anoBytes | TECHNOLOGY SOLUTIONS

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 legal or compliance advice. Adapt it to your context and obligations. Published 2026-07-19.

3 frameworks it maps to

ISO/IEC 27001:2022, NIST CSF 2.0, and CIS Controls v8.1 each address it directly

10 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 good intentions, someone trying to get the job done, and the result is 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 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.

02 Why it undermines an ISMS

When security does not know a system exists, it cannot assess it, so its weaknesses and compliance gaps stay invisible. People will always reach for tools that help them get the work done, and the ones that never get recorded are the ones no one assesses.

Blind spots in risk management

A system nobody has recorded is never risk-assessed, so its vulnerabilities and misconfigurations go unnoticed. Sensitive data can also drift into unmanaged places, breaking the classification and handling rules the ISMS sets.

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.

A drifting inventory and scope

Every unrecorded system pulls the asset inventory and the ISMS scope further from reality. Risk assessment and audit evidence both rest on that inventory being accurate.

03 The risks that are easy to overlook

Four risks sit behind the obvious exposure.

Data residency and cross-border transfer

WHERE THE DATA LANDS IS A LEGAL QUESTION

An unsanctioned SaaS tool may store data in a jurisdiction that breaches a data-protection regime such as the GDPR, whose Chapter V governs transfers of personal data outside the EU and EEA. Whether that regime applies depends on your data and markets. Either way, the storage location has to be checked before the tool 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, or installs a browser extension with broad scopes, that app gains persistent, token-based access to corporate data. Resetting the user's password does not revoke it; the grant and its refresh tokens have to be withdrawn explicitly. Because the app reaches the data through the cloud provider's API, the access is also largely invisible to traditional network monitoring.

Orphaned access at offboarding

YOU CANNOT DEPROVISION WHAT YOU DO NOT KNOW EXISTS

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.

License, cost, and contract exposure

DUPLICATE SPEND AND UNREVIEWED TERMS

Duplicate or unmanaged subscriptions waste budget and create true-up risk at renewal, and a click-through sign-up can commit the organization to terms no one reviewed.

04 Framework alignment

Managing Shadow IT draws on several controls at once, which is useful when you need to justify the work or evidence it to an auditor. The mapping below is to the current published versions of three widely used frameworks.

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	3.2
Assess and contract external providers before use	5.19-5.22 Supplier relationships	GV.SC-04, GV.SC-06	15.1
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
Restrict who can deploy or configure	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
Detect unmanaged systems and activity	8.16 Monitoring activities	DE.CM-01, DE.CM-03, DE.CM-06, DE.CM-09	1.2, 2.3

Underneath these controls sits the management-system duty to treat Shadow IT as a tracked, reviewed risk: that runs through the ISO/IEC 27001 risk process (Clauses 6.1.2-6.1.3, 9.3, and 10) and NIST CSF 2.0's ID.RA-07 (changes and exceptions are managed and assessed for risk). 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. Five practices do most of the work.

Start with visibility

Identify the systems in use and pull them into your risk assessment. You cannot protect, classify, or offboard something you have never recorded.

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.

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, review it in management meetings, and 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

THE MOST EFFECTIVE CONTROL IS OFTEN A FAST APPROVAL PROCESS

Shadow IT usually appears because the approved route is too slow. A fast, low-friction way to request and approve a new tool removes the incentive to go around governance in the first place. Combine that with discovery and assessment, and new tools get recorded and assessed as they appear.

06 Finding what is actually in use

Network monitoring has three blind spots for discovery, and closing them takes more than one tool.

Where network monitoring falls short

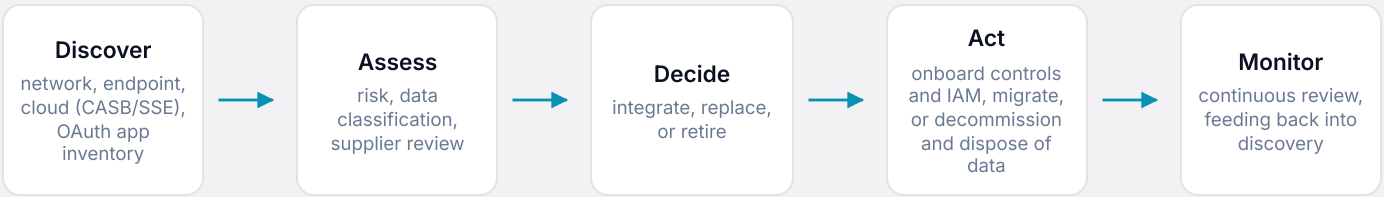
It cannot see inside encrypted SaaS sessions, it misses cloud-to-cloud OAuth grants that never touch your network, and it does not see SaaS reached from an employee's home or phone.

The combined approach

Pair network monitoring with endpoint software inventory, a Cloud Access Security Broker (CASB, increasingly delivered inside a broader Security Service Edge platform), and your identity provider's OAuth and SaaS app inventory. Together these show what is genuinely in use, on the network and off it.

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.



The decision has three outcomes: integrate the tool under proper controls, replace it with an approved alternative, or retire it and dispose of the data. Whichever you choose, the system then feeds continuous monitoring, which surfaces the next round.

08 Quick adoption checklist

A short self-check you can lift into your own ISMS. Each item maps to the controls in Section 04.

- 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.

- A standard, fast request-and-approval path exists for new tools and vendors.
- Supplier security assessment is performed before onboarding an external service.
- License, cost, and contract terms are reviewed for external subscriptions.
- Continuous discovery is in place across network, endpoint, cloud (CASB/SSE), and OAuth or SaaS app inventory.
- Data residency and cross-border transfer are checked for each external service.
- Offboarding covers shadow accounts and revokes OAuth and app grants alongside the usual password reset.
- Shadow IT is tracked as a standing risk with defined treatment actions and a review cadence.

REF References

ISO/IEC 27001:2022, Information security management systems, Requirements · 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 · cisecurity.org/controls

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

Gartner glossary: Security Service Edge (SSE) and Cloud Access Security Broker (CASB) · gartner.com/en/information-technology/glossary

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