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.17735203

26 nov. 2025

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

1. The problem you actually face

Your identity stack is huge: AD/Entra, Okta, PAM, SSO, APIs, bots, containers, contractors, SaaS.
Yet every serious incident review says the same thing:

- The dangerous accounts **became** dangerous over time – they weren't born that way.
- Federation and "temporary" access hide the riskiest identities.
- Dashboards show **hundreds of controls**, but boards ask: "Are we safe?" and you still don't have a hard answer.

You don't need more features. You need a **thin, measurable identity baseline** that you can defend in front of regulators, auditors and your own board.

2. Deep InfoSec's SIB: a thin, sovereign identity baseline

We work from one simple idea:

> *Reduce identity blast radius by prioritizing the attack-path.*

Our **Sovereign Identity Baseline (SIB)** reduces your identity posture to **three numbers your board can read in five minutes**:

1. **IBRI – Identity Blast Radius Index**
   How much damage can your top 1–5% of identities do if they go bad?
   - Privileged humans, service accounts, robots, break-glass, CI/CD pipes.
   - Includes federation and "shadow" identities created by automation.
2. **CHS – Credential Hygiene Score**
   How easy is it to steal or abuse those identities?
   - Keys, tokens, legacy auth, local admins, dormant accounts, over-privileged robots.
   - Penalizes age, reuse, weak rotation, opaque ownership.

3. **IRT – Identity Recovery Time**
   How long until you can take back control when something goes wrong?
   - Kill-switches, emergency playbooks, recovery tests, cloud/on-prem integration.
   - Measures **real** recovery, not paper plans.

These metrics are:

- **Regulation-agnostic**: we map them to NIS2, DORA, GDPR, sector rules, local laws.
- **Sovereign-aware**: they respect African/European data-location and supervisory constraints.
- **Vendor-neutral**: they sit on top of Entra, Okta, Ping, homegrown, PAM, Kubernetes, etc.

3. What changes in 90 days

A typical 90-day SIB engagement looks like this:

Days 0–15

- Connect to your existing telemetry and IAM (no rip-and-replace).
- Identify the **1–5% of identities** that drive **80% of catastrophic risk**.
- Deliver a **board-ready, 4-page pack**: IBRI/CHS/IRT, top attack paths, plain-language narrative.

Days 15–60 – Cut the blast paths

- Decommission or restrain unused and over-privileged identities.
- Fix federation and robot/service account sprawl where it matters.
- Tie each change to a **measurable drop** in IBRI/CHS/IRT.

Days 60–90 – Prove control

- Run attack-path simulations and recovery tests on critical services.

- Produce evidence for internal audit and regulators.
- Leave you with a **repeatable, 1-page quarterly identity report**.

Across seven years with banks, regulators, hospitals and industrial clients, **we have observed zero repeat incidents on remediated services when clients completed the full SIB remediation roadmap**. Not because threats disappeared, but because their **paths into their core systems were removed**.

4. Why boards and regulators like this

- **One language for everyone** – the same three numbers appear in CISO briefings, board packs and supervisory meetings.
- **Risk-appetite aware** – we tune thresholds to your own risk appetite instead of imposing a vendor magic number.
- **Audit-ready** – we give internal audit and external assessors concrete evidence: before/after identity maps, tracked decision logs, tested recovery times.
- **Sovereign & independent** – our methods align with **PASC**, **IGS-C** and **ONPC-RDC** standards and avoid lock-in to any single provider.

5. If you are a CISO / CIO reading this

You probably **don't** need:

- Another 80-page IAM slide deck.
- Another generic "zero trust" roadmap.
- Another compliance checklist for a new regulation.

You likely **do** need:

- **Three hard numbers** that you can defend in front of the board.
- A way to cut the **small set of identity paths** that can kill the bank / hospital / group.
- A practice that can safely modify live architecture**, not just write policies**.

6. Next step (low-friction)

Reply or write to **contact@deepinfosec.com** with:

- Your role
- Your biggest fear around identity
- Any major audit / regulatory deadline in the next 12 months

We will respond with a **concrete, 90-day SIB roadmap** and a short **board-ready sample pack** so you can see exactly what your leadership and regulators would receive.