ProSight™

ProSight Technology Risk Framework

BAI & RMA:
Together we're ProSight

ProSightFA.org

About ProSight Financial Association

ProSight Financial Association empowers financial services leaders to strengthen and advance our industry. Formed through the merger of BAI and RMA, trusted organizations with rich histories and deep expertise in risk, compliance, and retail and commercial banking, we are here to support you during times of great change, guide you towards new opportunities for growth, and help you act with confidence. As ProSight, we've enhanced our ability to support you at a time when the industry is challenged to meet changing customer needs, adopt new technologies, and manage more complex risk and compliance issues. Our work creates positive ripple effects throughout financial services organizations and our industry—and ultimately helps consumers, businesses and communities thrive. Learn more at ProSightFA.org.

Acknowledgments

ProSight Technology Risk Framework is published by ProSight Financial Association.

ProSight gratefully acknowledges the contributions of individuals contributing to refinements and revisions in this 2025 update to the ProSight Technology Risk Framework: **Joshua M. Henrich**, *CPA, CISSP, CCSP, CRISC, CISM, CDPSE, CISA; SVP, Executive Director, Head of Information Security Governance & Risk Management*, U.S. Bank; **Caitlin Barre,** *Senior Vice President, Head of IT and Data Risk Management*, Regions Bank; **Matthew Beard**, *CISA, CRISC, SVP, Sr. Director, Tech & Security Risk Oversight*, Fifth Third Bank; **Robert Boutell**, Technology Risk Officer, Huntington Bank; **Denise Cramer**, *EVP - Technology and Cybersecurity Risk*, M&T Bank; **Erika Crandall**, *Chief Risk Officer*, Xpansiv Limited; **Robert Hach**, Senior Director, Technology, Cybersecurity, & Resiliency Risk Oversight, KeyBank; **Jennifer Wolf Harris**, *Director - Technology and Cybersecurity Risk*, M&T Bank; **James Johnson**, *SVP/Sr. Division Director, Consumer and Marketing BRCO*, Comerica Bank; **Stuart Strepman**, *Managing Director, Enterprise and Operational Risk Management*, Charles Schwab & Co., Inc.

ProSight gratefully acknowledges the efforts of the members of the 2020 Technology Risk Committee: **Heather Bannon**, *Director, IT Risk Management*, Discover Financial Services; **Rob Boutell**, *Technology Risk Officer*, The Huntington National Bank; **Michael Cornelsen**, *Managing Director, Technology Risk*, Charles Schwab Corporation; **Gary Olsen**, *Managing Director, IT Risk and Compliance*, FHL Bank of San Francisco; **CJ Paul**, *Director, Operational & Technology Risk/Operational & Strategic Risk*, TD Ameritrade; **Brian M. Smith**, *Head of Information Risk and Resilience*, Prudential Financial

The Technology Risk Committee is a committee under the Operational Risk & Resiliency Council, chaired by **Mary Kapferer**, KeyBank.

Please direct inquiries to Edward DeMarco, Jr. at edemarco@ProSightFA.org, and Sylwia Czajkowska at sczajkowska@ProSightFA.org.

Design by Christopher Santoro.

September 2025

Table of Contents

Section 1

Introduction

At publication in 2020, ProSight's Technology Risk Framework clarified language the banking industry uses to describe Technology Risk. With new definitions in place, ProSight has collaborated with its members to develop a more mature understanding of this risk.

Now, in this latest 2025 revision of the framework, we support banks with structure for a more holistic assessment of technology risk in your environment, among your customers, and across the industry. This revised framework adjusts to your size, complexity and business structure, and works in conjunction with other risk frameworks available through ProSight Financial Association. It also provides varied and differing perspectives about Technology Risk among the many different organizations that manage it.

The simplest and most important way to apply this framework is by performing a gap analysis against your own risk management programs. Are you already covering everything in this framework? If so, have you covered it holistically across the entire organization? And are your risks in plain view?

Section 2

Problem Statement

Understanding the complexity of risks facing financial institutions is imperative. Technology Risk, once a subset of operational risk, is now its own category within enterprise risk taxonomies, reflecting technology's importance to modern business. It runs across other risk domains and can manifest anywhere technology is deployed.

While some institutions carve out Technology Risk within their technology organizations, aligning it this way can limit visibility into these risks and an institution's ability to properly assess them. Approaches continue to evolve, with some now using an integrated "Product" model, where technology is embedded in the business.

Other existing frameworks look at controls and how to layer and implement them, but few look at the risks behind the controls. The ProSight Technology Framework fills these gaps in our understanding, and applicability, of technology-driven risks, while introducing customization to meet an institution's particular needs.

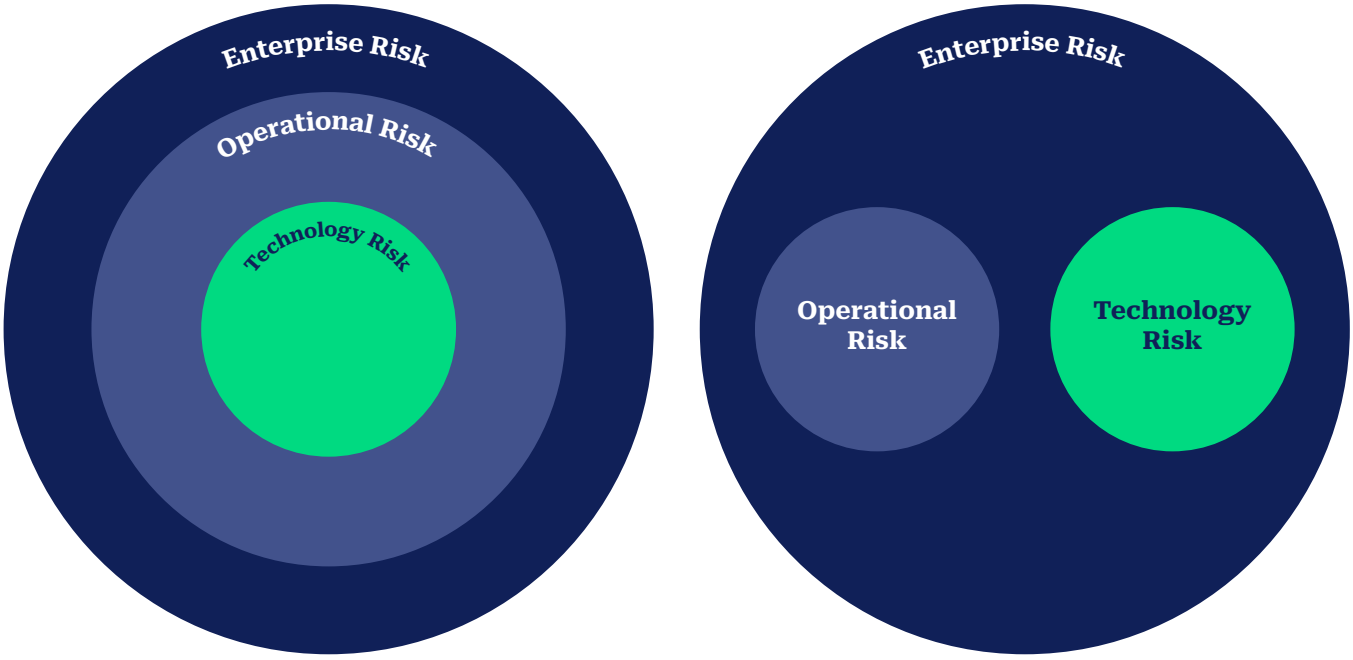
Removing organizational structure from risk considerations clarifies that everyone is responsible for identifying, managing, and mitigating Technology Risk. Technology touches most everyone in business today. Your role is to understand the risks in your domain and do your part to reduce them.

We recognize in this version of the framework that not all institutions view Technology Risk in traditional "CIA (Confidentiality, Integrity, and Availability) plus Value Delivery' terms, and so we have included the Technology Risk Committee's perspective on an alternative method of organizing these risks. There is no right or wrong way to organize them, however we do believe that this is a strong, mutually exclusive and collectively exhaustive set of Technology Risks to which every institution has some degree of exposure.

Interplay Among Enterprise, Operational, and Technology Risk

The ProSight Enterprise Risk Framework and the ProSight Technology Risk Framework are intricately connected, as they both serve to guide institutions in identifying, assessing, monitoring, mitigating, communicating and escalating risk across the entire enterprise. The Enterprise Risk Framework provides a comprehensive approach to risk management by considering all types of risks—credit, market, operational, and others—and how they interact at an organizational level. It sets forth principles for appropriate coverage, governance structure and oversight, policies and procedures, risk appetite, risk data and infrastructure, measurement, control environment, response, stress testing and culture.

The connection between the two frameworks lies in the understanding that technology risks cannot be managed in isolation. The Technology Risk Framework is applied within the broader context set by the Enterprise Risk Framework, ensuring that technology risks are evaluated alongside all other risks to achieve a holistic risk management strategy. This interconnectedness ensures that risk management efforts are aligned with the organization's overall risk appetite and strategic objectives, providing a layered yet cohesive defense against potential risk impacts that damage the institution's ability, resiliency and integrity.



Section 3

Framework Risk Categories

3.1 Confidentiality: Preserving authorized restrictions on information access and disclosure, including means for protecting personal privacy and proprietary information.

3.1.1. **Logical data theft or exfiltration**
Non-public data is inappropriately removed from its authorized location, including internal systems, cloud-based systems, and third parties.

Alternative Framework Category Mapping: Cybersecurity/Information Security

3.1.2. **Unauthorized data access**
Unauthorized viewing of non-public data, including data stored on internal systems, cloud-based systems, and third parties or data transmitted by internal or external networks.

Alternative Framework Category Mapping: Cybersecurity/Information Security

3.1.3. **Inadvertent data exposure**
Non-public data is inadvertently made publicly available, lost, or exposed to an unauthorized recipient.

Alternative Framework Category Mapping: Cybersecurity/Information Security

3.1.4. **Physical data theft**
Physical documents or data-bearing assets are inappropriately removed from their authorized physical location(s).

Alternative Framework Category Mapping: Physical Security

3.2 Integrity: Guarding against improper information modification or destruction and includes ensuring information, non-repudiation, and authenticity.

3.2.1. Unauthorized modification of data

Unauthorized modification of data, including (but not limited to) direct modification of transactional data, personal data, or financial statement data.

Alternative Framework Category Mapping: Cybersecurity/Information Security

3.2.2. Unauthorized System Changes

Unauthorized changes to system files, source code, configurations and/or system interfaces.

Alternative Framework Category Mapping: Systems/Technology Operations

3.2.3. Lack of non-repudiation

Inability to prove a person performed a particular action, such as a system change, sending a message, or approving a transaction.

Alternative Framework Category Mapping: Cybersecurity/Information Security

3.2.4. Unauthorized network intrusion

Unauthorized intrusion into networks that may allow for reconnaissance, installation of malware, and remote manipulation of systems.

Alternative Framework Category Mapping: Cybersecurity/Information Security

3.2.5. Processing failures

System processing failures that result in incomplete, inaccurate, or untimely outputs, including transactions or calculations.

Alternative Framework Category Mapping: Systems/Technology Operations

3.2.6. Lack of data quality

Data that is entered into or stored by IT systems that is incomplete, inconsistent, unreliable, or inaccurate.

Alternative Framework Category Mapping: Data Management

3.2.7. Insufficient data/asset inventory

Inability to specify the physical or logical location of, or interrelationships between, electronic or physical data, hardware, or software.

Alternative Framework Category Mapping: Systems/Technology Operations

3.3 Availability: Ensuring timely and reliable access to and use of information.

3.3.1. Unauthorized data destruction

Unauthorized destruction of data through deletion, corruption, or encryption (i.e., ransomware).

Alternative Framework Category Mapping: Resiliency

3.3.2. Unplanned system downtime

Systems that are not available to the users when required (includes subsystems).

Alternative Framework Category Mapping: Systems/Technology Operations

3.3.3. Inadequate incident response and recovery

Unprepared to respond to and recover from operational or information security incidents.

Alternative Framework Category Mapping: Resiliency

3.3.4. Slow system performance

System slowness that impedes business operations, processing, or communications.

Alternative Framework Category Mapping: Systems/Technology Operations

3.3.5. Critical infrastructure outage (e.g., electricity, internet)

Critical infrastructure services that are not available to support the environment when required, including electricity, internet, and cooling systems.

Alternative Framework Category Mapping: Resiliency

3.4 Value Delivery: Ensuring technology meets the needs of its users and objectives of the organization.

3.4.1. System delivery failures

Inability to deliver IT systems that meet defined business requirements within needed timeframes and agreed budgets.

Alternative Framework Category Mapping: Systems/Technology Operations

3.4.2. Lack of fit-for-purpose systems

Systems prevent meeting current business objectives, including customer retention, regulatory compliance, poor customer/user experience and/or cost effectiveness.

Alternative Framework Category Mapping: Systems/Technology Operations

3.4.3. Inability to maintain and scale systems (e.g., documentation / knowledge)

Lack of relevant information or architecture needed to maintain or scale technology assets (hardware, software, network), including code documentation, runbooks, dataflow diagrams, configuration databases, and network diagrams.

Alternative Framework Category Mapping: Systems/Technology Operations

Appendix 1

Mapping Specific Risk Types To Causation Categories

Category		Framework	Definitions	Examples
Confidentiality	Preserving authorized restrictions on information access and disclosure, including means for protecting personal privacy and proprietary information.	Logical data theft or exfiltration **Alternative Framework Category Mapping:** Cybersecurity/Information Security	Non-public data is inappropriately removed from its authorized location, including internal systems, cloud-based systems, and third parties.	• Data breach by a malicious external threat actor (e.g., a cybercriminal or nation state). • Intellectual property stolen or compromised by an employee or consultant (e.g. an Insider Threat).
		Unauthorized data access **Alternative Framework Category Mapping:** Cybersecurity/Information Security	Unauthorized viewing of non-public data, including data stored on internal systems, cloud-based systems, and third parties or data transmitted by internal or external networks.	• Employee accesses sensitive personal information without a business purpose (e.g., for a celebrity, ex-spouse, etc.) with either approved or prohibited access to the information. • Former or transferred employee's access was not removed. • Sharing your password.
		Inadvertent data exposure **Alternative Framework Category Mapping:** Cybersecurity/Information Security	Non-public data is inadvertently made publicly available, lost, or exposed to an incorrect recipient.	• Unsecured Cloud Storage buckets (e.g. publicly facing, with no authentication requirements) exposing confidential or personal information. • E-mailing sensitive information to the wrong person, such as "reply all". • Sending a physical statement to the wrong address. • One user seeing another user's information on a customer portal.
		Physical Data Theft **Alternative Framework Category Mapping:** Physical Security	Physical documents or data-bearing assets are inappropriately removed from their authorized physical location(s).	• Technology facilities are physically breached by a malicious threat actor and technology equipment is stolen. • Documents containing sensitive information are disposed of in an insecure manner and are found by unauthorized personnel.

Category		Framework	Definitions	Examples
Integrity	Guarding against improper information modification or destruction and includes ensuring information non-repudiation and authenticity.	Unauthorized modification of data **Alternative Framework Category Mapping:** Cybersecurity/Information Security	Unauthorized modification of data, including direct modification of transactional data or financial statement data.	• Database administrator performs an unauthorized modification of data (for whatever purposes - either personal gain), or for other perceived benefit not approved by the data owner. • Employee changes financial data record without proper authorization.
		Unauthorized System Changes **Alternative Framework Category Mapping:** Systems/Technology Operations	Unauthorized changes to systems files, source code, configurations and/or system interfaces.	• Undocumented changes implemented by a system administrator, or other similarly entitled employee who institutes change outside of defined approval processes. • Change was mistakenly made to the wrong file/system/asset.
		Lack of non-repudiation **Alternative Framework Category Mapping:** Cybersecurity/Information Security	Inability to prove a person performed a particular action, such as a system change, sending a message, or approving a transaction.	• Lack of logging or system tracking. • Weakness within the digital signature process.
		Unauthorized network intrusion **Alternative Framework Category Mapping:** Cybersecurity/Information Security	Unauthorized intrusion into networks that may allow for reconnaissance, installation of malware, and remote manipulation of systems.	• Exploitation of a vulnerability, system misconfiguration, or insufficient access controls to gain access to a network or its systems.
		Processing failures **Alternative Framework Category Mapping:** Systems/Technology Operations	System processing that results in invalid outputs, including transactions or calculations.	• Job scheduling failed causing the prior day's file to be processed. • Records dropped from a file during transfer. • Failed data or API transmissions which cause incomplete, untimely or inaccurate data.
		Lack of data quality **Alternative Framework Category Mapping:** Data Management	Data that is entered into or stored by IT systems that are incomplete, inconsistent, unreliable, or inaccurate.	• Lack of time stamps on record creation, deletion, or modification. • Adding data into data warehouse without data quality requirements and checks (e.g. Extract-Transform-Load controls to ensure completeness and accuracy of processing). • Inability to leverage data across the company when meta data/context is missing. • No input checks (all free form text) for an application.
		Insufficient data/asset inventory **Alternative Framework Category Mapping:** Systems/Technology Operations	Inability to specify the physical or logical location of, or inter- relationships between, electronic or physical data, hardware, or software.	• IT assets (data, systems, applications, etc.) are not holistically captured in an inventory system of record. • Up- and down-stream systems are not adequately known so as to predict impact of changes, incidents, etc. • Use of unapproved technology. • Unknown assets connected to the network.

Category		Framework	Definitions	Examples
Availability	Ensuring timely and reliable access	Unauthorized data destruction **Alternative Framework Category Mapping:** Resiliency	Unauthorized destruction of data through deletion, corruption, or encryption (i.e., ransomware).	• Ransomware or destructive malware (e.g. NotPetya). • Dropped a table without a backup. • Accidentally deleting files when on a share drive.
		Unplanned system downtime **Alternative Framework Category Mapping:** Systems/ Technology Operations	Systems that are not available to the users when required (includes subsystems).	• Denial of Service or unavailability of: business applications, business intelligence tools, cloud platforms, internal networks, telephony, and e-mail. • Operational outages. • Degraded services (part of the application is unavailable) such as when Online Banking is up but bill pay capabilities are down.
		Inadequate incident response and recovery **Alternative Framework Category Mapping:** Resiliency	Unprepared to respond to and recover from operational or information security incidents.	• Inability to detect incidents. • MTR (mean time to recover) is above SLA (service level agreement). • Inability to prioritize efforts. • Not involving proper stakeholders (e.g. privacy, legal, communications).
		Slow system performance **Alternative Framework Category Mapping:** Systems/ Technology Operations	System slowness that impedes business operations, processing, or communications.	• Email that takes 15 minutes to get delivered. • Needing to reboot the computer to enable patches. • Unacceptable levels of network or application latency.
		Critical infrastructure outage (e.g., electricity, internet) **Alternative Framework Category Mapping:** Resiliency	Critical infrastructure services that are not available to support the environment when required, including electricity, internet, and cooling systems.	• Electricity is insufficient to support IT assets (could be either an outage or “brownouts”). • Internet Service Providers or other telecoms (including phone companies) upon which the business relies become unavailable, or do not perform to required service levels (e.g., latency, call clarity, etc.).

Category		Framework	Definitions	Examples
Value Delivery	Ensuring technology meets the needs of its users and objectives of the organization.	System delivery failures **Alternative Framework Category Mapping:** Systems/ Technology Operations	Inability to delivery IT systems that meet defined business requirements within needed timeframes and agreed budgets.	• Poor project or portfolio management. • Lack or silo of information, leading to incorrect decisions. • Lack of business involvement in Agile project efforts.
		Lack of fit- for-purpose systems **Alternative Framework Category Mapping:** Systems/ Technology Operations	Systems prevent meeting current business objectives, including customer retention, regulatory compliance, poor customer/ user experience and/or cost effectiveness.	• Systems have functionality gaps that result in the system not meeting business requirements. • Work around is too cumbersome. • Websites with user interface that are not intuitive. • Multiple Case Management tools. • Websites that are not mobility aware or do not meet ADA requirements.
		Inability to maintain and scale systems (e.g.: documentation/ knowledge) **Alternative Framework Category Mapping:** Systems/ Technology Operations	Lack of relevant information needed or architecture to maintain or scale technology assets (hardware, software, network), including code documentation, runbooks, dataflow diagrams, configuration databases, and network diagrams.	• No COBOL developers to maintain systems. • Not storing third party code in escrow. • Third party software no longer supported. • Code that is not commented. • Highly customized systems that may it difficult to upgrade to the current version. • Specialized/small/startup software company used to develop a core application.

Overall notes:
1. Third party intentionally excluded from this framework.
2. Risks tied to an IT organization are broader than this framework and would include enterprise and operational risk areas as well.
3. Expanding and contracting the framework based on size and complexity.

Appendix 2


CONFIDENTIALITY
Preserving authorized restrictions on information access and disclosure, including means for protecting personal privacy and proprietary information.
INTEGRITY
Guarding against improper information modification or destruction and includes ensuring information, non-repudiation, and authenticity.
AVAILABILITY
Ensuring timely and reliable access to and use of information.
VALUE DELIVERY
Ensuring technology meets the needs of its users and objectives of the organization.
TECHNOLOGY RISK FRAMEWORK
• Logical data theft or exfiltration: Non-public data is inappropriately removed from its authorized location, including internal systems, cloud based systems, and third parties.
• Unauthorized data access: Unauthorized viewing of non-public data, including data stored on internal systems, cloud-based systems, and third parties or data transmitted by internal or external networks.
• Inadvertent data exposure: Non-public data is inadvertently made publicly available, lost, or exposed to an incorrect recipient.
• Physical data theft: Physical documents or data-bearing assets are inappropriately removed from their authorized physical location(s).
• Unauthorized modification of data: Unauthorized modification of data, including direct modification of transactional data or financial statement data.
• Unauthorized System Changes: Unauthorized changes to systems files, source code, configurations and/or system interfaces.
• Lack of non-repudiation: Inability to prove a person performed a particular action, such as a system change, sending a message, or approving a transaction.
• Unauthorized network intrusion: Unauthorized intrusion into networks that may allow for reconnaissance, installation of malware, and remote manipulation of systems.
• Processing failures: System processing that results in invalid outputs, including transactions or calculations.
• Lack of data quality: Data that is entered into or stored by IT systems that are incomplete, inconsistent, unreliable, or inaccurate.
• Insufficient data/asset inventory: Inability to specify the physical or logical location of, or inter-relationships between, electronic or physical data, hardware, or software.
• System delivery failures: Inability to delivery IT systems that meet defined business requirements within needed timeframes and agreed budgets.
• Lack of fit-for-purpose systems: Systems prevent meeting current business objectives, including customer retention, regulatory compliance, poor customer/user experience and/or cost effectiveness.
• Inability to maintain and scale systems (e.g.: documentation/knowledge): Lack of relevant information needed or architecture to maintain or scale technology assets (hardware, software, network), including code documentation, runbooks, dataflow diagrams, configuration databases, and network diagrams.
• Unauthorized data destruction: Unauthorized destruction of data through deletion, corruption, or encryption (i.e. ransomware).
• Unplanned system downtime: Systems that are not available to the users when required (includes subsystems).
• Inadequate incident response and recovery: Unprepared to respond to and recover from operational or information security incidents.
• Slow system performance: System slowness that impedes business operations, processing, or communications.
• Critical infrastructure outage (e.g., electricity, internet): Critical infrastructure services that are not available to support the environment when required, including electricity, internet, and cooling systems.

ProSight™

ProSightFA.org