

Cryptographic Risk:

The 30-Second CISO Kickstart

Encrypted doesn't mean secure, especially when cryptographic risk goes unmanaged. Think: expired certificates, deprecated algorithms, hardcoded keys, weak encryption.

No one owns cryptography, so no one sees the risks — until it's too late.

As CISO, you can't personally hunt every hidden risk. But you can make sure your team knows where to look, and what to look for.



THE CHALLENGE

Imagine waking up one morning to find your company's encrypted data...

exposed.

Quick-Start Checklist:

Cryptographic Visibility



Discovery



Inventory



Risk Reduction



Democratization



Resilience

While presented sequentially, progress often happens in parallel—especially when it comes to reducing critical risks.



Resilience is not an end state, but rather a continuous state of active management and adapting to change.

Phase

What To Do

Why It Matters

Discovery



Scan code, infrastructure, and network traffic for cryptographic use:

- Keys, certificates, protocols, algorithms, libraries
- Unencrypted flows, weak protocols
- Source code, CI/CD environments, endpoints, servers, third-party

Cryptography is everywhere — but often invisible

Inventory



Centralize findings in a living inventory:

- Map assets to applications, systems, and owners
- Track usage, compliance status, risk level

You can't manage what you can't see

Risk Reduction



Identify and prioritize high-risk issues:

- Hardcoded, reused, or exposed keys
- Expired or long-lived certificates
- Obsolete algorithms and cipher suites
- Unencrypted or weakly encrypted traffic
- Non-compliant or custom cryptography

Move from discovery to accountable action

Democratization

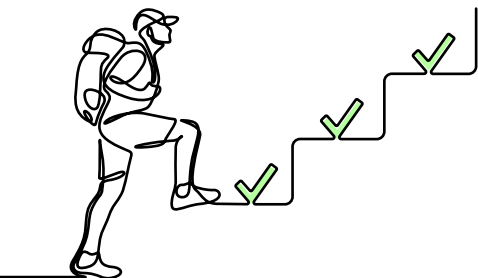


Embed cryptographic responsibility into workflows:

- Automate certificate and key management
- Provide clear policies and alerting
- Assign ownership across teams

Security improves when cryptography isn't a silo

Resilience



Build long-term crypto-agility:

- Automate renewals and key rotation
- Monitor for post-quantum readiness
- Review policies and responsibilities regularly
- Assign owners, track via ITSM/GRC/CMDB tools

Cryptographic standards evolve, so your response must too



Auditors expect clear answers

| Standards are shifting fast

| Complacency isn't an option

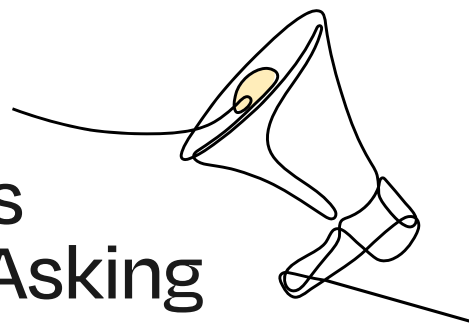
"What do we have?"

"What's hiding?"

"Is it secure and compliant?"

Tough Questions:

What CISOs Should Be Asking



These aren't technical questions, they're strategic ones. If your team can't answer them, you're exposed to operational, regulatory, and financial risk.

To Security Architecture & Engineering Leads

- Can we produce a current inventory of all cryptographic assets — and who owns them?
- Where are we still relying on insecure protocols or weak ciphers?
- Can we identify quantum-vulnerable algorithms in use today?



To PKI / Cryptography Stakeholders

- Are certificate expirations, key rotation, and algorithm usage actively tracked and enforced?
- How are we assessing our exposure to post-quantum threats?
- If we had an audit tomorrow, could we produce a complete cryptographic inventory?

To AppSec / DevSecOps Leaders

- Are secrets, certificates, and cryptographic libraries properly managed across the SDLC?
- Do development teams clearly understand what's approved — and what's not?
- Can we identify cryptographic dependencies in third-party or open-source components?

Final Word for the CISO

You don't need to be a cryptography expert — but you do need to lead the charge. Ask hard questions. Seek answers. Share this with your team. Start the conversation. Understand the risks.