AUGUST 20, 2026

21st IIA Atlanta Conference

Cyber & Third-Party Risk Without the Jargon

Agenda

1. INTRODUCTIONS
2. CYBER RISK
3. TPRM RISK
4. QUESTIONS

Introductions

Donel Martinez

Technology Solutions and Risk Director

Scott Campbell

Technology Solutions Manager

Cyber Response & Materiality

myna PARTNERS

SEC cyber disclosure: the rule remains in force—but the story has evolved

MAR 2022

PROPOSAL
Standardize incident and annual cyber-risk disclosures.

JUL–DEC 2023

FINAL RULE GOES LIVE
Effective Sept. 5; compliance phased in Dec. 2023–Jun. 2024.

MAY–JUN 2024

STAFF CLARIFIES
Item 1.05 = material only; use Item 8.01 for voluntary disclosure.

JUN–OCT 2024

ENFORCEMENT
RRD: $2.1M. Four SolarWinds customers (CHKP, UIS, AVYAQ, MIME): ≈$7M total.

2025–AUG 2026

RULE STILL IN FORCE
Rescission petition pending; SolarWinds case dismissed with prejudice. However, settled with class-action from investors.

A material incident starts a four-business-day disclosure clock

ITEM 1.05 • FORM 8-K

4 BUSINESS DAYS

The clock begins when the company determines the incident is material—not when it is first discovered.

CYBERSECURITY INCIDENT

Unauthorized occurrence—or related occurrences—that jeopardizes the confidentiality, integrity, or availability of information systems or the information in them.

01	**TRIGGER**	A cybersecurity incident is determined to be material.
02	**DISCLOSE**	Material aspects of its nature, scope and timing—and its material or reasonably likely material impact.
03	**DELAY**	The Attorney General may authorize delay when immediate disclosure would substantially risk national security or public safety.
04	**FOLLOW UP**	Amend the Form 8-K when required information was unavailable or not determined at the initial filing.

Source: SEC Release No. 33-11216 (July 26, 2023), Form 8-K Item 1.05.

Materiality depends on the reasonable investor—not a numeric threshold

THE DECISION TEST

Would the incident alter the "total mix" of information available to a reasonable investor?

There is no automatic dollar, severity or data-record threshold.

- **OBJECTIVE** Use the investor's perspective—not management's preferred outcome.
- **HOLISTIC** Consider qualitative and quantitative evidence together.
- **FACT-SPECIFIC** Assess all circumstances and immediate and longer-term consequences.

TEST THE INCIDENT ACROSS SIX DIMENSIONS

01	**OPERATIONS**	Disruption, downtime, recovery and business continuity
02	**FINANCIAL**	Costs, lost revenue, financial condition and results
03	**DATA & SYSTEMS**	Sensitivity, scope and confidentiality / integrity / availability
04	**LEGAL & REGULATORY**	Claims, investigations, reporting duties and potential penalties
05	**CUSTOMERS & PARTNERS**	Trust, contracts, critical vendors and dependencies
06	**REPUTATION & COMPETITION**	Brand, market position and longer-term consequences

Sources: TSC Industries v. Northway, 426 U.S. 438 (1976); Basic v. Levinson, 485 U.S. 224 (1988); SEC Release No. 33-11216.

Materiality is already embedded in public-company reporting

MICROSOFT FY2026 FORM 10-K • AUDITOR'S REPORT

REPORT OF INDEPENDENT REGISTERED PUBLIC ACCOUNTING FIRM

To the Stockholders and the Board of Directors of Microsoft Corporation
Opinion on the Financial Statements

"In our opinion, the financial statements present fairly,

in all material respects,

the financial position of the Company as of June 30, 2026 and 2025, and the results of its operations and its cash flows … in conformity with accounting principles generally accepted in the United States of America."

WHERE TO LOOK Auditor's Report → Opinion on the Financial Statements

WHAT THIS ADDS TO THE STORY

01 FAMILIAR DISCIPLINE

"Material" is already a core concept in external reporting.

02 ESTABLISHED GOVERNANCE

Management, audit committees and auditors already make and challenge materiality judgments.

03 IMPORTANT LIMIT

The cyber decision is not an accounting percentage or a financial-statement-only test.

TAKEAWAY **Borrow the discipline—not a financial-only threshold.**

Source: Microsoft Corporation Form 10-K, fiscal year ended June 30, 2026, Report of Independent Registered Public Accounting Firm. Cyber materiality remains governed by the traditional securities-law standard.

Existing controls provide the operating model for cyber escalation

MICROSOFT FY2026 FORM 10-K • ITEM 9A

REPORT OF MANAGEMENT ON INTERNAL CONTROL OVER FINANCIAL REPORTING

"Our management is responsible for establishing and maintaining adequate internal control over financial reporting for the Company."

Internal control over financial reporting is a process to provide reasonable assurance regarding the reliability of external financial reporting.

The control system is designed so activity with a **material effect** on the financial statements would be **prevented or detected on a timely basis**.

WHERE TO LOOK Item 9A → Controls and Procedures

Next: translate the escalation discipline into a cross-functional cyber incident decision framework.

Source: Microsoft Corporation Form 10-K, fiscal year ended June 30, 2026, Item 9A.

TRANSLATE THE DISCIPLINE TO CYBER

01 CAPTURE

Establish reliable facts; quantify what is known and unknown.

02 ROUTE

Move incident information to legal, finance and disclosure decision-makers.

03 DECIDE

Document the investor-focused materiality analysis and assumptions.

04 ACT & UPDATE

File or amend when required—and retain the evidence trail.

GUARDRAIL **ICFR is narrower than disclosure controls; use its discipline, not its scope.**

A practical Cyber Incident materiality decision framework

INCIDENT OCCURS	INCIDENT IMPACTS DATA	REGULATED DATA IMPACTED	DOWNTIME	THIRD-PARTY	CONTRACTUAL OBLIGATIONS
Does incident meet internal policy criteria as being “severe” or “critical”? Is incident ongoing? Are critical systems impacted including SOX systems? Can incident be quantified based on systems impacted? Is incident related to SOX deficiency?	Known or possible exfiltration of data? Was sensitive data compromised? Was sensitive-compromised data unencrypted? Can volume/records of sensitive data be determined?	Industry data (e.g., PCI). Government data (e.g., PHI).	Was downtime experienced? Did the DR/BCM processes get triggered?	Did critical outsource service provider incident impact firm operations?	Any significant breaches to customer agreements? Any obvious changes to existing litigation or prior settlements?
If NO, then go to next column. If YES, then evaluate for disclosure	If NO, then go to next column. If YES, then evaluate for disclosure	If NO, then go to next column. If YES, then evaluate for disclosure	If NO, then go to next column. If YES, then evaluate for disclosure	If NO, then go to next column. If YES, then evaluate for disclosure	If YES, then evaluate for disclosure

IR Materiality RACI

RESPONSIBLE (R)	Person that works to complete the task. **Control Performer**.
ACCOUNTABLE (A)	Ultimately answerable for the correct and thorough completion of the task. Must sign off (approve). **Control Owner**.
CONSULTED (C)	Person that would provide suggestions and will be consulted prior to completion of task.
INFORMED (I)	Person that is kept up-to-date on progress, often only on completion of the task or deliverable; and with whom there is just one-way communication.

Activity	BoD	CEO	CFO	General Counsel	CISO
Item 9A controls and disclosures certification process	I	A	R	C	C
Quarterly Disclosure Committee update	I	I	C	A	R
Determine incident materiality					
Incident response process policy & procedure					
Third party cyber risk oversight					
Determine whether cybersecurity threat exist					
Description of cybersecurity processes incorporated into overall risk management processes or systems					
Description of board/subcommittee oversight of risks from cybersecurity threats					
Description of management's role in assessing and managing material risks from cybersecurity risks					
Collection and aggregation of incident information, including third parties					
Disclosure filings of 8K's					
Disclosure filings of 10K's					

Validate Cyber Maturity

myna PARTNERS

Read Item 1C as a map of how cyber risk is governed

MICROSOFT FY2026 FORM 10-K • A LEARNING EXAMPLE

"We operate a cybersecurity program and governance framework … ***and we have controls, policies, and procedures to identify, manage, and mitigate cybersecurity threats."***

WHEN READING ANY ITEM 1C DISCLOSURE, LOCATE FOUR THINGS

01	**PROCESS**	How risk is identified, assessed and managed.
02	**INTEGRATION**	How cyber risk connects to enterprise risk and strategy.
03	**VALIDATION**	How the program is monitored, tested and improved.
04	**THIRD PARTIES**	How third-party and supply-chain risk is governed.

IIA LEARNING LENS

TRANSLATE	Turn each statement into a testable control claim.
LOCATE	Identify the owner, cadence, evidence and exceptions.
COMPARE	Determine whether actual practice supports the narrative.

TAKE IT BACK **Choose one Item 1C paragraph and list the evidence that would make it supportable.**

Source: Microsoft Corporation Form 10-K, fiscal year ended June 30, 2026, Item 1C. Item 106 requires disclosure of material process and governance information.

Trace how cyber facts become governance decisions

MICROSOFT FY2026 FORM 10-K • INCIDENT RESPONSE & GOVERNANCE

“Incidents are first triaged for severity, and then more deeply assessed to establish a plan of record and activate internal and external notification, disclosure, and communication plans, as applicable.”

01 TRIAGE	02 ASSESS	03 ESCALATE	04 ACT	05 LEARN
What happened?	What is the impact?	Who must decide?	Disclose / respond	What must change?

WHAT INTERNAL AUDIT CAN TEACH AND TEST

THRESHOLDS	DECISION RIGHTS	RECORD	FEEDBACK
Are severity and escalation criteria understood?	Are accountable decision-makers named and available?	Can the timeline, inputs, judgments and approvals be reconstructed?	Do incidents change controls, risk ratings and plans?

ROLE BOUNDARY **Audit does not decide disclosure; it evaluates whether information is timely, complete and evidenced.**

Source: Microsoft Corporation Form 10-K, fiscal year ended June 30, 2026, Item 1C.

Use maturity as a learning lens—not a compliance score

ITEM 106 DOES NOT REQUIRE A MATURITY RATING • THE MODEL HELPS ORGANIZE OBSERVATIONS

1 INITIAL	2 DEVELOPING	3 DEFINED	4 MANAGED	5 OPTIMIZING
Reactive and person-dependent	Structure is emerging	Common process and evidence	Repeatable, measured and integrated	Evidence drives improvement

ASK THREE QUESTIONS BEFORE ASSIGNING A LEVEL

DESIGN

Are roles, thresholds and workflows defined?

EXECUTION

Do people follow them consistently and at the right time?

EVIDENCE

Could an independent reviewer reproduce the conclusion?

GUARDRAIL **Use maturity to support judgment and learning—not to imply SEC certification or a required score.**

IRM – Maturity Rating Definitions

GRC AREA	INITIAL	DEVELOPING	DEFINED	MANAGED	OPTIMIZING
Policy Management	Reactive approaches to policy management at the department level. No active management of policies; few if any resources are allocated to policy management. The department addresses policy management in a reactive mode - writing policies when forced to.	Departments with some structure and focus on policy management within respective functions, but not working together. Information and processes are highly redundant, manual, document-centric, and lack integration. With siloed approaches to policy management, the organization is still very document centric.	Some areas of policy management are managed well at a department level, but it lacks integration to address policy management across departments. Accountability and oversight for certain policy domains are beginning to emerge.	Cross-department strategy for managing policies across departments and functions. Policy management is aligned across several departments to provide consistent strategies, frameworks, templates, and processes supported by a common policy information and technology architecture. The organization addresses policy management through shared processes.	Completely moved to an integrated approach to policy management across the business and leveraging artificial intelligence/cognitive technologies for regulatory change and policy mapping. Consistent core policy management processes in place. Benefits from consistent relevant and harmonized processes for policy management with minimal overhead.
Exception Management	Reactive approaches to exceptions. Exceptions are not actively managed, or are managed in an ad hoc way. Exception management policy is not documented, or documentation is sparse. Few if any resources are allocated to the process. Exceptions are acted upon in a reactionary way.	Exception management policy and processes are being developed. Exceptions are being managed in a less ad hoc way. Minimal staff have been assigned to address exceptions.	Exception management policy is developed, and procedures are beginning to emerge for most scenarios. Mitigation methodology is defined, but not always consistently followed. Accountability over certain domains is starting to emerge. Exception review timelines have been defined. Staff has been improved to capture the developing backlog of exceptions.	Fully developed processes and documentation to manage the exceptions through the entire lifecycle for all scenarios. Processes are repeatable and adopted across the organization. Mitigation methods are consistently followed. Accountability over all domains is in place. Exception review timelines are consistently being followed. Exception management staff is sufficient to manage the exception load.	Integrates the policies and procedures into the existing security framework. It lends visibility into the exception backlog in 'real-time'. Exceptions are reportable and actively managed. Exceptions are reviewed consistently for extension or closure. The organization understands it's risk posture and appetite for risk acceptance in all exception scenarios.
Third-Party Risk Management	Siloed approaches to third-party governance, risk, and compliance at the department level. Businesses at this stage do not understand risk and exposure in third party relationships; few if any resources are allocated to third party governance. The organization addresses third party GRC in a reactive mode — doing assessments when forced to. There is no ownership or monitoring of risk and compliance, and no integration of risk and compliance information and processes in context of third party performance.	Departments with some focus on third party GRC within respective functions - but information and processes are highly redundant and lack integration. With siloed approaches to third party GRC, the organization is still very document-centric. Processes are manual and they lack standardization, making it hard to measure effectiveness.	Some areas of third-party GRC are managed well at a department level, but it lacks integration to address third party risk across departments. Defined processes for third-party GRC in some departments or business functions, but there is no consistency. Third party GRC processes have the beginning of an integrated information architecture supported by technology and ongoing reporting. Accountability and oversight for certain domains such as bribery and corruption risk and compliance, and/or information Security are beginning to emerge.	Cross-department strategy for managing third-party governance across risk and compliance. Third-party GRC is aligned across several departments to provide consistent frameworks and processes. The organization addresses third party GRC through shared processes and information that achieve greater agility, efficiency, and effectiveness. However, not all processes and information are completely integrated, and there is not an integrated view of third party performance.	Organization has completely moved to an integrated approach to third party GRC across the business that includes an understanding of risk and compliance in context of performance and objectives in third party relationships. Consistent core third party GRC processes span the entire organization. The organization benefits from consistent, relevant, and harmonized processes for third party governance with minimal overhead.
Identity & Access Management	Fragmented identity experience across the organization. Strategy and technology are lacking, thus not enabling digital identities.	Identity has centralized management, and some technology has been implemented, but processes are mainly manual.	Centralized management adopted more widely across the company, and processes have been automated. Identity management has been digitalized.	Processes are centralized and automated, advanced tools such as AI and predictive use cases have been implemented.	Identity management is serving as a critical control point in reducing cybersecurity risk and supporting business in next-generation technology innovation.

IRM – Maturity Rating Definitions

GRC AREA	INITIAL	DEVELOPING	DEFINED	MANAGED	OPTIMIZING
Security Operations	Majority of processes are ad hoc and undocumented. Unvalidated data is being sent blindly to the SIEM with no context. Fragmented teams, processes, and tools exist. Alert overload is a common theme. Reactive instead of proactive due to the volume of work and inability to get ahead.	Although visibility has improved, little to no automation exists. Team is often small, inundated, and overworked. Processes are documented but mostly completed manually. Tools in place are disparate and not communicating the way that they should. Team members express desire to do more advanced, or different, types of work.	Stable security program with defined processes. A threat intelligence, security automation, and/or Incident Response Platform is in place. Reports are being generated but may not be demonstrating the business value & selling security to other departments. Removed immediate need for additional headcount to meet requirements.	Organizations recognize they are unaware of many high-impact threats. They have invested in the organizational processes and headcount to significantly improve ability to detect and respond to all classes of threats. Have invested in and established a formal security operations and incident response center (SOC) that is running effectively with trained staff	Extremely clearly defined processes and playbooks where the security team is working collaboratively across the department. Threat intelligence is used across the program to increase efficiency and accuracy across all functional areas. The SOC is running 24/7 physical or virtual. Extensive automation of investigation and mitigation workflow is in place. Log data; security events; server, network and endpoint forensics are holistic and centralized.
Business Continuity & Disaster Recovery	Organization has launched BCM by defining the scope, establishing a BCM policy and by having assigned the organizational roles, responsibilities and authorities required by the initiative. The core business processes have been recognized. Management demonstrates leadership and commitment with respect to the BCM program. A clear owner has been defined for BCM, who has the necessary power and influence to fulfill the tasks. The BCM initiative has been established.	BIA and risk assessments have been performed and by using the outputs from these a business continuity strategy has been determined and selected. Business continuity objectives have been determined based on the BCM policy, and plans have been made to achieve these objectives. Roles and responsibilities are starting to develop. The BCM blueprint has been established.	Established and implemented business continuity procedures, including incident response structure and business continuity plans. BCM awareness is promoted and exists among the employees - everyone knows their role in respect to the BCM related plans. Internal communication plans and procedures for crisis situations exist. Initial tests and exercises have been planned and conducted ensuring the validity of the plans. BCM is more of a project - it is not yet a continuous process.	At this stage, BCM is finally considered a process instead of a project. An organization on this level measures, analyzes and evaluates its BCM as well as conducts exercises and tests on a regular basis on its business continuity procedures to ensure they are consistent with the objectives. External communication plans and procedures for the times of crisis exist. The BCM is reviewed by management.	Organization is maximizing its BCM by aiming at continually improving its suitability adequacy and effectiveness. Internal and external audits are performed at planned intervals to monitor need for changes or opportunities for improvement in BCM. Management reviews are conducted on a regular schedule at this level. The organization utilizes its BCM excellence strategically, for example to gain commercial advantage or to strive for operational excellence as a business strategy.
Asset Management	Capabilities are characteristic of individuals, not of the organization. IT Asset Management strategy, process, and responsibilities are not defined. Processes are ad hoc. Technology solutions are not utilized. Accurate inventories do not exist. There are no specific vendor relationships developed for IT asset purchases.	Processes and discipline exist to allow for repeatable results. Informal IT asset request process is in place. Inventories are manually created. Company's economies of scale are leveraged for IT asset purchases, and hardware and software are viewed separately.	Processes are standardized across the organization. ITAM Program is in place. Policies, procedures, roles and responsibilities have been communicated. Service level agreements are defined. Process metrics are utilized. ITAM tool integrated to auto-discovery, and the ITAM tool is linked to financial and contract management system.	Risks are measured and managed quantitatively and aggregated on an enterprise-wide bases. Asset management has been Integration with other technology management tools (e.g., Help Desk, Change Management). Performance metrics against functional requirements are monitored. Process improvements are identified and implemented. Automated requisition is integrated with purchased and ERP systems.	Focused on continuous improvement. Process metrics are well-established, consistently analyzed, and process/service level performance is linked directly with IT management performance. Fines and violations of software and hardware agreements rarely occur, or not at all. There is a cost recovery process in place. Decision support and analytic tools are available for mining asset data.
Vulnerability Management	Vulnerability assessment solution is in place; however, it is performing ad-hoc vulnerability scanning. Basic patching Processes & metrics exist.	Scanning is driven by regulatory framework. Scheduled vulnerability scanning occurs, and there is a scan to patch lifecycle. Emerging processes are developing, however, there is little measurability and busy metrics.	Risk focused scan data prioritized through analytics. Patching is data- driven by priority. Processes are now measurable, and there are emerging metrics and trends.	Scanning is attacker and threat focused, and multiple threat vectors are scanned and prioritized. Patching is based on risk to critical assets. Efficient metric-based processes are in place, and threat driven metrics and trends are visible.	Threats and risks aligned with business goals. All threat vectors are scanned and prioritized. Continuous patching is in place. Business and IT processes are unified. Measurement is integrated to enterprise risk management.

IRM – Maturity Rating Definitions

GRC AREA	INITIAL	DEVELOPING	DEFINED	MANAGED	OPTIMIZING
Incident Management	Organizations have an awareness that cyber incidents are taking place, but enterprise preparedness for cyber incidents doesn't exist.	IT security teams attempt to mitigate cyber incidents in an unstructured fashion, primarily focused on "crisis-level" response. At this stage, the escalation thresholds from alert to event to incident to crisis are not well defined.	Organizations invest in and develop minimum resources, policies and processes for ongoing detection and response. Response teams are enabled to make decisions regarding mitigation vs. remediation.	Enhanced, repeatable IR program. Organization has matured to incorporate automated response activities. The IR program contributes to security strategy and feeds crisis management and continuous operations programs/plans.	Global enterprise IM program matures to take proactive actions based on threat landscape. The business is a key partner of the security IM process; integrates business risk and can evidence contribution to the corporate strategy and/or bottom line.
Risk Management & Risk Assessment	Risk management is ad hoc/chaotic and depends primarily on individual heroics, capabilities, and verbal wisdom.	Risk is defined differently at different levels of the organization. Risk is managed in silos, and risk interactions are identified in limited manner. There is limited alignment of risk to strategies, and disparate monitoring and reporting functions exist.	Common risk assessment, program statement, and policy Enterprise-wide integrated risk assessments. Communication of top strategic risks to the board occurs along with Executive/steering committee Knowledge sharing across risk functions. A dedicated risk team is in place to manage risk.	Coordinated risk management activities across silos. Risk appetite is fully defined. Enterprise-wide risk monitoring, measuring. And reporting is in place. Technology-enabled processes exist. Contingency plans and escalation procedures are developed, and regular risk management training happens company-wide.	Risk discussions are embedded in strategic planning, capital allocation, product development, etc. Risk sensing and early warning risk indicators are used. Linkage to performance measures and incentives are part of the human resource element. Risk modeling/ scenarios are regular practice, and industry benchmarking is used regularly.
Compliance Training	Security awareness practices do not exist in the company. Employees easily fall victim to cyber-attacks.	Program is compliance focused and created to meet specific compliance regulations. Training is provided on ad-hoc basis.	Organization promoting awareness and behavior change. The training program is communicated in a positive & engaging manner. Employees understand and recognize awareness policies.	Long-term sustainment and culture change is in place. Security awareness programs are part of the organization's culture.	A metric framework exists to analyze the effect of training (e.g., phishing, ransomware & other attacks reduced by 75%).
Privacy & Legal	Identification of personal information is irregular, incomplete, inconsistent, and potentially out of date. Personal information is not adequately addressed in the organization's privacy and related security policies and procedures. Personal information may not be differentiated from other information.	Basic categories of personal information have been identified and covered in the entity's security and privacy policies. However, the classification may not have been extended to all personal information.	All personal information collected, used, stored and disclosed within the entity has been classified and risk rated.	All personal information is covered by the entity's privacy and related security policies and procedures. Procedures exist to monitor compliance. Personal information records are reviewed to ensure appropriate classification.	Management maintains a record of all instances and uses of personal information. Changes to business processes and procedures and any supporting computerized systems result in an updating of personal information records. Personal information records are reviewed regularly to ensure appropriate classification.
Regulatory Compliance	Unstructured approach. Constantly putting out fires. Often caught off guard.	Limited structure in regulatory change responsibilities. Process is accomplished via email and documents with limited accountability and oversight.	Roles & responsibilities are defined with use of technology to manage workflow and tasks to provide accountability. Inconsistencies remain. There is no integration of technology and content.	Regulatory intelligence architecture across the organization enables consistent management of regulatory change process with the integration of content feeds from regulatory intelligence knowledge providers.	Regulatory intelligence architecture that integrates feeds from regulatory knowledge providers that map to policies, risks, controls, etc. Enables full situational awareness of regulatory change in the context of business.
Audit & Assessment	Limited number of samples in audit testing. Audits are Point-in-time, consist of manual analysis. Audits are time-consuming and have error-prone processes.	Data extractions are completely manual; however, more frequent audits are occurring. Rules and algorithms used for analysis. Roughly 50% audit coverage.	Continuous audit process. There is reduced overhead. Ability to correlate data across complex processing/ transactions. Exceptions are auto discovered. There is 100% audit coverage.	Automated controls are monitored on a 'real-time' basis and potential exceptions are flagged to risk and/or controls owners on a real-time basis. Preventative controls exist that stop events at run-time. Control weaknesses are identified and remediated in a 'real-time' manner prior to risk materializing.	KPI to KRI monitoring is active. Advanced data analytics are incorporated into audits. Proactive, predictive and timely notification and decision support enables the business to course correct and provides continuous business assurance.

Map Item 106 topics to the GRC capabilities that support them

ITEM 106 DISCLOSURE TOPIC	GRC CAPABILITIES THAT PROVIDE SUPPORTING EVIDENCE
RISK-MANAGEMENT PROCESSES	Risk Management & Assessment • Policy / Exception Management • Incident Management • Security Operations • Vulnerability, Asset & Identity Management • BCM / DR
INTEGRATION WITH ENTERPRISE RISK	Risk Management & Assessment • Audit & Assessment • Regulatory Compliance • enterprise reporting and escalation
USE OF THIRD PARTIES	Third-Party Risk Management • Policy / Exception Management • Privacy & Legal • contractual notification and monitoring
BOARD OVERSIGHT	Risk reporting and escalation • Audit & Assessment • Incident Management • governance cadence and minutes
MANAGEMENT'S ROLE & EXPERTISE	Defined accountability • Incident Management • Policy Management • Compliance Training • performance metrics

Score capabilities using observable evidence—not aspiration

ILLUSTRATIVE DEEP DIVE • INCIDENT MANAGEMENT

1 INITIAL	2 DEVELOPING	3 DEFINED	4 MANAGED	5 OPTIMIZING
Awareness exists, but enterprise preparedness does not.	Response is unstructured; alert-to-crisis thresholds are unclear.	Minimum resources, policies and decision processes are established.	Response is repeatable, measured and integrated with crisis and continuity plans.	Threat-informed action is proactive and connected to business risk and strategy.

EVIDENCE THAT SHOULD SUPPORT THE SCORE

GOVERN	EXECUTE	ESCALATE	VALIDATE	MEASURE
Policy, roles, severity criteria and decision rights	Incident records, timelines, playbooks and communications	Materiality assessments, executive / Board escalation records	Exercises, post-incident reviews and remediation tracking	Response metrics, trends, exceptions and improvement actions

SCORING RULE **If the evidence is inconsistent, outdated or unavailable, the capability has not achieved the claimed level.**

Convert maturity gaps into disclosure and remediation priorities

FROM ASSESSMENT TO ACTION

01	02	03	04	05
RATE CURRENT STATE	**SET THE TARGET**	**IDENTIFY THE GAP**	**TEST DISCLOSURE SUPPORT**	**ASSIGN ACTION**
Use the five-level criteria and available evidence.	Align the required level to risk, complexity and strategy.	Separate process weakness from missing evidence.	Ask whether public statements are complete and supportable.	Name the owner, timing, proof and validation method.

PRIORITIZE BY DISCLOSURE RELEVANCE × EVIDENCE WEAKNESS

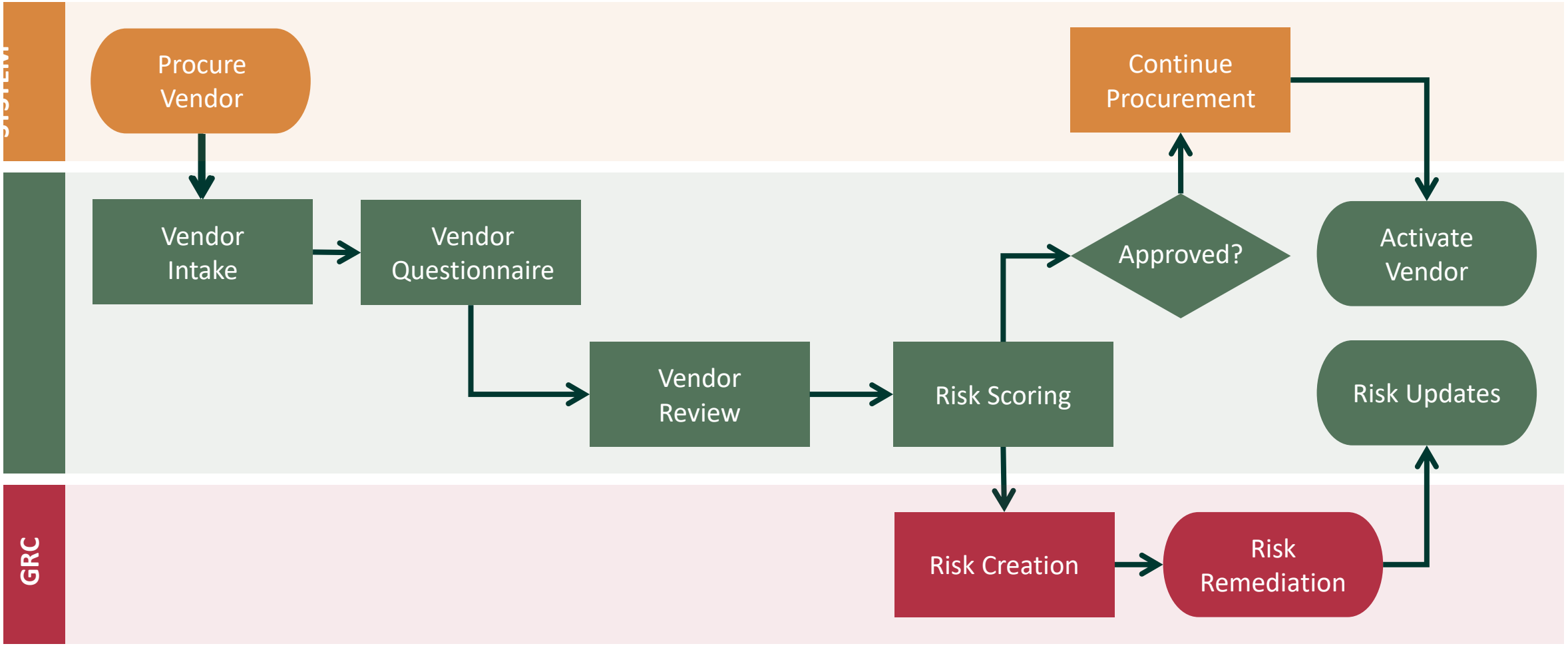
- **IMMEDIATE** — Directly supports an Item 106 topic—and evidence is missing, stale or contradicted.
- **PLANNED** — The process exists but is inconsistent, partially integrated or weakly evidenced.
- **MONITOR** — The capability is repeatable, measured and independently validated.

OUTPUT **A defensible roadmap linking maturity, evidence, disclosure implications, accountable owners and validation.**

Third-Party Risk

myna PARTNERS

Third-Party Risk Management Lifecycle



A complete TPRM program operates as a closed loop

SIX STAGES • ONE CONTROL SYSTEM

01 IDENTIFY & INTAKE

Capture the owner, purpose, data, access and criticality.

02 ASSESS & VALIDATE

Tier risk, corroborate evidence and resolve exceptions.

03 DECIDE & CONTRACT

Document acceptance, approvals and required protections.

04 ACTIVATE & INTEGRATE

Enable payment, access and connectivity only after gates.

05 MONITOR & REMEDIATE

Reassess changes, incidents, performance and open issues.

06 OFFBOARD & LEARN

Remove access, address data, close records and improve.

THE LOOP CLOSES WHEN NEW INFORMATION CHANGES THE DECISION

EVENTS

incidents and control failures

CHANGE

Service, data, access or ownership

PERFORMANCE

SLA, financial and resilience indicators

EXIT

termination, access removal and data disposition

AUDIT TAKEAWAY **Each event must update risk, ownership and action in the system of record.**

Control gates determine whether a vendor can proceed

FIVE NON-NEGOTIABLE DECISION GATES

01 POPULATION

Is the third party captured before spend, access or commitment?

EVIDENCE

Procurement • AP • contracts • IAM

02 TIERING

Does classification reflect service, data, access and criticality?

EVIDENCE

Approved methodology • rationale

03 EVIDENCE

Are claims corroborated and material exceptions addressed?

EVIDENCE

Reports • attestations • review trail

04 AUTHORITY

Did the proper owner accept residual risk and conditions?

EVIDENCE

Approval matrix • escalation • expiry

05 COMMITMENT

Are contract, activation and monitoring requirements complete?

EVIDENCE

Clauses • provisioning • reassessment

NO / NOT YET **Stop, remediate or escalate—do not allow payment, contract execution, access or go-live to become the de facto approval.**

DESIGN PRINCIPLE **Gate ownership, evidence, override authority and expiration should be explicit.**

Internal audit tests decision integrity—not merely documentation

AUDIT LENS	QUESTION TO REPERFORM	EVIDENCE TO RECONCILE
COMPLETENESS	Are all in-scope third parties in the population?	Procurement, AP, contracts, IAM and TPRM inventories
TIMELINESS	Did assessment and approval precede commitment?	Due-diligence, approval, signature, payment and activation dates
CONSISTENCY	Did comparable risks receive comparable treatment?	Tiering rules, scores, overrides, exceptions and required reviews
AUTHORITY	Did the right person accept the residual risk?	Approval matrix, delegation, escalation and acceptance conditions
EVIDENCE	Can an independent reviewer reproduce the conclusion?	Source documents, reviewer rationale, issue closure and monitoring

BOTTOM LINE **A complete file is not enough if the sequence, judgment or authority behind the decision failed.**

Red flags emerge where process and system records diverge

RECONCILE	AGAINST	INVESTIGATE THE MISMATCH
VENDOR POPULATION	Procurement / AP / contract records	■ Third-party activity with no TPRM record
DECISION SEQUENCE	Approval and contract timestamps	■ Commitment occurred before risk decision
ACTIVATION	IAM / ERP status and due-diligence status	■ Access or payment enabled before required gates
ONGOING RISK	Alerts / incidents and GRC risk records	■ Risk changed without reassessment or escalation
OFFBOARDING	Termination records, IAM and data disposition	■ Access, integrations or data remain after exit

AUDIT TAKEAWAY **A mismatch is an audit lead—not a finding. Investigate rationale, control design and evidence.**

PROCURE VENDOR

OBJECTIVE

Identify business need and initiate acquisition

KEY SYSTEMS

- Ariba
- Coupa
- ERP (SAP, Oracle, Dynamics)
- Workday

KEY PROCESSES

- Need identified
- Budget approval
- RFP/vendor selection
- Route to TPRM

AUDIT FOCUS

- Procurement policy
- Bid requirements
- Budget approvals
- TPRM integration

RISKS

STRATEGIC	FINANCIAL	COMPLIANCE	CYBER/TPRM	LEGAL
Vendor does not align with business objectives Redundant suppliers	Excessive spending Overpricing due to limited competitors	Policy bypassing Non-competitive Bidding	Vendor selected before due diligence Shadow IT procurement	

RED FLAGS

- **Contract signed before procurement review**
- **Repeated sole-source purchases**
- **Payments to vendors not in procurement system**
- **Purchases split to avoid approval thresholds**

VENDOR INTAKE

OBJECTIVE

Formally register and classify a vendor for risk assessment

KEY SYSTEMS

- ServiceNow
- Archer
- OneTrust
- ProcessUnity

KEY PROCESSES

- Ownership assignment
- Service categorization
- Data classification
- Preliminary risk tiering

AUDIT FOCUS

- Intake forms validation
- Vendor ownership assignment
- Risk-tier methodology
- Vendor reconciliation

RISKS

STRATEGIC	FINANCIAL	COMPLIANCE	CYBER/TPRM	LEGAL
Incorrect vendor classification	Duplicate vendors	Incomplete onboarding documentation	Vendor bypass intake process Incorrect inherent risk classification	

RED FLAGS

- **Missing Business or Relationship Ownership**
- **Incomplete or Inaccurate Intake Record**
- **Vendor payments before intake process**
- **High-risk vendors classified as lower risk**

VENDOR QUESTIONNAIRE

OBJECTIVE

Collect due diligence information directly from the vendor

KEY SYSTEMS

- ServiceNow
- Archer
- OneTrust
- ProcessUnity

KEY PROCESSES

- Questionnaire
- Vendor response
- Gathering documents
- Evidence validation
- Exception identification

AUDIT FOCUS

- Due diligence process
- Evidence validation
- Documentation retention
- Escalation of exceptions

RISKS

STRATEGIC	FINANCIAL	COMPLIANCE	CYBER/TPRM	LEGAL
Incorrect vendor compliance capability	Financial instability	Insufficient regulatory attestations	Self-assessment inaccuracies Undisclosed weaknesses	

RED FLAGS

- **Missing attestation report (e.g., SOC 2)**
- **Expired certification or attestation**
- **Excessive questionnaire exceptions**
- **Incomplete responses accepted by reviewer**

VENDOR REVIEW

OBJECTIVE

Perform cross-functional review of vendor risks and controls

KEY SYSTEMS

- ServiceNow
- Archer
- OneTrust
- AuditBoard
- ProcessUnity

KEY PROCESSES

- Security review
- Privacy assessment
- Legal review
- Compliance assessment
- Operational review

AUDIT FOCUS

- Required reviewers
- Review criteria consistency
- Decision audit trail
- SLA compliance

RISKS

STRATEGIC	FINANCIAL	COMPLIANCE	CYBER/TPRM	LEGAL
Critical stakeholder excluded	Hidden financial obligations	Regulatory requirement not addressed	Inconsistent review practices	Unfavorable contractual terms

RED FLAGS

- **Missing necessary approvals by risk owners**
- **Reviews completed after contracting**
- **Undocumented exceptions**
- **Reviewer conflicts of interest**

RISK SCORING

OBJECTIVE

Assess and quantify vendor risk exposure

KEY SYSTEMS

- ServiceNow
- Archer
- OneTrust
- Custom scoring

KEY PROCESSES

- Inherent risk scoring
- Control evaluation
- Residual risk calculation
- Risk ranking

AUDIT FOCUS

- Scoring methodology governance
- Override approvals
- Accuracy of calculations

RISKS	STRATEGIC	FINANCIAL	COMPLIANCE	CYBER/TPRM	LEGAL
	Critical vendors underrated Improper input from all risk SMEs	Financial exposure understated	Regulatory impact incorrectly weighted	Subjective scoring Overrides Security risks not considered	

RED FLAGS

- **Frequent manual overrides**
- **Inconsistent scoring outcomes**
- **Missing rationale for risk rating**
- **Large fluctuations in risk scores**

VENDOR APPROVAL

OBJECTIVE

Determine whether residual risk is acceptable

KEY SYSTEMS

- ServiceNow
- Archer
- OneTrust
- Custom scoring

KEY PROCESSES

- Risk review
- Risk acceptance
- Escalation
- Approval documentation

AUDIT FOCUS

- Approval matrix compliance
- Exception governance
- Approval authority validation

RISKS

STRATEGIC	FINANCIAL	COMPLIANCE	CYBER/TPRM	LEGAL
Excessive risk acceptance	High-risk vendors approved without justification	Improper approval authority	Inconsistent decision making Lack of accountability	

RED FLAGS

CONTINUE PROCUREMENT

OBJECTIVE

Proceed with contracting and purchasing activities

KEY SYSTEMS

- Ariba
- Coupa
- ERP (SAP, Oracle, Dynamics)
- Workday

KEY PROCESSES

- Contract negotiation
- Purchase order creation
- Contract execution
- Funding approval

AUDIT FOCUS

- Contract review
- Applicable addendums
- Procurement approval requirements

RISKS

STRATEGIC	FINANCIAL	COMPLIANCE	CYBER/TPRM	LEGAL
Vendor lock-in	Unfavorable pricing terms	Missing contractual protections	Risk requirements omitted from contracting	Weak indemnification and liability provisions

RED FLAGS

RISK CREATION

OBJECTIVE

Formally document identified risks in the GRC environment

KEY SYSTEMS

- ServiceNow
- Archer
- OneTrust
- AuditBoard

KEY PROCESSES

- Risk registration
- Risk categorization
- Owner assignment
- Escalation management
- Reporting

AUDIT FOCUS

- Risk-register completeness
- Risk ownership
- Escalation procedures
- Risk reporting quality

RISKS	STRATEGIC	FINANCIAL	COMPLIANCE	CYBER/TPRM	LEGAL
	Material risks not tracked	Significant exposures omitted	Regulatory findings not documented	Risk ownership unclear Lack of accountability	

RED FLAGS

- **Vendor risk with inadequate ownership**
- **Duplicate risks**
- **Missing risk description or information**
- **Significant findings not entered in GRC**

RISK REMEDIATION

OBJECTIVE

Reduce identified risks to acceptable levels

KEY SYSTEMS

- ServiceNow
- Archer
- OneTrust
- AuditBoard
- Ticketing (Jira, Workday)

KEY PROCESSES

- Corrective action plans
- Milestone tracking
- Validation testing
- Risk acceptance requests

AUDIT FOCUS

- Remediation timeliness
- Closure validation
- Risk acceptance governance
- Aging analysis

RISKS	STRATEGIC	FINANCIAL	COMPLIANCE	CYBER/TPRM	LEGAL
	Business disruption from unresolved issues	Losses resulting from inadequate controls	Regulatory deficiencies unresolved	Ineffective corrective actions Open vulnerabilities	

RED FLAGS

- **Outstanding findings over expected timelines**
- **Repeated risk exceptions**
- **Weak or inadequate remediation plans**
- **Risk closure without adequate evidence**

ACTIVATE VENDOR

OBJECTIVE

Enable the vendor to conduct business with the organization

KEY SYSTEMS

- ERP (SAP, Oracle, Dynamics)
- Workday
- IAM

KEY PROCESSES

- Vendor master setup
- Payment configuration
- Access provisioning
- System integrations
- Go-live activation

AUDIT FOCUS

- Vendor master controls
- Segregation of duties
- Access provisioning
- Approval validation
- Payment setup controls

RISKS

STRATEGIC	FINANCIAL	COMPLIANCE	CYBER/TPRM	LEGAL
Overdependence on single vendor	Vendor payment fraud Duplicate vendors	Incomplete approval requirements	Vendor activated before approval Excessive access granted	

RED FLAGS

- **Duplicate vendor records**
- **Missing approvals for access provisioning**
- **Excessive user or system access**
- **Vendor activated before TPRM completion**

RISK UPDATES (ONGOING MONITORING)

OBJECTIVE

Continuously monitor vendor performance and risk throughout the relationship lifecycle

KEY SYSTEMS

- SecurityScorecard
- BitSight
- Archer
- OneTrust
- ServiceNow GRC

KEY PROCESSES

- Continuous monitoring
- Annual reassessments
- Risk score updates
- Incident tracking
- Performance reviews

AUDIT FOCUS

- Ongoing monitoring
- Reassessments
- Third-party incident management
- Risk update governance
- Executive reporting

RISKS	STRATEGIC	FINANCIAL	COMPLIANCE	CYBER/TPRM	LEGAL
	Critical vendor failure	Vendor insolvency	Emerging regulatory violations	Stale risk ratings No active monitoring Security events	

RED FLAGS

- **Missed periodic assessment (as applicable)**
- **No monitoring of high-risk vendors**
- **Outdated risk ratings or rating deterioration without management action plan**
- **Vendor incidents not escalated**

Emerging trends to check whether TPRM can see—and respond to—change

FOUR TRENDS • ONE REUSABLE AUDIT LENS

01 VENDOR AI

AI may enter data processing or service delivery without visibility.

- Which vendors use AI with our data?
- Are use cases reviewed by AI governance and TPRM?
- Does the inventory capture approved AI use?

02 FOURTH PARTIES

Critical services may rely on subcontractors the organization has not assessed.

- Which subcontractors support critical services?
- Are key arrangements contractually disclosed?
- Must vendors notify us when critical subcontractors change?

03 CONTINUOUS MONITORING

Point-in-time reviews can miss meaningful changes between assessments.

- How quickly are material changes identified?
- Which events trigger reassessment and escalation?
- Is monitoring focused on critical vendors?

04 DEPENDENCY & EXIT

Shared providers or platforms can create concentrated exposure and difficult exits.

- Where do critical services share providers or platforms?
- Are exit, portability and continuity plans tested?
- Do geography or ownership changes trigger review?

VISIBILITY Can management identify exposure?

GOVERNANCE Does information reach owners?

ACTION Does change trigger reassessment?

Context: IIA Risk in Focus 2026; EU DORA / EBA; WEF Global Risks Report 2026.

Questions

myna PARTNERS

myna PARTNERS