Deep InfoSec LTD

71-75 Shelton St, London, UK
sales@deepinfosec.com | www.deepinfosec.com

OSPCRM-ACCREDITED

Accréditation ONPC - RDC **Ordre National des Professionnels de la Cybersécurité RDC**	**IGS-C** **International Governance & Security Standards Council**	**PASC** **Pan African Security & Strategic Council**
ONPC-ORG-2025-DDKZAEZD22	**IGS-ORG-ZEFER512EZ01**	**PASC-OSPCRM-SOL-2025-0002**

Prepared by:
Research Dpt
Ref /Peer reviewed paper: https://doi.org/10.5281/zenodo.17735625

26 nov. 2025

Deep InfoSec – Brief for CISOs, CIOs & Heads of Risk

Identity Everywhere, Owned by No One

Restoring Accountability In Federated, Multi-Cloud and Multi-Regulated Environments

Deep InfoSec · Board-Level Briefing

1. Why boards should care now

Your organisation probably has:

- Single sign-on for staff and partners
- One or more cloud identity providers
- Federated access to SaaS, vendors and robots

On slides this looks centralised. In incidents it is not.

When we investigate real outages and breaches, the most dangerous access paths rarely live inside a single directory or tenant. They sit in the seams between:

- On-prem AD and cloud IdPs
- IdPs and SaaS admin roles
- Internal identities and vendor or contractor accounts
- Human users and "temporary" robots that became permanent

Each team controls one segment and feels reasonably safe. Nobody owns the full chain. That is where attackers and failures live.

For a board, this creates three hard truths:

1. Identity risk is no longer a single system risk. It is a **chain risk** across vendors, clouds and jurisdictions.
2. Regulations still assume clear ownership, even when your identity reality does not.
3. Dashboards that show "MFA coverage" and "number of privileged accounts" hide the real problem: **who signs for the full path that can break a critical**

---

service, and can they cut that path fast.

---

2. What we see in the logs

Deep InfoSec has processed more than one million anonymised identity events and change records since 2018 across:

- Banks, insurers and payment providers
- Hospitals and health networks
- Universities and research platforms
- Critical infrastructure and public services

The clients are highly regulated; the sample is not random. It is exactly where identity mistakes have serious consequences.

Across this base, three patterns repeat.

2.1 High-risk identities live in the seams

When we map "who can really break or corrupt this service" we often find:

- More than half of the truly dangerous paths cross at least one federated boundary.
- Robots, vendor accounts and "temporary" exceptions appear again and again.
- Human accounts become dangerous over time through layers of exceptions and migrations, not at creation.

Central identity tools show neat diagrams. The real blast radius sits between them.

2.2 Federation adds delay where you can least afford it

Every organisation claims to have joiner-mover-leaver processes. Federation stretches them.

- HR or the primary directory changes first.
- Cloud IdPs lag behind.
- SaaS admin roles lag even further.

- Robots and scripts may never update at all.

The result: real deprovisioning for a high-impact account often takes **hours or days**, while leadership believes it takes minutes. Attackers need the lag, not the full system.

2.3 Nobody feels fully responsible for the chain

Federation simplifies the sign-in experience, which reassures people. One login. One portal. One IdP logo. It looks like one owner.

In reality:

- Each team owns only a segment.
- Vendors own key segments that sit outside your legal jurisdiction.
- Emergency backdoors and support flows live in a grey zone "between" contracts.

When something goes wrong, everyone explains their part. Very few people feel fully responsible for the combined effect.

---

3. The Sovereign Federation Baseline (SFB) in one page

Boards and regulators do not need another 200-page framework. They need a thin baseline that sits **above** tools and vendors.

Deep InfoSec uses the **Sovereign Federation Baseline**:

3.1 Five rules

1. **Every federated path has a named sovereign owner**
   For each critical service, the full identity chain is documented end-to-end. One senior owner signs for the entire chain, not only their local system.

2. **Every critical service has a bounded identity radius**
   The organisation knows exactly which identities (human, robot, vendor, emergency) can administer, shut down or exfiltrate from that service. The list is

short, justified and reviewed.

3. **Federation contracts are security contracts**
   Every federated link that matters for critical services includes: log access, retention, right to share with regulators, a defined kill-switch and clear jurisdiction terms.
4. **Emergency and backdoor paths are tested and reversible**
   Break-glass accounts and vendor backdoors exist only if they can be rehearsed safely and rolled back on demand. Unrehearsed backdoors are treated as critical findings.

5. **No high-impact identity without a living owner**
   For each dangerous identity chain there is a named person responsible, visible in crisis plans and exercises.

3.2 Three tests any board can demand

These tests require courage, not new tools.

1. **Kill-switch in ten minutes**[1]
   Pick one critical service. Ask the CISO to demonstrate how the organisation can cut **all** identity paths that administer or disable that service in ten minutes or less, across IdPs, SaaS and vendor paths. If this requires meetings with multiple vendors, the kill-switch does not exist.
2. **Propagation reality check**
   Take one high-impact account. Trigger a change at the source of truth. Measure how long it takes until all federated platforms reflect it. Compare real numbers to what you have been told in risk presentations.
3. **Owner in the room**
   In an executive or risk committee session, show a simple diagram of a critical service and its identity chain. Ask: "Who is accountable for this full chain?" and "Who speaks for each segment in a crisis?" If the room hesitates, ownership is missing.

[1] n some environments (global card schemes, certain utilities with government golden keys) it is closer to 30–60 minutes

4. How regulators and supervisors will read this

Regulations in Europe, Africa and elsewhere do not talk about IdPs and federation in detail. They talk about:

- Governance and accountability for critical and important functions
- Control over outsourced and ICT third-party providers
- Traceability of incidents, logs and decision making
- Data protection across controllers and processors

In a federated world, you still need to tell a convincing story:

> "For each critical service, we can show who owns the identity chain, how many identities can really break it, how quickly we can cut those paths, and how this aligns with local and cross-border obligations."

Deep InfoSec translates the SFB into regulatory language using open, vendor-neutral standards:

- **PASC**: Pan-African governance and cyber standards anchored in measurable controls.
- **IGS-C**: Multi-regional governance alignment that helps you talk to European and African supervisors with a single narrative.
- **OSPCRM**: A risk and resilience standard that connects identity chains to critical function, third-party and operational resilience requirements.

The same SFB work you do internally becomes your story for DORA, NIS2, AU conventions, national laws, SADC / EAC guidance and sector regulators.

5. What this means for your next board or CISO conversation

You do not need to become an identity engineer. You need to ask questions that force clarity.

Suggested questions for your next session:

---

1. **"Show me one critical service and the full identity chain that can break it. Who owns that chain?"**
2. **"How many identities, including robots and vendors, can administer or shut down that service today?"**
3. **"If one of those identities goes rogue or gets compromised on a Friday night, how long before we can cut every path?"**
4. **"Which of our federation contracts give us the logs and kill-switch we need to satisfy our regulators?"**
5. **"Who will stand in front of the supervisor and explain this chain calmly after an incident?"**

If your CISO cannot answer these with confidence, the issue is not a missing feature. It is a missing baseline.

---

6. How Deep InfoSec helps

Deep InfoSec does not sell another IdP or dashboard. We act as the **sovereign engineering arm** for organisations that want to regain control over identity in federated, multi-cloud and multi-regulated environments.

In practice we:

- Map real identity chains for your most critical services across on-prem, cloud, SaaS and vendors.
- Apply the **Sovereign Federation Baseline**: five rules, three tests, one ownership model.
- Reduce the identity radius and remove dangerous backdoors without breaking operations.
- Align the outcome with PASC, IGS-C and OSPCRM so you can speak to supervisors with a single story.
- Provide an AI-assisted view through the Deep Advisor platform that stays explainable and auditable.

Our track record over the last seven years: every client that applied this approach has avoided repeat identity-driven crises on the same service. Not because we patched

faster than everyone else, but because we cut the path that made patching a constant race.