2026

The SigmaSRC® Playbook

HOW A COMPANY CONDUCTS A FULL CRYPTOGRAPHIC INVENTORY

A Step-by-Step, Board-Defensible Approach

Prepared by: SigmaSRC

Version: 1.0

Date: January 2026

Why a Cryptographic Inventory Matters

You cannot manage quantum risk, compliance exposure, or "***harvest now, decrypt later***" threats without knowing exactly where encryption exists, how it's implemented, and what data it protects.

A cryptographic inventory answers five critical questions:

1. Where is encryption used?
2. What algorithms and key sizes are in use?
3. What data is being protected—and for how long?
4. Who owns and manages the cryptography?
5. How quickly can it be changed? (crypto-agility)

Phase 1. Establish Scope & Ownership (Week 1)

Assign Clear Ownership

This must be cross-functional, not just security.

Recommended owners:

- Executive Sponsor: CISO or CIO
- Program Lead: Security Architecture or GRC
- Contributors: IT, Cloud, App Dev, DevOps, Legal, Compliance, Vendor Management

SigmaSRC guidance: Treat this as an enterprise risk exercise, not a tool inventory.

Define What “Counts” as Cryptography

Include all forms, not just obvious ones:

- Data at rest encryption
- Data in transit (TLS, VPNs)
- Authentication and identity (certificates, keys)
- APIs and service-to-service encryption
- Backups and archives
- Tokens, hashes, and digital signatures
- Third-party and SaaS cryptography

Phase 2: Discover Cryptographic Assets (Weeks 2–4)

System & Application Discovery

Create an inventory across:

Category	Examples
Applications	ERP, CRM, billing, HR, custom apps
Infrastructure	Servers, databases, storage
Cloud	AWS, Azure, GCP services, IBM Cloud
Networks	VPNs, load balancers, firewalls
Endpoints	Laptops, mobile devices
OT / IoT	SCADA, embedded systems

Use:

- Architecture diagrams
- CMDBs
- Cloud security tools
- Interviews with system owners

Identify Cryptographic Usage Per System

For each system, document:

- Encryption purpose
  (At rest, in transit, authentication, signing)
- Algorithms used
  (RSA, ECC, AES, SHA, TLS versions)
- Key sizes and modes
- Certificate usage
- Key storage method
  (HSM, KMS, software, hard-coded)

Red flag: Hard-coded keys, deprecated algorithms, or unknown key management.

Phase 3. Data Classification & Longevity Mapping (Weeks 4–6)

Map Encryption to Data Types

For each cryptographic instance, answer:

- What data is protected?
- How sensitive is it?
- How long must it remain confidential?

Example:

Data Type	Sensitivity	Retention	Quantum Risk
PHI	Very High	25+ years	Critical
Financial Records	High	7–10 years	High
IP / Trade Secrets	Very High	20+ years	Critical
Operational Logs	Medium	3–5 years	Moderate

Identify “Harvest Now, Decrypt Later” Exposure

Flag systems where:

- Data is encrypted today
- Retention exceeds 10 years
- Algorithms are quantum-vulnerable (RSA, ECC)

These become top-priority quantum risk assets.

Phase 4. Assess Crypto-Agility & Vendor Risk (Weeks 6–8)

Evaluate Crypto-Agility

For each system, assess:

- Can encryption algorithms be swapped without redesign?
- Is encryption abstracted or hard-coded?
- Are updates vendor-controlled?
- Can PQC (Post Quantum Cryptography) be added later?

Score systems as:

- Agile
- Partially Agile
- Not Agile

Third-Party & SaaS Cryptography Review

Require vendors to disclose:

- Encryption algorithms in use
- Roadmap for post-quantum cryptography (PQC)
- Ability to support hybrid encryption

SigmaSRC best practice: Add quantum readiness clauses to vendor risk assessments.

Phase 5. Document, Prioritize & Report (Weeks 8–10)

Create the Cryptographic Inventory Register

Each record should include:

- System name & owner
- Data protected
- Algorithm(s) and key sizes
- Key management method
- Data retention period
- Quantum vulnerability
- Crypto-agility score
- Compliance impact

This becomes a living enterprise artifact, not a one-time exercise.

Prioritize Remediation

Rank assets by:

1. Data sensitivity
2. Data longevity
3. Quantum vulnerability
4. Compliance exposure
5. Business impact

Focus first on:

- Long-retention + high-sensitivity data
- Systems that cannot be upgraded easily
- Third-party dependencies

Governance & Continuous Monitoring

Integrate Into Risk & Compliance Programs

- Tie inventory results to:
    - Enterprise risk register
    - Compliance audits (HIPAA, SOX, GDPR, NERC CIP)
    - Board reporting
- Update annually or upon major system changes

Prepare for Post-Quantum Transition

Use the inventory to:

- Define PQC pilot candidates
- Create a phased migration roadmap
- Support regulatory and board inquiries
- Demonstrate due diligence

What Success Looks Like

A company that completes a full cryptographic inventory can confidently say:

- "We know where our encryption lives."
- "We understand which data is vulnerable to quantum threats."
- "We can change cryptography without breaking the business."
- "We are defensible to regulators, auditors, and boards."

SigmaSRC Value Alignment

SigmaSRC enables organizations to:

- Unify security, risk, and compliance views
- Track cryptographic risk in real time
- Support quantum readiness and crypto-agility
- Translate technical findings into board-level insight

About SigmaSRC®

SigmaSRC stands at the forefront of adaptive cybersecurity assurance, enterprise risk management, and automated compliance enforcement. The **SigmaSRC Enterprise Platform**™ empowers organizations of any scale to centrally orchestrate, monitor, and automate security, compliance, and risk (SRC) across every system operating in fast-changing environments.

Engineered as a unified, AI-driven SaaS platform (v1.5), SigmaSRC provides deep visibility and precise control across dynamic computing infrastructures, enabling enterprises to meet regulatory and internal compliance obligations while significantly strengthening their overall security posture.

SigmaSRC is incorporated in Texas and operates throughout North America and Europe.

To learn more, visit ***www.sigmasrc.com***.