AUDREY MAGENNIS

Performing IT Risk Assessments: Identifying and Mitigating Key Risks

KEYS 2026 HORIZONS

1

DISCLAIMER

- **This presentation is for information only.**
  Evaluate risks before acting based on ideas from this presentation.
- **This presentation contains the presenters' opinions.**
  Opinions may not reflect the opinions of Tandem.
- **This presentation is proprietary.**
  Unauthorized release of this information is prohibited.

KEYS

2

Audrey Magennis

Director
Cherry Bekaert

Cherry Bekaert
Your Guide Forward

KEYS

3

ABOUT CHERRY BEKAERT

Digitally driven, industry-aligned advisory, tax, and assurance services, leveraging practical knowledge and proven experience to **help middle-market financial institutions meet their financial, operational, regulatory and strategic goals.**

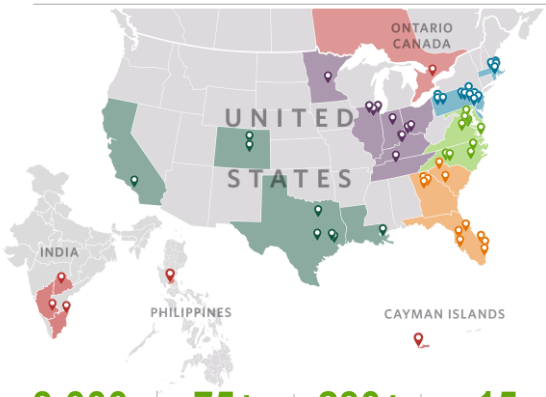
100+
Dedicated Industry Professionals

Specialized Credentials
CPA, CIA, CRCM, AAP, CITP, CAMS, CISA

Significant Industry Association Involvement & Regulator Relationships

420+
Financial Institutions Clients

55+ North American Offices & Global Reach



3,000	75+	230+	15
Employees	Years in Business	Partners	Acquisitions Since 2022

KEYS

4

ASSET TYPES FEEDING THE RISK ASSESSMENT

Each asset category contributes distinct risk vectors that must be inventoried and evaluated as inputs to the formal risk assessment.

KEYS

5

KEY THREAT CATEGORIES

TECHNOLOGY	INFORMATION SECURITY	CYBERSECURITY
System/Application Failures	Unauthorized Data Access	Ransomware & Malware
Legacy System Vulnerabilities	Data Leakage / Exfiltration	Phishing / Social Engineering
IT Infrastructure Outages	Insider Threats	DDoS Attacks
Unpatched Software & OS	Weak Access Controls / IAM	Advanced Persistent Threats
Cloud Misconfiguration	Regulatory Non-Compliance	Credential Compromise
Disaster Recovery Gaps	Third-Party Data Breaches	Supply Chain Attacks

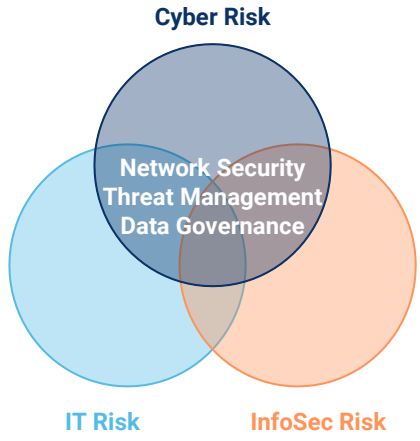
Financial institutions face threats spanning all three domains simultaneously — requiring an integrated assessment approach.

KEYS

6

SAMPLE IT RISK ASSESSMENT

Intersection	Shared topics	Why it matters
IT Risk/InfoSec	Data availability, backup integrity, access controls on IT systems	IT outages can expose data; access controls are both IT and InfoSec concerns
IT Risk/Cyber	Network infrastructure security, patch management, endpoint hardening	Unpatched systems are an IT risk AND a cybersecurity attack surface
InfoSec/Cyber	IAM, threat intelligence, incident response, encryption in transit/at rest	Most cybersecurity attacks target information assets — shared ownership
All three	Vendor/third-party risk, cloud security, BCP/DR, privileged access	Enterprise-wide risks that require cross-functional assessment and ownership



KEYS

7

RISK RATINGS FRAMEWORK

INHERENT RISK

Critical
Immediate threat to operations / compliance

High
Significant exposure requiring urgent action

Moderate
Noticeable risk; monitor and mitigate

Low
Minimal impact with existing controls

LIKELIHOOD

Almost Certain
>80% probability in 12 months

Likely
50–80% probability

Possible
20–50% probability

Unlikely
<20% probability

IMPACT

Significant
>Organization wide or material consequences

High
Serious disruption or exposure

Moderate
Noticeable, but manageable impact

Low
<Minimal disruption or exposure

CONTROLS

Strong
Automated, tested, and audited controls

Adequate
Effective but with minor gaps noted

Partial
Controls exist but inconsistently applied

Insufficient
Weak or absent controls; residual risk high

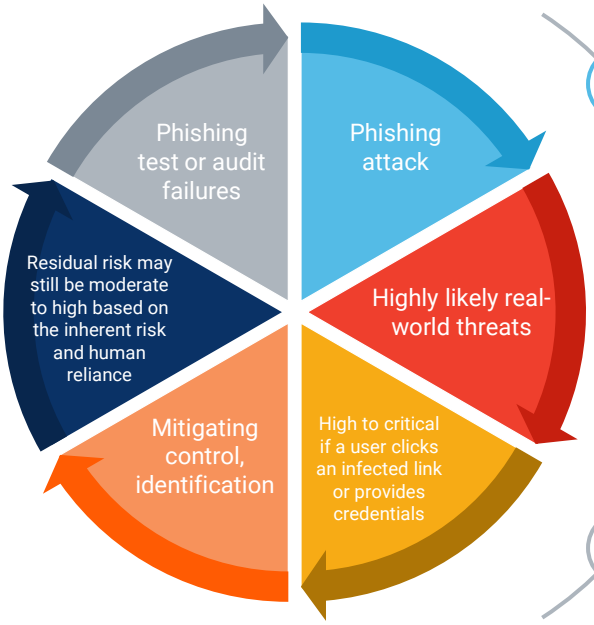
Residual Risk = Inherent Risk adjusted by the strength of Mitigating Controls. Likelihood further weights each risk score.

KEYS

8

WALKTHROUGH SPECIFIC RISK

KEYS



- SPAM, malware, attachment blocking and/or sandboxing
- MFA, password vaulting/complex passwords, remote access/VPN
- Security Awareness training, role-based training, frequent Phishing simulation tests
- User reporting (report Phish button), Incident Response Procedures and Training
- Formal Policies, Board reporting, KPI monitoring, Board training, Tabletop Exercises
- Reduced public exposure, monitoring for impersonation domains, executive specific phishing exercises

9

SAMPLE RISK ASSESSMENT TEMPLATE & HEAT MAP

KEYS

RISK HEAT MAP

	Negligible	Minor	Moderate	Major	Critical
Almost Certain	5	10	15	20	25
Likely	4	8	12	16	20
Possible	3	6	9	12	15
Unlikely	2	4	6	8	10
Rare	1	2	3	4	5

LEGEND

High (15–25) | Medium-High (10–14) | Medium (5–9) | Low (1–4)

SAMPLE RISK REGISTER

Risk / Threat	Inherent	Likelihood	Impact	Control	Residual
Ransomware Attack	Critical	Likely	High	Partial	High
Core Banking Outage	High	Possible	Medium	Adequate	Moderate
Phishing / BEC	High	Likely	High	Adequate	Moderate
Third-Party Breach	High	Possible	Medium	Partial	High
Insider Data Theft	Moderate	Unlikely	Low	Adequate	Low
DDoS Attack	Moderate	Possible	Medium	Strong	Low
Unpatched Vulnerabilities	High	Almost Certain	Significant	Insufficient	Critical
Cloud Misconfiguration	Moderate	Possible	Medium	Partial	Moderate

10

PULLING IT ALL TOGETHER: THE ASSESSMENT LIFECYCLE

KEYS

1	2	3	4	5
Asset Inventory	**Threat Identification**	**Risk Rating**	**Heat Map & Register**	**Treat & Monitor**
Catalog all IT assets across hardware, software, data, network, vendors, and staff	Map threats across technology, infosec, and cybersecurity domains per asset type	Score inherent risk, likelihood and evaluate existing mitigating controls	Plot residual risks on heat map; document in risk register with ownership and due dates	Apply controls, accept, transfer or avoid risks; review quarterly

OUTCOME: *A defensible, board-ready IT Risk Assessment aligned to FFIEC, NIST CSF, and Regulatory requirements — with clear ownership, timelines, and remediation plans.*

11

IT RISK ASSESSMENT

Financial Institution — Technology, Information Security & Cybersecurity

Assessment Period: Q1 2026 | Prepared by: IT Risk & Compliance Team | Classification: CONFIDENTIAL

1. PURPOSE & SCOPE

This IT Risk Assessment identifies, evaluates, and prioritizes technology, information security, and cybersecurity risks facing the institution. It supports compliance with FFIEC IT Examination Handbooks, NIST Cybersecurity Framework (CSF), and applicable regulatory guidance. Risk scores reflect the **inherent risk** level adjusted by the strength of **mitigating controls** to determine the **residual risk** posture.

Institution	ABC Bank — All Lines of Business
Assessment Date	March 2026
Domains Covered	Technology Infrastructure, Information Security, Cybersecurity
Regulatory Alignment	FFIEC, NIST CSF 2.0, ISO 27001, GLBA
Next Review	September 2026 (semi-annual cadence)

2. RISK RATING METHODOLOGY

Risks are scored using a **5×5 matrix** combining **Inherent Risk / Impact** and **Likelihood of Occurrence**. The resulting score (1–25) is then adjusted downward based on the effectiveness of **Mitigating Controls** to arrive at a **Residual Risk** rating.

INHERENT RISK / IMPACT	LIKELIHOOD	MITIGATING CONTROLS
Critical — Catastrophic — operations, solvency, or legal jeopardy	**Almost Certain** — >80% probability in next 12 months	**Strong** — Automated, tested, audited — significant risk reduction
High — Significant financial, reputational, or regulatory harm	**Likely** — 50 – 80% probability	**Adequate** — Effective controls with minor gaps
Moderate — Noticeable disruption; manageable with effort	**Possible** — 20 – 50% probability	**Partial** — Controls exist but inconsistently applied
Low — Minor impact; routine recovery	**Unlikely** — 5 – 20% probability	**Insufficient** — Weak or absent — high residual exposure
Negligible — Minimal; no meaningful effect	**Rare** — <5% probability	**None** — No controls in place

Residual Risk Formula: Raw Score = Likelihood Score × Impact Score (1–25). Residual Risk adjusts the raw score downward based on control effectiveness: Strong (−2 levels), Adequate (−1 level), Partial (no change), Insufficient/None (+1 level).

Purpose, Scope, Risk Methodology

- Establishes **what risks are being evaluated and why**, ensuring the assessment supports Board oversight and strategic decision-making.
- Defines **what is included and excluded**, preventing gaps, overlaps, or misinterpretation of reported risk levels.
- Applies a **consistent likelihood and impact framework** to prioritize risks based on potential business effect.
- Clearly distinguishes **inherent risk verses residual risk**, enabling the Board to see where controls are effective and where risk remains above tolerance.

KEYS

12

3. RISK HEAT MAP

RISK HEAT MAP (Likelihood × Impact)

← LIKELIHOOD → \ ← IMPACT →	Negligible	Minor	Moderate	Major	Critical
Almost Certain	5	10	15	20	25
Likely	4	8	12	16	20
Possible	3	6	9	12	15
Unlikely	2	4	6	8	10
Rare	1	2	3	4	5

4. RISK REGISTER — SAMPLE ENTRIES

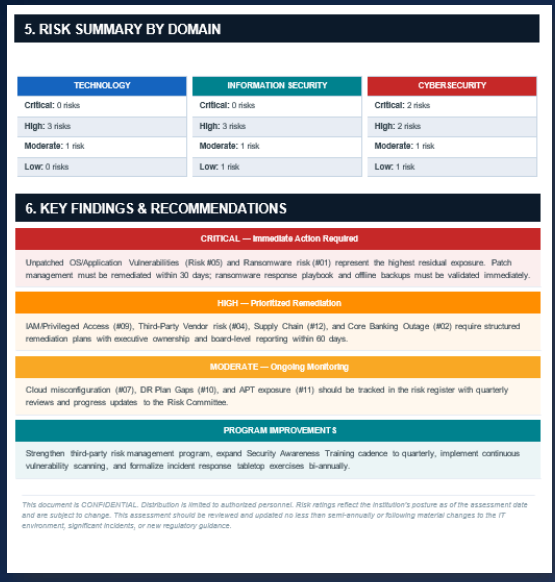
#	Risk / Threat	Domain	Asset Type	Inherent Risk	Likelihood	Controls	Residual Risk	Owner	Due Date
01	Ransomware / Extortion Attack	Cybersecurity	Network	Critical	Likely	Partial	Critical	CISO	Apr 2026
02	Core Banking System Outage	Technology	Software	Critical	Possible	Adequate	High	CTO	May 2026
03	Phishing / Business Email Compromise	InfoSec	Personnel	High	Likely	Adequate	Moderate	InfoSec	Apr 2026
04	Third-Party Vendor Data Breach	InfoSec	Vendors	High	Possible	Partial	High	Vendor Mgmt	Jun 2026
05	Unpatched OS / Application Vulns	Technology	Hardware	High	Almost Certain	[redacted]	Critical	IT Ops	Mar 2026
06	Insider Threat / Data Exfiltration	InfoSec	Personnel	High	Unlikely	Adequate	Low	HR/InfoSec	Ongoing
07	Cloud Misconfiguration	Cybersecurity	Network	Moderate	Possible	Partial	Moderate	Cloud Team	May 2026
08	DDoS Attack on Online Banking	Cybersecurity	Network	Moderate	Possible	Strong	Low	NetOps	Ongoing
09	Weak IAM / Privileged Access	InfoSec	Software	High	Likely	Partial	High	IAM Team	Apr 2026
10	Disaster Recovery Plan Gaps	Technology	All	High	Unlikely	Partial	Moderate	BCP Team	Jun 2026
11	Advanced Persistent Threat (APT)	Cybersecurity	Network	Critical	Unlikely	Adequate	Moderate	CISO	Ongoing
12	Supply Chain / SW Dependency Attack	Cybersecurity	Software	High	Possible	Partial	High	CTO	Jul 2026

Risk Heat Map | Risk Register

- A **quick view of the most significant IT risks**, prioritized by likelihood and business impact.
- Enables the Board to quickly identify **which risks require immediate attention versus ongoing monitoring**.
- Serves as the **authoritative record of material IT risks**, including ownership, mitigation actions, and status.
- Allows the Board to track **whether risks are being actively managed and trending in the right direction**.

KEYS

13



5. RISK SUMMARY BY DOMAIN

TECHNOLOGY	INFORMATION SECURITY	CYBERSECURITY
Critical: 0 risks	**Critical:** 0 risks	**Critical:** 2 risks
High: 3 risks	**High:** 3 risks	**High:** 2 risks
Moderate: 1 risk	**Moderate:** 1 risk	**Moderate:** 1 risk
Low: 0 risks	**Low:** 1 risk	**Low:** 1 risk

6. KEY FINDINGS & RECOMMENDATIONS

CRITICAL — Immediate Action Required

Unpatched OS/Application Vulnerabilities (Risk #05) and Ransomware risk (#01) represent the highest residual exposure. Patch management must be remediated within 30 days; ransomware response playbook and offline backups must be validated immediately.

HIGH — Prioritized Remediation

IAM/Privileged Access (#09), Third-Party Vendor risk (#04), Supply Chain (#12), and Core Banking Outage (#02) require structured remediation plans with executive ownership and board-level reporting within 60 days.

MODERATE — Ongoing Monitoring

Cloud misconfiguration (#07), DR Plan Gaps (#10), and APT exposure (#11) should be tracked in the risk register with quarterly reviews and progress updates to the Risk Committee.

PROGRAM IMPROVEMENTS

Strengthen third-party risk management program, expand Security Awareness Training cadence to quarterly, implement continuous vulnerability scanning, and formalize incident response tabletop exercises bi-annually.

This document is CONFIDENTIAL. Distribution is limited to authorized personnel. Risk ratings reflect the institution's posture as of the assessment date and are subject to change. This assessment should be reviewed and updated no less than semi-annually or following material changes to the IT environment, significant incidents, or new regulatory guidance.

Risk Summary | Recommendations

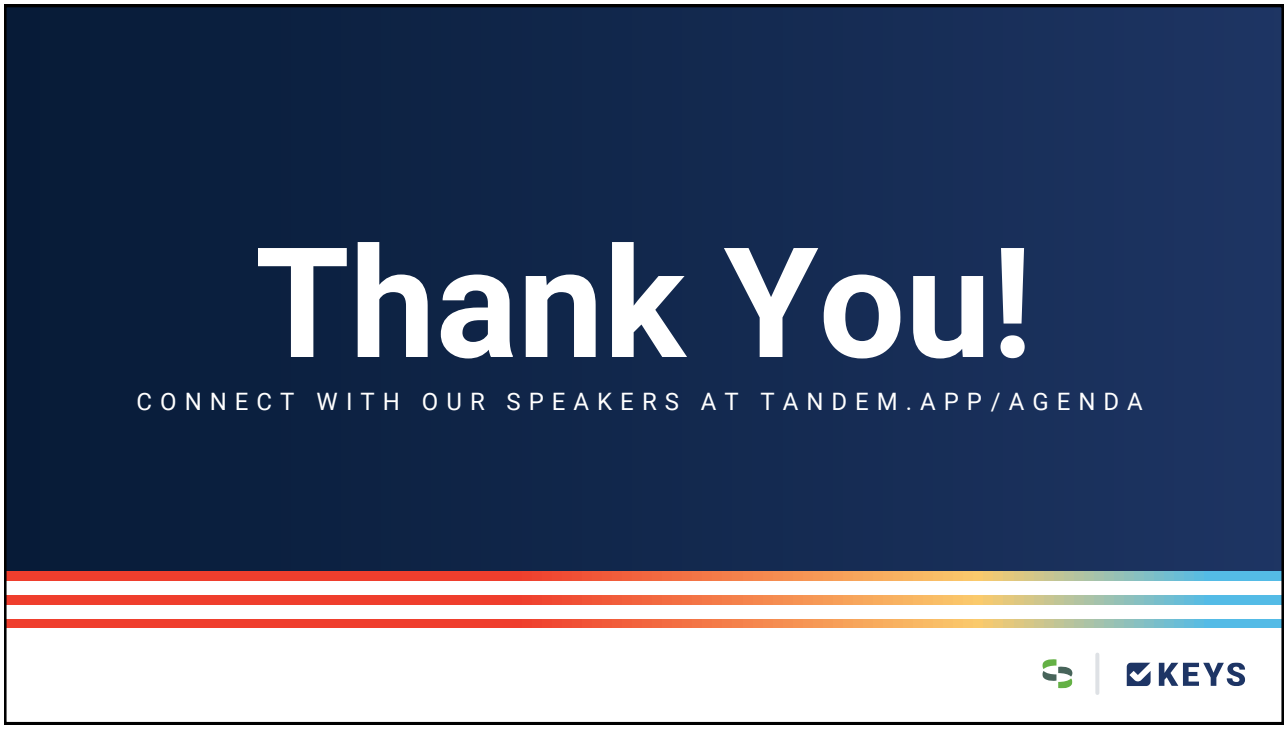
- Provides a **concise view of risk levels across major IT domains** (i.e. cyber, TPRM, resilience), enabling the Board to understand where risk is concentrated.
- Highlights **relative risk exposure**, allowing the Board to focus oversight on domains with the greatest potential business impact.
- Summarizes the **most significant control gaps and risk drivers** identified during the assessment.
- Presents **clear, actionable recommendations** to reduce risk and align exposure with the Board's risk appetite, supporting informed prioritization and investment decisions.

KEYS

14

15

16


Thank You!
CONNECT WITH OUR SPEAKERS AT TANDEM.APP/AGENDA
KEYS

17