CONFIDENTIAL

Voya Financial, Inc.

Cybersecurity Program Summary

Risk Management, Strategy & Governance | Fiscal Year 2025 (ended December 31, 2025)

Filed: February 20, 2026 | NYSE: VOYA | Financial Services | New York, NY

This document synthesizes Voya Financial's cybersecurity risk management, strategy, and governance framework from two authoritative sources: the Form 10-K filed with the SEC (February 20, 2026) and Voya's published Cybersecurity Program disclosure on Voya.com.

At a Glance

COMPANY	FRAMEWORKS	INFOSEC TEAM	BOARD OVERSIGHT	CISO EXPERIENCE	MATERIAL INCIDENTS
Voya Financial	**6 Standards**	**100+**	**Risk + Audit Committees**	**30+ Years**	**None**
NYSE: VOYA | Financial Services	NIST 800-53, ISO 27001:2022, COSO, COBIT, SOC 1 & SOC 2	Employees, 150+ certifications	Dual Board committee model	Former Voya CTO	No material incidents in 3 years

Voya Financial is a leading provider of workplace benefits, savings solutions, and investment management services with over 18 million individual customer relationships, more than 50,000 employer and institutional clients, and approximately $1.1 trillion in total assets under management and administration. Voya's cybersecurity program is one of the most comprehensively documented in the financial services sector — drawing on six distinct standards and frameworks, ISO 27001:2022 certification with annual revalidation, SOC 1 and SOC 2 Type II attestations, and a 100+ person information security team holding more than 150 industry certifications.

Combined Source Advantage: This summary synthesizes both Voya's SEC 10-K Item 1C disclosure and Voya's published Cybersecurity Program overview. Together these sources reveal a substantially more mature and comprehensive program than the 10-K alone reflects — including NIST 800-53 adoption, Secure SDLC practices, automated patch management, BC/DR plans, end-to-end encryption, and a multi-framework compliance posture that ranks among the most rigorous in this peer group.

1. Framework & Compliance Posture

Voya operates one of the broadest multi-framework compliance postures in the financial services peer group, drawing on six distinct standards across information security, risk management, and technology governance. This depth of framework adoption provides assurance to participants, clients, and regulators across all of Voya's regulated business lines.

Framework / Standard	Description & Relevance	Status
NIST 800-53	National Institute of Standards and Technology Special Publication 800-53 — Security and Privacy Controls for Information Systems. More prescriptive and control-specific than NIST CSF, widely required in government and regulated financial services environments.	**Integrated**
ISO 27001:2022	International standard for information security management systems — most current 2022 version. Voya holds active certification with annual third-party revalidation. Most peers reference NIST without pursuing formal external certification.	**Certified — Annual Revalidation**
SOC 1 & SOC 2 Type II	Service Organization Control reports per Department of Labor best practices. Attests that internal controls, processes and systems are independently evaluated for both security and operational effectiveness.	**Active — DOL Best Practice**
COSO	Committee of Sponsoring Organizations of the Treadway Commission — integrated framework for enterprise risk management, internal control, and fraud deterrence. Ensures technology controls align with enterprise risk management objectives.	**Integrated**
COBIT	Control Objectives for Information and Related Technologies — IT governance and management framework ensuring technology supports enterprise risk management efforts and business objectives.	**Integrated**
DOL Cybersecurity Best Practices	U.S. Department of Labor cybersecurity guidance for retirement plan providers — directly applicable to Voya's core retirement business serving nearly 10 million participant accounts.	**Compliant**

Peer Benchmark: Voya's six-framework posture — combining NIST 800-53, ISO 27001:2022, SOC 1, SOC 2 Type II, COSO, and COBIT — is the most comprehensive framework stack in this peer group. CVS Health, previously the peer leader with seven standards, overlaps in several areas (NIST, SOC, PCI-DSS) but Voya's addition of COSO and COBIT reflects a more integrated enterprise risk management orientation.

2. Program Pillars

Voya's cybersecurity program is built around nine distinct operational pillars, each formally defined with dedicated resources, processes, and accountability. Cybersecurity is described as 'built-in' to all business practices and products and represents a considerable portion of Voya's IT budget.

1. Governance & Executive Oversight

Active executive oversight of cybersecurity initiatives to align with business objectives. The CISO reports to the Chief Technology and Operations Officer (CTOO) and provides regular updates to senior leadership on risk assessments, security posture, and key metrics. Cybersecurity is a strategic priority at every level of the organization.

2. Risk Management & Compliance

Integrates NIST 800-53 controls and follows DOL best practices including SOC 1 and SOC 2 Type II reports. Incorporates COSO and COBIT frameworks to ensure technology supports enterprise risk management. ISO 27001:2022 certification is maintained with annual third-party revalidation. The comprehensive compliance framework provides assurance to participants, clients, and regulators.

3. Vulnerability Management

Automated patch management system promptly identifies and patches critical software and hardware vulnerabilities. Internal and external penetration testing is a cornerstone of proactive security. Monthly internal vulnerability scans are conducted, complemented by tabletop exercises that simulate both offensive and defensive security scenarios.

4. Secure Software Development Lifecycle (SDLC)

Security is embedded throughout the Software Development Lifecycle. Applications and systems undergo rigorous security assessments during development, including code reviews, static and dynamic analysis, and secure coding practices. This ensures security is built into every phase rather than applied as a post-development layer.

5. Data Protection & Encryption

End-to-end encryption and data masking techniques protect sensitive data both at rest and in transit. Access controls and least privilege principles ensure that only authorized personnel can access critical systems and data, minimizing the attack surface and potential for unauthorized access.

6. Incident Response & Legal Oversight

An incident response framework provides a quick and coordinated response to mitigate damage. The team works closely with Voya's legal department, including the Chief Privacy Officer, to advise on relevant regulations, data breach notification requirements, and other legal considerations. The IRP includes regularly tested playbooks.

7. Employee Training & Awareness

Employee training programs raise awareness on phishing, social engineering, incident reporting, password security, and safe computing practices. Regular training ensures employees remain vigilant and understand how their actions impact overall organizational security. A secure environment begins with an informed workforce.

8. Third-Party & Supply Chain Risk

A dedicated team evaluates, assesses, and addresses third-party risks using a risk-based approach. The team conducts due diligence on vendors and service providers — evaluating their information security controls — to identify potential risks and implement appropriate controls. The goal is protecting sensitive information and operational security across the entire supply chain.

9. Business Continuity & Disaster Recovery

Strong business continuity and disaster recovery plans enable Voya to quickly recover from disruptions. Plans include regular testing to validate that systems and data can be restored in the event of a cyber incident — going beyond incident response to ensure sustained operational resilience.

3. Governance & Leadership

CISO & Leadership Profile

Named CISO	Stacy Hughes — Senior Vice President & Chief Information Security Officer	**Reports To**	Chief Technology and Operations Officer (CTOO)
Experience	30+ years of professional IT experience in financial services	**Prior Role at Voya**	Chief Technology Officer — responsible for infrastructure, cloud, and business resiliency office
Team Size	100+ information security professionals	**Team Certifications**	150+ certifications from leading industry organizations
Reporting Cadence	Regular updates to senior leadership on risk assessments, security posture, and key metrics	**Board Reporting**	Regular updates to the Board Risk Committee; collaborates with Audit Committee on disclosures

Governance Structure

Governance Body	Role	Notes
Board Risk Committee	Provides Board-level oversight of information technology and cybersecurity risk. Responsible for overseeing cybersecurity risk. Collaborates with the Audit Committee on disclosure.	Receives regular CISO updates on cybersecurity matters.
Board Audit Committee	Collaborates with the Risk Committee on cybersecurity risk disclosures. Provides a second Board-level governance lens specifically covering disclosure adequacy.	Joint oversight model separates risk management from disclosure governance — a leading practice.
Technology & Operational Risk Committee (TORC)	Management-level committee delegated by the Management Risk Committee to oversee operational risk including information and technology risk, legal, compliance, and regulatory risks.	Cross-functional membership: operations, technology, information security, legal, compliance, data privacy, and operational risk. Information security team participates directly.
CISO & Information Security Team	Day-to-day cybersecurity operations: continuous monitoring, risk identification, incident response, and vendor oversight. Provides regular updates to senior management and Board.	100+ team members with 150+ certifications. CISO designated under Voya's risk management principles to oversee evaluation and mitigation of information security risks.

Governance Body	Role	Notes
Cross-Functional Partners	Compliance, Human Resources, Internal Audit, Legal, Privacy, and Enterprise Risk Management teams are formally recognized as essential contributors to information security.	Reflects an organization-wide ownership model — cybersecurity is embedded across the enterprise, not siloed in IT.

4. Technology Controls

Authentication	Multi-factor authentication (MFA) including voice and fingerprint biometrics as additional factors beyond standard MFA	**Defense Model**	Layer-of-defense architecture protecting against both external and internal threats through multiple overlapping security controls
Threat Detection	Active threat detection and prevention protocols with proactive real-time threat intelligence sharing across the industry	**Monitoring**	Continuous monitoring and evaluation of technology and digital infrastructure to identify and assess threats in real time
Patch Management	Automated patch management system to promptly identify and patch critical software and hardware vulnerabilities	**Vulnerability Scanning**	Monthly internal vulnerability scans plus internal and external penetration testing as a cornerstone of proactive security
Encryption	End-to-end encryption and data masking for sensitive data both at rest and in transit	**Access Controls**	Least privilege principles ensuring only authorized personnel access critical systems and data, minimizing the attack surface
Secure SDLC	Code reviews, static and dynamic analysis, and secure coding practices embedded throughout the software development lifecycle	**Session Controls**	Secure email systems and time-based session logoff controls deployed across Voya's environment

5. Program At-a-Glance Scorecard

NIST 800-53 Controls Integrated	**Confirmed**	ISO 27001:2022 Certification — Annual Review	**Certified**
SOC 1 Report — Independently Attested	**Confirmed**	SOC 2 Type II Report — Independently Attested	**Confirmed**
COSO Framework Integration	**Confirmed**	COBIT Framework Integration	**Confirmed**
DOL Cybersecurity Best Practices	**Confirmed**	Designated CISO — SVP Level	**Confirmed**
CISO: 30+ Years IT/Financial Services	**Confirmed**	CISO: Former Voya CTO	**Confirmed**
InfoSec Team of 100+ Professionals	**Confirmed**	150+ Industry Certifications (Team)	**150+**
Board Risk Committee Oversight	**Confirmed**	Board Audit Committee — Disclosure Collab.	**Dual**
TORC — Management Risk Committee	**Active**	Cross-Functional Security Partners (6 teams)	**Confirmed**
Continuous Threat Monitoring	**Active**	Automated Patch Management	**Confirmed**
Monthly Vulnerability Scans	**Monthly**	Internal & External Penetration Testing	**Confirmed**
Tabletop Exercises	**Confirmed**	Secure SDLC Embedded in Development	**Confirmed**
End-to-End Encryption (At Rest & Transit)	**Confirmed**	MFA + Biometric Authentication	**Confirmed**
Layer-of-Defense Architecture	**Confirmed**	Least Privilege Access Controls	**Confirmed**
Employee Training & Awareness Program	**Confirmed**	Dedicated Third-Party Vendor Risk Team	**Dedicated**
BC/DR Plans with Regular Testing	**Confirmed**	Integrated Incident Response Plan	**Confirmed**
No Material Incidents — 3-Year Period	**None**		

6. Key Observations & Benchmarking Notes

Most Comprehensive Framework Stack in the Peer Group

Voya's six-framework posture — NIST 800-53, ISO 27001:2022, SOC 1, SOC 2 Type II, COSO, and COBIT — is the broadest in this benchmarking peer group. NIST 800-53 is more prescriptive than the NIST CSF used by most peers. The addition of COSO and COBIT reflects Voya's integration of cybersecurity with enterprise risk management and IT governance — not just technical controls.

CISO Is a Former CTO — Uniquely Valuable Credential

Voya's CISO previously served as the company's Chief Technology Officer, with direct responsibility for infrastructure, cloud, and business resiliency. This means the person responsible for securing Voya's systems helped build them — providing institutional knowledge that is rarely available in a CISO hire.

Nine Formally Defined Program Pillars — Most Structured in Peer Group

Voya explicitly defines nine distinct cybersecurity program pillars with named owners, specific practices, and documented processes. This level of structural formality — including a Secure SDLC, automated patch management, BC/DR with regular testing, and cross-functional governance — reflects a program built with enterprise-grade architectural discipline.

Dual Board Committee Governance Is a Leading Practice

Routing cybersecurity oversight through both a Board Risk Committee and an Audit Committee that collaborates on disclosure provides more formal separation than the Audit Committee-only model used by most Fortune 500 peers. This ensures both risk management and disclosure governance are independently addressed at the Board level.

Cybersecurity Explicitly 'Built-In' — A Cultural Statement

Voya's disclosure that cybersecurity is 'built-in' to all business practices and products — and represents a considerable portion of the IT budget — is a stronger cultural claim than most peers make. Combined with the cross-functional partner framework (Compliance, HR, Legal, Internal Audit, Privacy, and ERM), this signals organization-wide ownership rather than IT-department ownership.

Monthly Vulnerability Scans + Automated Patching = Proactive Posture

Monthly internal vulnerability scans combined with an automated patch management system represents a notably proactive vulnerability management program. Most peers disclose periodic testing without specifying frequency or automation — Voya's specificity here signals operational maturity.

Sources: Voya Financial, Inc. — Form 10-K filed February 20, 2026 (Fiscal Year 2025 (ended December 31, 2025)) and Voya.com Cybersecurity Program disclosure. SEC EDGAR: https://www.sec.gov/Archives/edgar/data/1535929/000153592926000043/voya-20251231.htm | Prepared: May 15, 2026 | vpop.com | For Internal Distribution Only