Sentinelcore-Ai

WHITEPAPER · CLOUD



Continuous Multi-Cloud Governance for NIS2 and DORA

Why point-in-time audits fail in multi-cloud estates, and how to run cloud posture as a daily control that produces evidence auditors accept.

By Harsukh Singh

Eight years in security engineering, information security governance and identity

September 2026 · sentinelcore-ai.com

Free to share with attribution

EXECUTIVE SUMMARY

The audit is annual. Your cloud changes every hour.

Most European organisations now run workloads in more than one public cloud, plus SaaS, plus an identity provider that ties it all together. Compliance programmes, however, still tend to test cloud configuration once a year, with screenshots. That gap is where real incidents live: a storage bucket made public during a migration, a logging trail switched off to save cost, an admin account created without MFA for a weekend fix.

NIS2 and DORA both move the goalposts from *having* policies to *operating* controls and being able to show they work. This paper sets out a practical model for continuous multi-cloud governance: one control set across AWS, Microsoft Azure and Google Cloud; organisation-wide coverage with read-only access; daily scoring; and a direct line from each failing check to a corrective action and to the requirement it affects.

3	Daily	Read-only	1 → N
major clouds, one control set	posture measurement	access model	evidence reused across frameworks

What the regulations actually ask for

NIS2 (Directive (EU) 2022/2555)

Article 21 requires essential and important entities to take **appropriate and proportionate technical, operational and organisational measures**, based on an all-hazards approach. The minimum list in Article 21(2) includes risk-analysis and information-system security policies, incident handling, business continuity, supply-chain security, security in acquisition, development and maintenance (including vulnerability handling), policies to **assess the effectiveness** of those measures, basic cyber hygiene and training, cryptography, access control and asset management, and multi-factor authentication.

Article 20 makes management bodies responsible for approving and overseeing these measures, and requires them to follow training. Article 21(2)(f), effectiveness assessment, is the one that point-in-time audits struggle with most: showing that a control was in place on the day of the audit says little about the other 364.

DORA (Regulation (EU) 2022/2554)

DORA applies to EU financial entities from 17 January 2025. Its ICT risk-management framework (Chapter II) expects entities to identify ICT assets and their configurations, protect them, **continuously monitor** and detect anomalous activity, and document all of it. Chapter V adds explicit management of ICT third-party risk, which for most firms starts with their cloud providers.

ISO/IEC 27001:2022

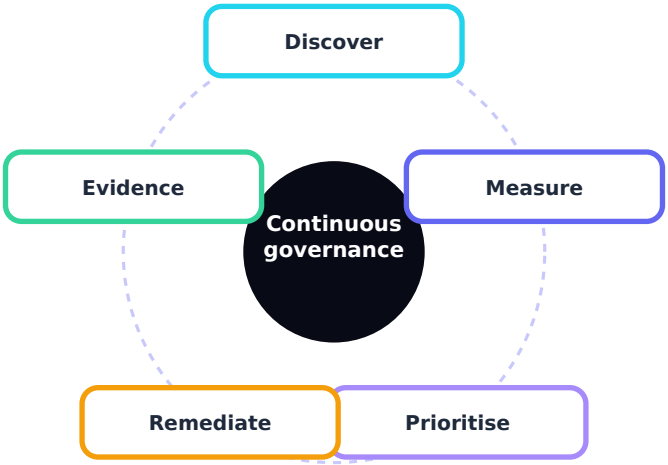
Annex A control 5.23 (information security for use of cloud services), 8.9 (configuration management), 8.16 (monitoring activities) and 8.15 (logging) are the natural anchors for cloud posture evidence, with 5.15 and 8.5 covering access control and secure authentication.

> **The common thread**
> None of these texts prescribe a specific tool, but all three reward the same thing: a defined control set, measured continuously, with documented follow-up when a control fails.

Why multi-cloud breaks the annual audit

- **Scale.** Organisations commonly run dozens of AWS accounts, Azure subscriptions and Google Cloud projects. Sampling a handful tells you little about the rest.
- **Velocity.** Infrastructure-as-code and self-service portals mean configuration changes daily. A screenshot is stale by the time it is filed.
- **Different vocabularies.** A public S3 bucket, a publicly readable Azure blob container and an allUsers binding on a Cloud Storage bucket are the same risk under three names.
- **Ownership drift.** New accounts and projects appear outside the central team's view, often created for a proof-of-concept that quietly becomes production.
- **Evidence overhead.** The same control is evidenced separately for ISO 27001, NIS2, DORA and SOC 2, multiplying the work without improving security.

A model for continuous cloud governance



1. Discover everything, with least privilege

Coverage is the first control. Connect at the top of each cloud's hierarchy so new accounts are included automatically, and use read-only roles designed for security auditing:

Cloud	Scope	Read-only access pattern
AWS	Every account in the Organization	A role such as SecurityAudit + ViewOnlyAccess deployed to member accounts (e.g. via a StackSet), assumed from a central account with a per-customer external ID
Microsoft Azure	Every subscription under a management group	An app registration with Reader and Security Reader assigned at the tenant-root or a parent management group
Google Cloud	Every project in the organisation or folder	A service account with Viewer and Security Reviewer granted at organisation or folder level

> **Why the external ID matters**
> When a SaaS platform assumes a role in your AWS accounts, a unique external ID in the role's trust policy prevents the 'confused deputy' problem: another customer of the same platform cannot trick it into using your role.

2. Measure with one control set

Normalise the three clouds into one set of checks, each mapped to the control it evidences. A practical baseline covers identity (MFA for privileged users, no long-lived root or owner keys, stale access), data (public storage, encryption at rest, key management), network (open management ports, default network rules), logging (audit trails enabled in every region, retention, export to a central store) and threat detection (the provider's native service turned on).

Score each account as the share of checks passing, with warnings counted as half, and roll accounts up per provider and for the organisation. The absolute number matters less than the trend: a score that drops overnight is a change worth investigating.

3. Prioritise across clouds, not within them

The same failing check in forty accounts is one decision, not forty tickets. Group findings by check across every account and provider, show which accounts are affected, and rank by severity and by the number of requirements each failure touches. This keeps the remediation queue short and makes systemic problems, such as a landing-zone template that omits logging, visible.

4. Remediate with an owner and a date

Every failing high-severity check should open a corrective action automatically, with the affected resources, a recommendation, an owner and a due date. When a later scan shows the check passing, the action can be closed with the scan as evidence. This is what turns monitoring into the effectiveness assessment Article 21(2)(f) asks for.

5. Evidence once, reuse everywhere

Because each check is mapped to ISO 27001 Annex A, the same result can be cross-mapped to NIS2 Article 21 measures, DORA articles, SOC 2 criteria and GDPR Article 32. Auditors increasingly accept system-generated, time-stamped results with a history in place of screenshots, provided the method is documented and the data cannot be edited by the auditee.

Practical pitfalls

- **Tenant-wide checks counted N times.** Identity-provider settings apply once per tenant; don't repeat them for every subscription or they will dominate the score.
- **Scanning only the connected account.** Coverage should be explicit: list which accounts were scanned, which were skipped and why (for example, a role that could not be assumed).
- **Treating a scan failure as a pass.** If a check cannot run because of missing permissions, report it as 'unknown', never as passing.
- **No change history.** Keep at least 90 days of results so you can show when a control failed and how quickly it was fixed.

Getting started: a 30-day plan

- ☐ Week 1: inventory every cloud tenant, organisation and billing account; agree a single owner per cloud.
- ☐ Week 1: create read-only audit roles at the top of each hierarchy; record the access model in your ISMS.
- ☐ Week 2: run a first organisation-wide baseline; publish the score and top ten cross-cloud issues to management.
- ☐ Week 3: turn on daily scans and automatic corrective actions for high-severity failures.
- ☐ Week 4: map checks to your frameworks, retire screenshot evidence, and brief your auditor on the method.

How Sentinelcore-Ai helps

Sentinelcore-Ai's Cloud Posture hub scans AWS, Azure and Google Cloud across every account, subscription and project, plus connected identity and endpoint tools, daily or weekly. It shows one score with a 90-day trend, de-duplicates the same issue across accounts, maps each check to ISO 27001, NIS2, DORA, SOC 2 and GDPR, and opens corrective actions automatically. Assessments can reuse the latest results instead of rescanning.

References

Directive (EU) 2022/2555 (NIS2), Articles 20–21 · Regulation (EU) 2022/2554 (DORA), Chapters II and V · ISO/IEC 27001:2022, Annex A · CIS Benchmarks for AWS, Microsoft Azure and Google Cloud Platform · AWS documentation on cross-account roles and external IDs.

About the author

Harsukh Singh has spent eight years in hands-on cybersecurity work across security engineering, information security governance, and identity and access management. That work has meant building and running information security management systems to ISO/IEC 27001:2022, auditing them against the standard, and designing identity and access controls on Microsoft Entra ID, from conditional access and privileged roles to access reviews. Harsukh founded Sentinelcore-Ai to give security and compliance teams the tooling that work called for: posture measured against vendor baselines, findings tied to risks and corrective actions, and evidence an auditor can follow.