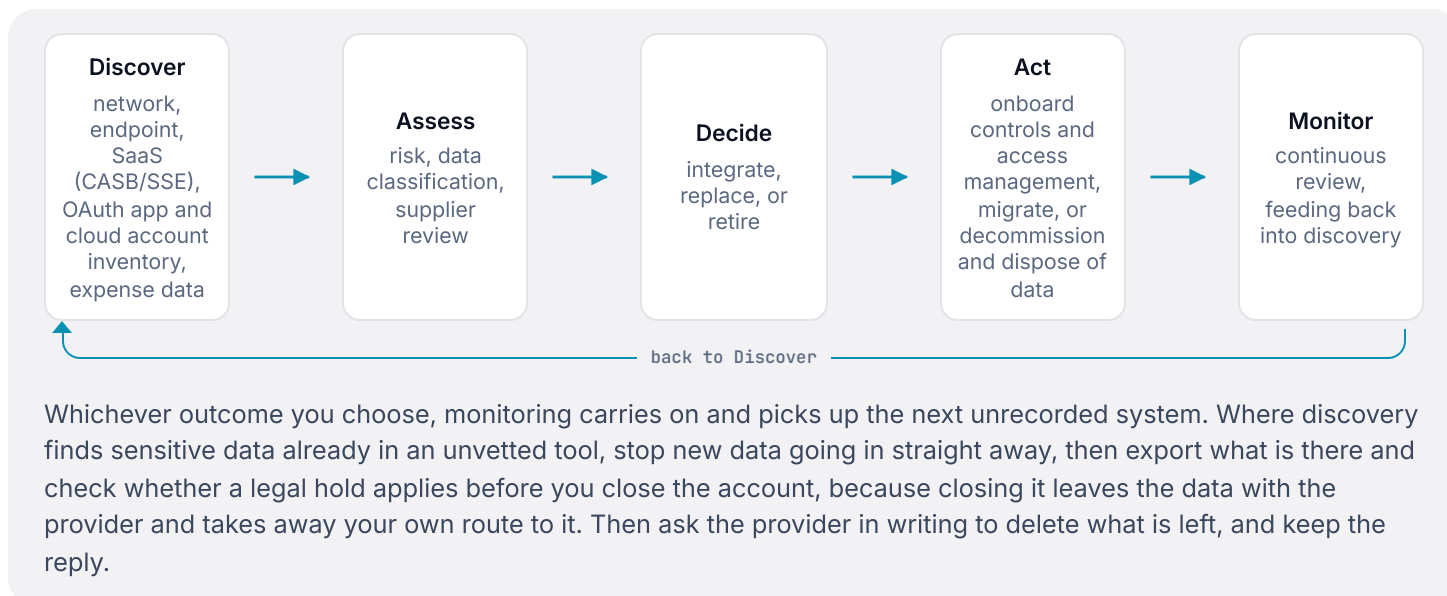
Pair network monitoring with four other sources: endpoint agents, a Cloud Access Security Broker (CASB), your identity provider's OAuth and SaaS app inventory, and your cloud providers' own asset and billing inventories. An endpoint agent can report both the software installed on a device and the cloud services it reaches off the network. A CASB is increasingly delivered inside a broader Security Service Edge (SSE) platform.

The identity provider's inventory is where AI assistants, meeting note-takers, and other agents with standing access show up, because they hold a grant rather than a network path. Of these, only the cloud providers' inventories show a resource someone created inside a sanctioned cloud account.

None of them shows a subscription paid for outside those accounts, so read the expense and card data as well, alongside the sign-up confirmations and invoices arriving in corporate mailboxes.

07 The Shadow IT lifecycle

Shadow IT starts when someone has a need the approved tools do not meet, and the workaround takes data and access outside governance. The response runs as a continuous loop: discover, assess, decide, act, monitor, and back to discover.



08 Quick adoption checklist

A short self-check you can lift into your own ISMS. Most items trace to a control in Section 04. The license and cost checks are commercial, the notice item is a legal duty, and the AI item follows the organization's own AI use policy.

- The asset inventory includes sanctioned tools and any unsanctioned ones you have discovered.
- Every system and service has a named owner.
- Least privilege is enforced for cloud subscriptions and deployment roles.
- User consent to third-party apps is restricted in the identity provider, with a request-and-approve route for the ones that should be allowed.
- A standard, fast request-and-approval path exists for new tools and vendors.
- The policy on adopting new tools is written down, and awareness training covers both the process and why it exists.
- People are told what the discovery collects, in writing where a monitoring law requires it.
- Every external service goes through a supplier security assessment before onboarding.
- License, cost, and contract terms are reviewed for external subscriptions.
- Continuous discovery is in place across every source in Section 06, including the expense and card data.
- Data residency, cross-border transfer, and a written processing contract are checked for each external service.
- Offboarding covers shadow accounts and revokes OAuth and app grants alongside the usual password reset.
- Approved AI tools are named on the organization's approved-tools list, with provider training on the organization's data switched off where the provider offers the setting.
- Shadow IT is tracked as a standing risk with a named risk owner, defined treatment actions, and a review cadence.

REF References

ISO/IEC 27001:2022, Information security, cybersecurity and privacy protection - Information security management systems - Requirements · [iso.org/standard/27001](https://www.iso.org/standard/27001)

NIST Cybersecurity Framework (CSF) 2.0, NIST CSWP 29 · doi.org/10.6028/NIST.CSWP.29

CIS Critical Security Controls, Version 8.1, Center for Internet Security · cisecurity.org/controls. Refer to cisecurity.org/controls for the current version of the CIS Controls.

Regulation (EU) 2016/679 (GDPR), Chapter V (Articles 44-50) · eur-lex.europa.eu/eli/reg/2016/679/oj

EDPB Guidelines 05/2021 on the Interplay between Article 3 and Chapter V of the GDPR, Version 2.0, adopted 14 February 2023 · edpb.europa.eu/our-work-tools/our-documents/guidelines/guidelines-052021-interplay-between-application-article-3_en

NIST SP 800-124 Rev. 2, Guidelines for Managing the Security of Mobile Devices in the Enterprise (May 2023), Section 3.1.13 · doi.org/10.6028/NIST.SP.800-124r2

Gartner glossary: Security Service Edge (SSE) · gartner.com/en/information-technology/glossary/security-service-edge-sse

Gartner glossary: Cloud Access Security Broker (CASB) · gartner.com/en/information-technology/glossary/cloud-access-security-brokers-casbs

Microsoft Learn: Cloud app discovery overview · learn.microsoft.com/defender-cloud-apps/set-up-cloud-discovery

Microsoft Learn: Detect and remediate illicit consent grants · learn.microsoft.com/defender-office-365/detect-and-remediate-illicit-consent-grants

Microsoft Learn: Refresh tokens in the Microsoft identity platform · learn.microsoft.com/entra/identity-platform/refresh-tokens

Microsoft Learn: Configure how users consent to applications · learn.microsoft.com/entra/identity/enterprise-apps/configure-user-consent

Google Workspace Admin Help: Control which apps access Google Workspace data · knowledge.workspace.google.com/admin/apps/control-which-apps-access-google-workspace-data

Chrome for Developers: Declare permissions · developer.chrome.com/docs/extensions/develop/concepts/declare-permissions

Microsoft: Enterprise Agreement licensing guidance · microsoft.com/licensing/guidance/Enterprise-Agreement