NAVEX GLOBAL®

Maturing Your IT and Third-Party Risk Management Programs

Lakshman Charanjiva, Technology Partner and CTO | BC Partners

Haywood Marsh, General Manager of NAVEX Integrated Risk Management | NAVEX Global

Shane Radford, Senior Solutions Engineer | NAVEX Global

Adam Billings, Product Specialist | NAVEX Global

Agenda

- IT and third-party risk management trends and challenges
- Identifying improvement opportunities
- Demo
- Taking the next step
- Q&A
- Appendix: more material for your use

Trends

- The number, impact and sophistication of ransomware attacks are increasing
  - Ransomware attacks doubled in frequency in 2021[1], and affected many industries, countries and company sizes[2]
  - 37% of global organizations were victims in the last year[3]
  - Double extortion and Ransomware as a Service (RaaS) are on the rise[4]
  - Supply chain attacks are more prevalent, increasing as much as 4X[5]
- Reliance on third parties is increasing[6]; they're more critical than ever in businesses' success and have more access to data than ever before
  - 82% of companies give highly privileged roles to vendors[7]
- COVID-19 has dramatically impacted our supply chains[8] and increased the exposure to IT security risk as work has shifted to remote and hybrid enviornments[9]
  - Only 30% of companies anticipate being "in-person first" moving forward[10]
- Regulation and the enforcement thereof is increasing
  - GDPR fines hit €1B in Q3, 3X more than all 2020[11] and CCPA is active
  - The COSO and US DOJ guidances were revised to focus more heavily on operationalization of risk management, including third-party risk[12]
  - Data breach notification laws differ by state in the US, and by industry and type of data use in the EU (EU Agency for Cybersecurity; ENISA)[13]
- Visibility of risk is increasing in the public eye, and at the board and executive level[14]

*See appendix for footnote citations

Case Study

Major International Airline

<u>Situation</u>: attacker altered third-party code on company site to skim customer data

<u>Impact:</u>

- 380K customer records and credit card information exposed through third-party code on website
- Fined £183.39M under GDPR
- £3B in settlements and reputational damage

<u>Lessons Learned:</u>

- IT, third-party, data privacy and reputational risks are converging. Ensuring risk owners, data sources and processes are aligned across silos is critical
- Operationalizing your risk management is critical. Ensure you understand your gaps vs. authority documents and frameworks, and ensure controls work
- The impact of breaches reach far beyond the walls of the attacked company
- The initial cost of an attack is small compared to the total cost

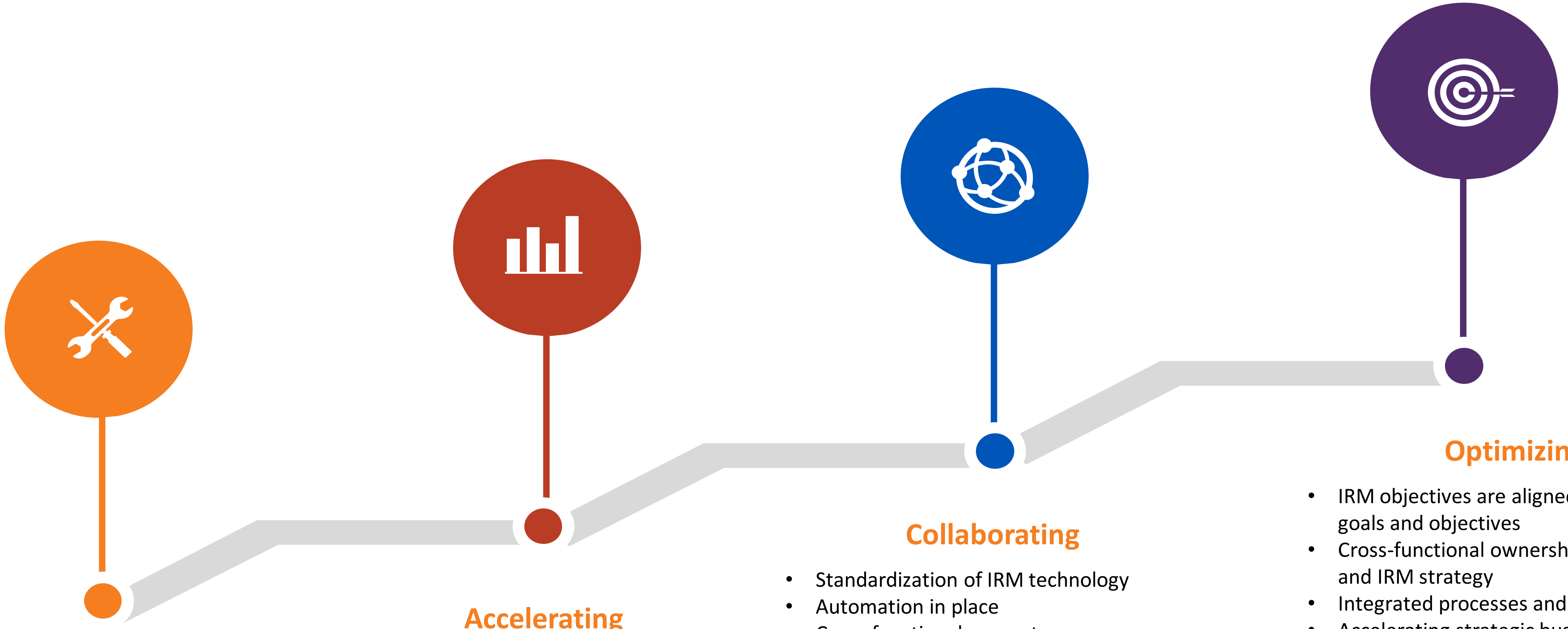
BC Partners Recommendation List

- Extended Detection and Response (XDR) across all endpoints, cloud, email, etc.
- Security Incident and Event Management (SIEM)
- 24/7 Security Operations Center (SOC)
- Zero trust network access
- Backup and recovery (immutable backups, air-gapped storage)
- Incident response retainer
- Other
  - Asset discovery and inventory
  - MFA
  - Laptop encryption
  - Timely patching
  - Email filtering to combat phishing
  - Annual pen tests
  - Vuln scanner
  - Cyber insurance

The Challenges You Face

- Protecting your company from increasingly sophisticated and numerous attacks
- Staying compliant with an increasing number of regulations and avoiding fines
- Getting your arms around all your third parties and ensuring they don’t expose you to data breach or supply chain risk
- Meeting your customers’ contractual requirements
- Dealing with increased scrutiny from the board and executives
- Making risk everyone’s responsibility
- Doing all of this with constrained resources and headcount

Risk Management Maturity Model



Reactive

- Ad-hoc approach
- Manual processes
- Difficult to scale
- Scattered resources and data
- High cost/ inefficient

Accelerating

- Initiation of IRM technology
- Automation of some tasks
- Defined IRM processes
- Limited cross-functional support
- Improved cost structure

Collaborating

- Standardization of IRM technology
- Automation in place
- Cross-functional support
- Strategic risk management program
- Enhanced ROI

Optimizing

- IRM objectives are aligned with strategic goals and objectives
- Cross-functional ownership of technology and IRM strategy
- Integrated processes and reporting
- Accelerating strategic business objectives and revenue

Information Technology Risk Management – Where to Begin

- Centralize your Asset Inventory
- Manage Asset Lifecycle
- Sync with your Vulnerability Scanner to Manage Findings
- Perform Risk Assessments on Devices, Systems, Facilities and More
- Track Findings and Corrective Action Plans
- Leverage Reports & Dashboards to Drive Decisions
- Identify and Respond to Risks
- Integrate your Data to Gain a 360° View of Risk

Configurable Solution

Flexible Workflow

Alerts & Reminders

Business Logic

Assessment Engine

Reports & Dashboards

Role-Based Access

NAVEX GLOBAL

Third-Party Risk Management – Where to Begin

- Centralize your Third Parties
- Manage Entire Vendor Lifecycle and Measure Performance
- Conduct Due Diligence by Collaborating with Internal Stakeholders
- Automated Scoring of Risk Assessments from Third Parties
- Track Findings and Corrective Action Plans
- Leverage Reports & Dashboards to Drive Decisions
- Identify and Respond to Risks
- Integrate your Data to Gain a 360° View of Risk

Configurable Solution

Flexible Workflow

Alerts & Reminders

Business Logic

Assessment Engine

Reports & Dashboards

Role-Based Access

NAVEX GLOBAL®

Demonstration

Next Steps to Improve Your Program

- Understand your inherent risks and risk appetite
- Pick a process to improve based on your residual risk
- Perform a gap analysis vs. authority documents or maturity models. Assess your:
    - Policies
    - Controls, workflows and assessments
    - Audit and testing process
    - Tools (e.g. risk management software, vuln scanners, SIEM, etc.)
    - Key Risk Indicators and dashboards/ reports
- Focus on continuous improvement not perfection

Q&A

Thank You!

For questions and/or product information, contact Jacob Sorensen at jsorensen@navexglobal.com

Appendix

Footnotes

1. https://www.verizon.com/business/resources/reports/dbir/2021/results-and-analysis/
2. https://www.blackfog.com/the-state-of-ransomware-in-2021/; https://www.pindrop.com/blog/uk-hospitals-hit-by-broad-cyberattack/; https://apnews.com/article/joe-biden-europe-government-and-politics-technology-business-88c51d8041b1afdd42fa9f571c3de446
3. https://www.idc.com/getdoc.jsp?containerId=US48093721
4. https://www.techtarget.com/searchsecurity/feature/Ransomware-trends-statistics-and-facts
5. https://portswigger.net/daily-swig/four-fold-increase-in-software-supply-chain-attacks-predicted-in-2021-report
6. https://fortunly.com/statistics/outsourcing-statistics/#gref
7. https://www.securitymagazine.com/articles/94435-of-companies-give-third-parties-access-to-all-cloud-data
8. https://hbr.org/2020/09/global-supply-chains-in-a-post-pandemic-world
9. https://www.mckinsey.com/featured-insights/future-of-work/whats-next-for-remote-work-an-analysis-of-2000-tasks-800-jobs-and-nine-countries; https://www.navexglobal.com/blog/article/it-and-corporate-compliance-bridging-the-gap-in-the-era-of-remote-and-hybrid-work/
10. https://www.cnbc.com/2021/07/08/how-many-workers-will-be-returning-to-offices-and-how-often.html
11. https://finbold.com/gdpr-fines-q3-2021/
12. https://www.justice.gov/criminal-fraud/page/file/937501/download; https://www.coso.org/Documents/Compliance-Risk-Management-Applying-the-COSO-ERM-Framework.pdf
13. https://www.itgovernanceusa.com/data-breach-notification-laws; https://www.enisa.europa.eu/topics/incident-reporting
14. https://corpgov.law.harvard.edu/2019/11/20/risk-management-and-the-board-of-directors-7/

Integrated Risk Management and How To Operationalize A Risk Program

C-Suite and Board of Directors

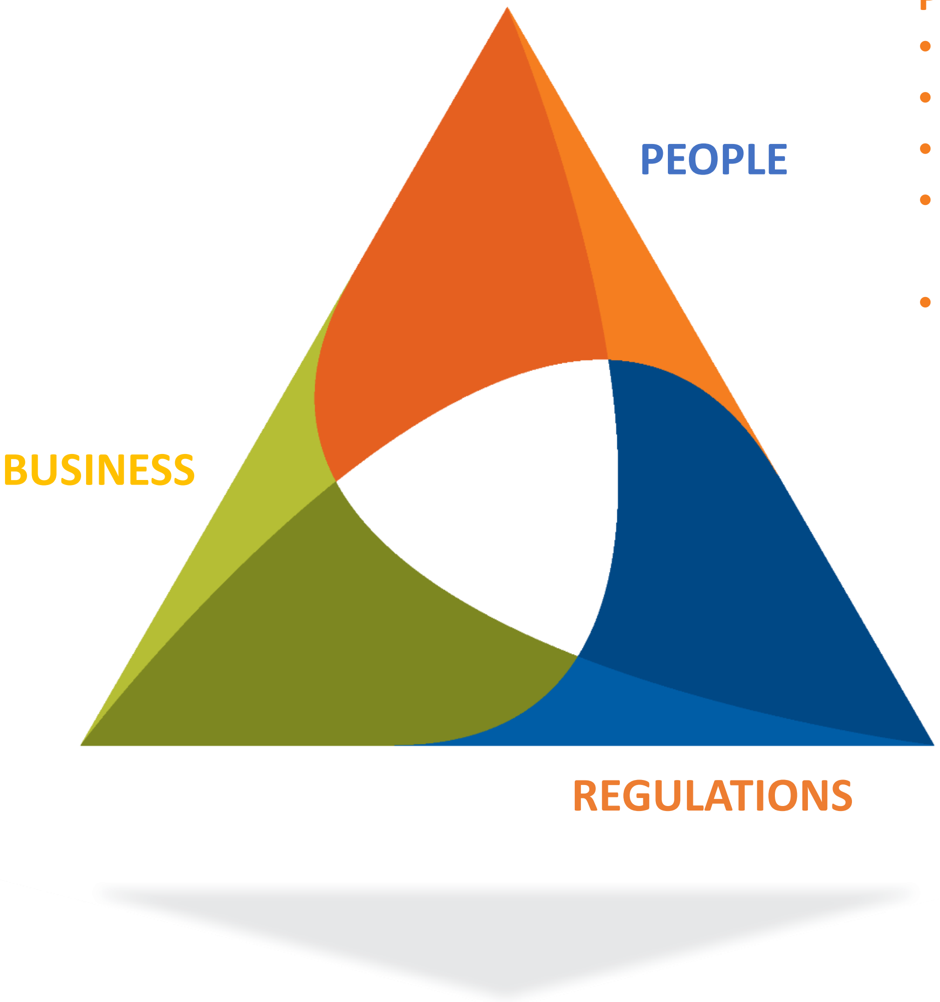
Increasingly concerned about three broad areas of risk…

People Risks:

- Ethical Lapses
- Employee Legal Actions
- Reputational Damage
- Negative Impact on Brand Image & Share Price
- Employee Recruitment, Retention & Loyalty

Business Risks:

- Data Security & Privacy
- Vendor Management
- Business Continuity
- Environmental Health & Safety
- Audit



Regulations Risks:

- Bribery & Corruption
- Insider Trading
- Conflict of Interest
- Wage & Hour Issues
- Fraud

What is Integrated Risk Management?

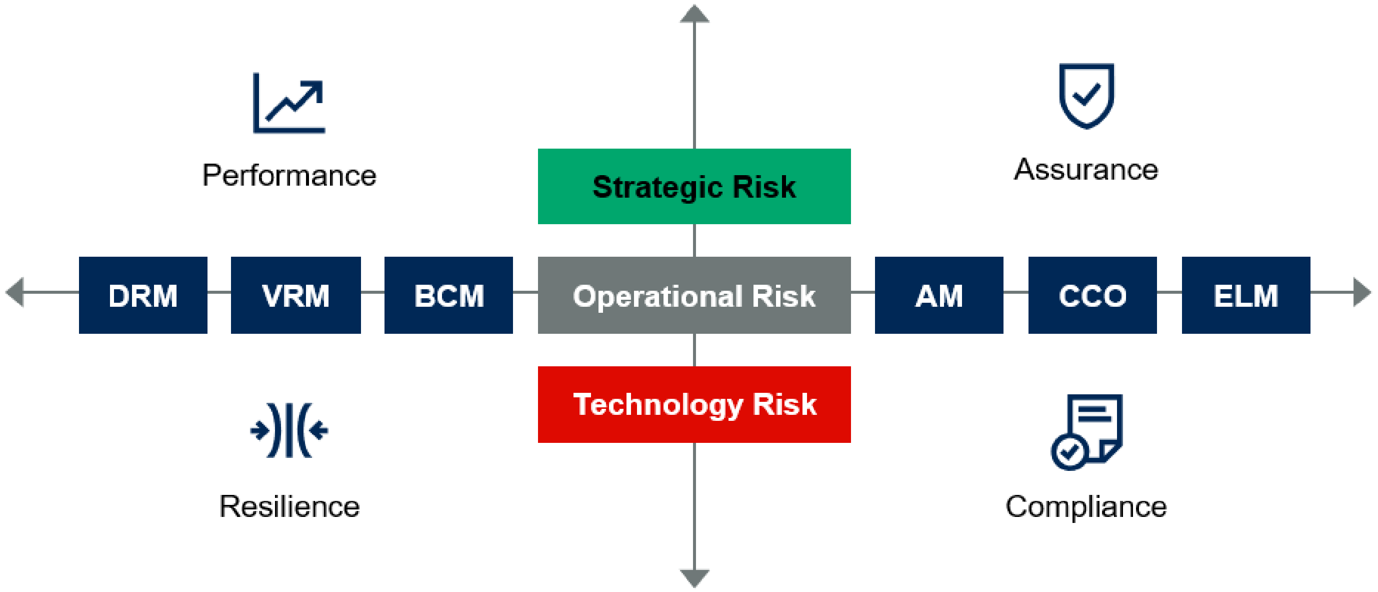
Gartner's Definition

Integrated Risk Management (IRM) is a set of practices and processes supported by a risk-aware culture and enabling technologies, that improves decision making and performance through an integrated view of how well an organization manages its unique set of risks.

1. **Strategy**: Enabling and implementation of a framework, including performance improvement through effective governance and risk ownership
2. **Assessment**: Identification, evaluation, and prioritization of risks
3. **Response**: Identification and implementation of mechanisms to mitigate risk
4. **Communication and reporting:** Provision of the best or most appropriate means to track and inform stakeholders of an enterprise's risk response
5. **Monitoring**: Identification and implementation of processes that methodically track governance objectives, risk ownership/accountability, compliance with policies and decisions that are set through the governance process, risks to those objectives and the effectiveness of risk mitigation and controls
6. **Technology**: Design and implementation of an IRM solution architecture

How to Align Across Risk and Compliance Silos

IRM Objectives and Risk Domains



Performance

Assurance

Strategic Risk

DRM

VRM

BCM

Operational Risk

AM

CCO

ELM

Technology Risk

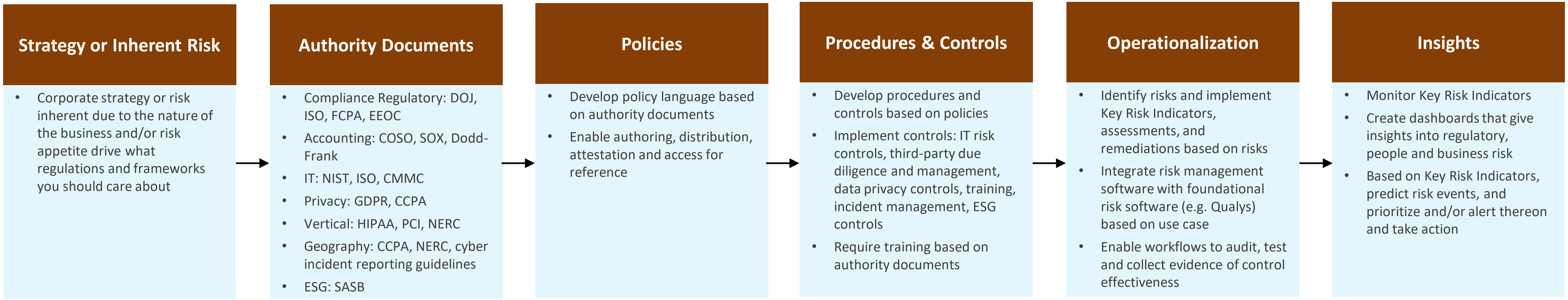
Resilience

Compliance

Source: Gartner
AM = audit management; BCM = business continuity management; CCO = corporate compliance and oversight; DRM = digital risk management; ELM = enterprise legal management; VRM = vendor risk management
ID: 450383

- Form a Risk and Compliance committee with owners across the business
- Pick a use case on which to focus first
- Share data across silos
- Establish a common language
- Meet regularly to identify and prioritize risks, and gain alignment on goals. Establish a risk register
- Get out of manual processes and ensure processes are complete
- Map authority documents to policies to controls. Audit, test and collect auditable evidence on these controls in a system of record
- Establish a workflow engine that collects assessments and evidence from the first line of defense, and ensures remediation of risks
- Report to and gain buy-in from the board and executives
- Pick the next use case

How to Operationalize A Risk Program



Strategy or Inherent Risk

- Corporate strategy or risk inherent due to the nature of the business and/or risk appetite drive what regulations and frameworks you should care about

Authority Documents

- Compliance Regulatory: DOJ, ISO, FCPA, EEOC
- Accounting: COSO, SOX, Dodd-Frank
- IT: NIST, ISO, CMMC
- Privacy: GDPR, CCPA
- Vertical: HIPAA, PCI, NERC
- Geography: CCPA, NERC, cyber incident reporting guidelines
- ESG: SASB

Policies

- Develop policy language based on authority documents
- Enable authoring, distribution, attestation and access for reference

Procedures & Controls

- Develop procedures and controls based on policies
- Implement controls: IT risk controls, third-party due diligence and management, data privacy controls, training, incident management, ESG controls
- Require training based on authority documents

Operationalization

- Identify risks and implement Key Risk Indicators, assessments, and remediations based on risks
- Integrate risk management software with foundational risk software (e.g. Qualys) based on use case
- Enable workflows to audit, test and collect evidence of control effectiveness

Insights

- Monitor Key Risk Indicators
- Create dashboards that give insights into regulatory, people and business risk
- Based on Key Risk Indicators, predict risk events, and prioritize and/or alert thereon and take action

NAVEX GLOBAL®

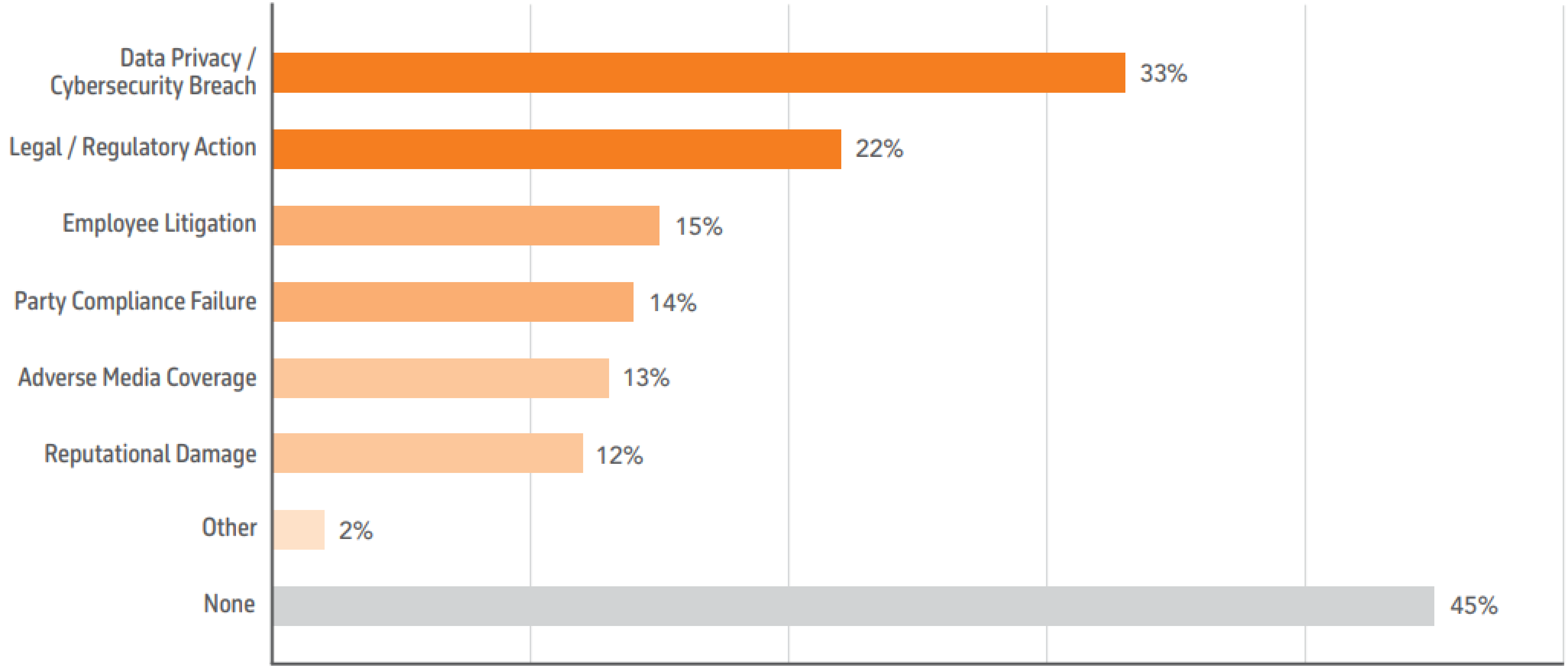
Highlights from the 2021 Definitive Risk & Compliance Benchmark Report (performed by NAVEX Global)

Download Benchmark Report

Risk and Compliance Challenges Faced

1,000 Risk and Compliance Professionals assessed

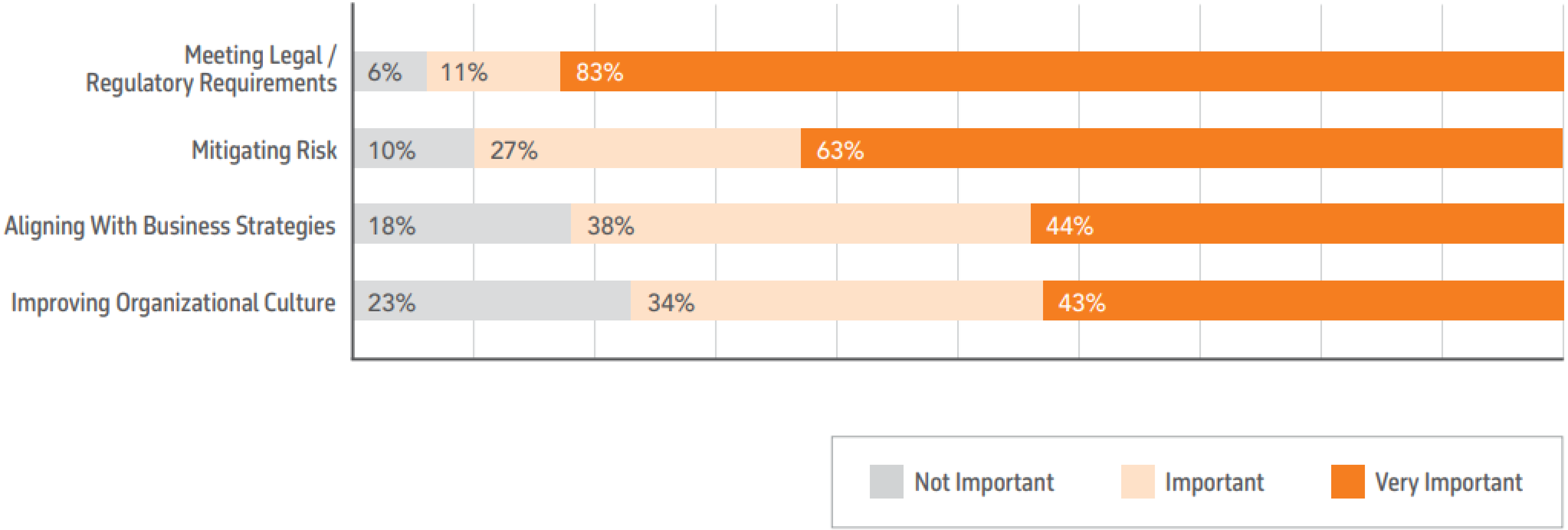
Shown: Percent of respondents who answered "yes" when asked if they had experienced any of the following in the past 3 years



Decision-Making Considerations

1,000 Risk and Compliance Professionals assessed

Shown: Responses to "How important are the following considerations in your R&C program's decision-making process?"

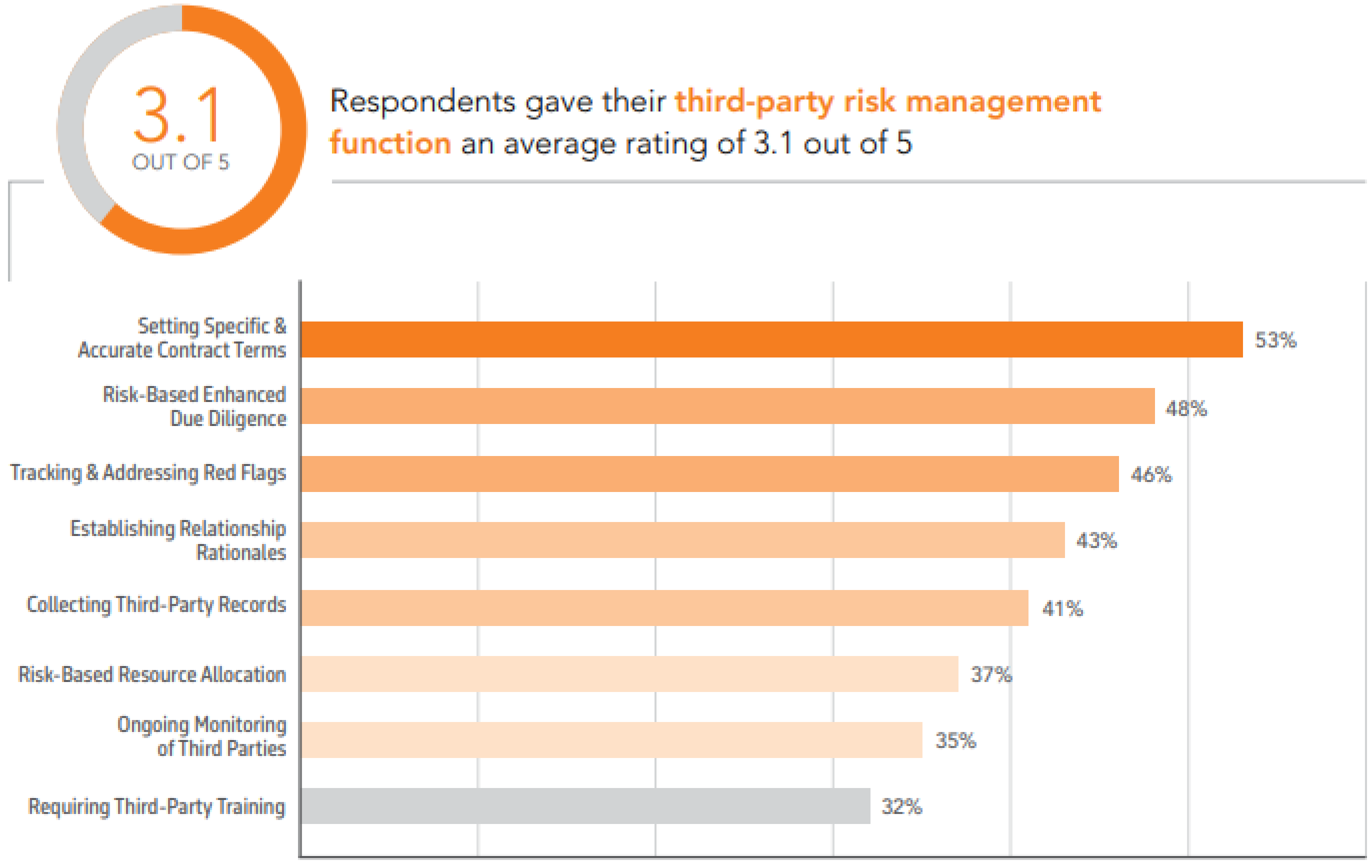


Where are we at today?

Third-Party Risk Management Performance Rating

Figure 6.8 Third-Party Risk Management Performance Rating

Shown: Percent of respondents who rated their program's third-party risk management performance as "good" to "great" in the following areas



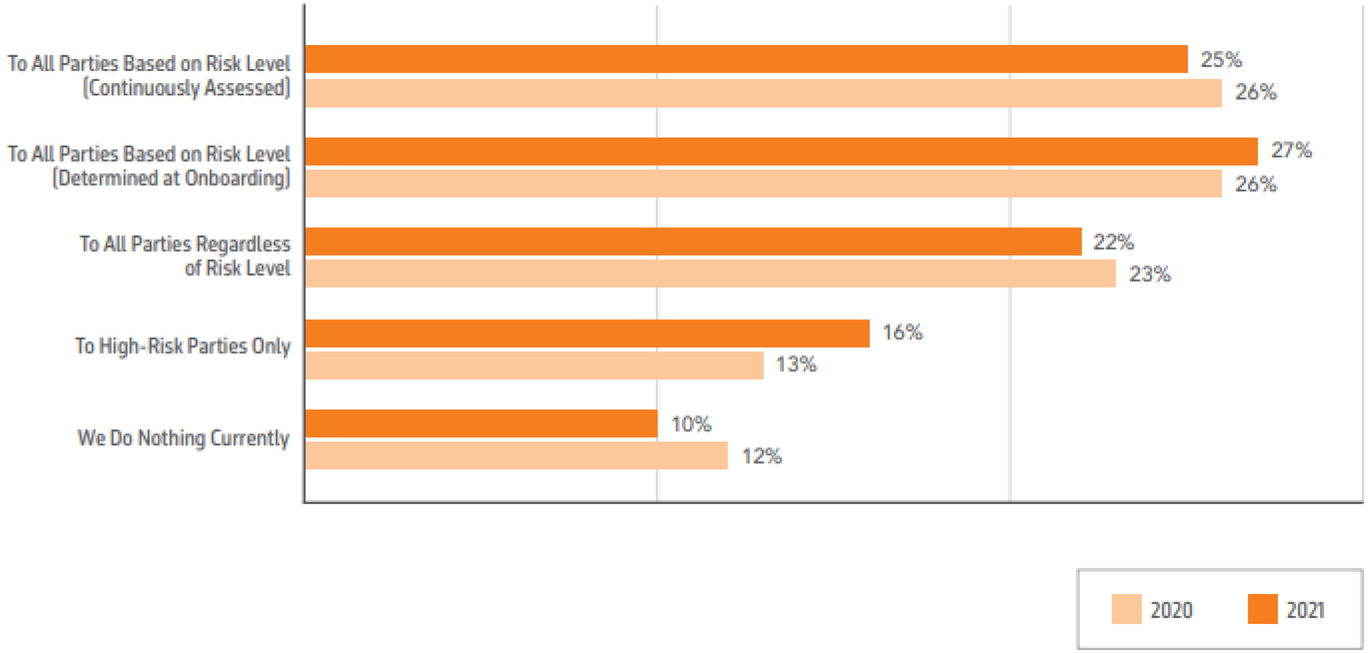
Respondents gave their **third-party risk management function** an average rating of 3.1 out of 5

Where are we at today?

Application of Third-Party Risk Management

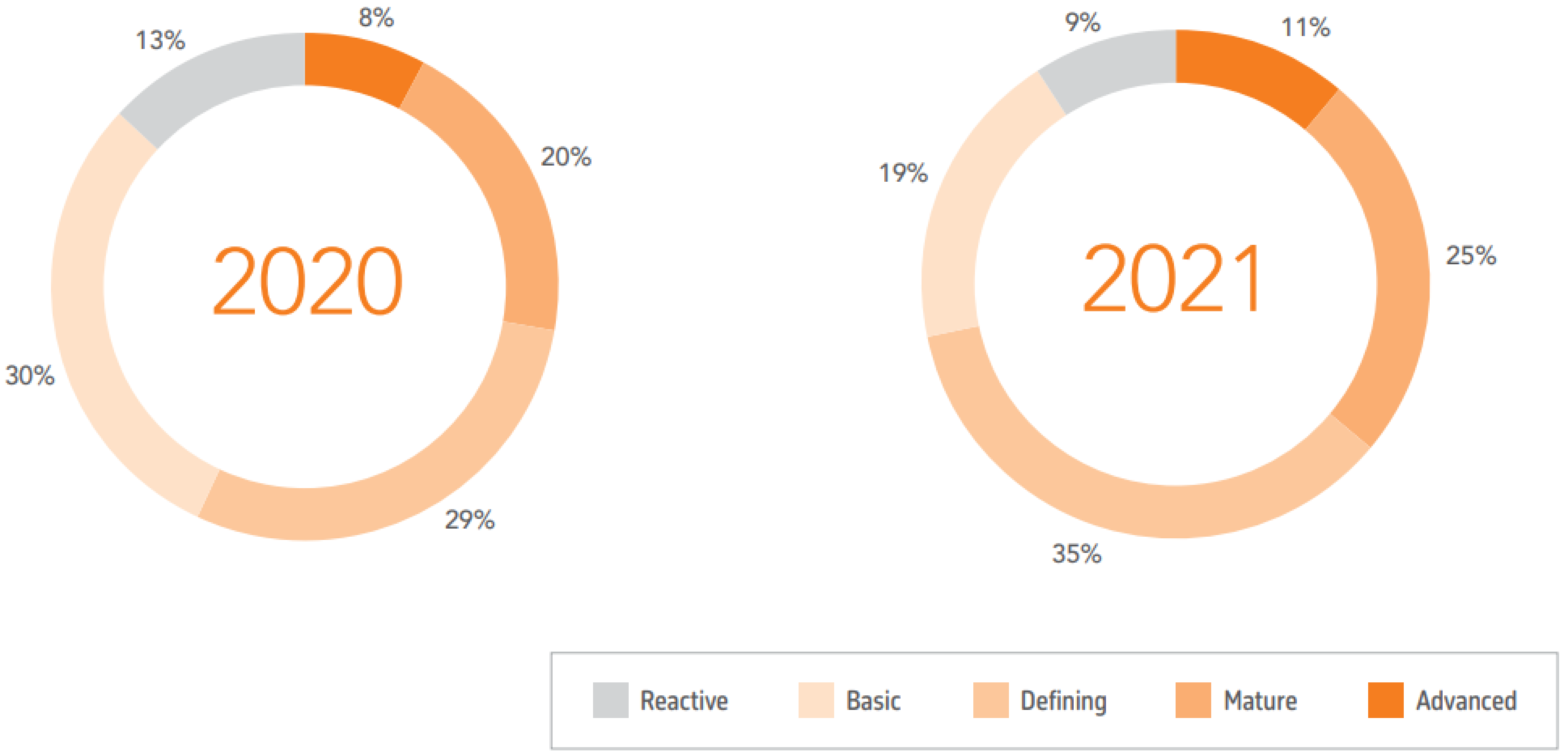
Figure 6.9 Application of Third-Party Risk Management

Shown: Responses to "How do you apply risk-based management?"



Where are we at today?

Risk & Compliance Program Maturity



NAVEX GLOBAL®

Ransomware Attacks in 2021: Compliance Lessons Learned

Matt Kelly, Editor & CEO| Radical Compliance

Kyle Martin, Senior Director, Customer Success & Professional Services | NAVEX Global

About the Presenters

Matt Kelly

Editor & CEO

Radical Compliance

Matt Kelly is the founder of Radical Compliance, which provides consulting and commentary on corporate compliance, audit, governance, and risk management. Formerly the editor of Compliance Week, Matt has also served as a reporter and contributor for numerous publications, and speaks frequently on corporate, audit, and governance issues.

Kyle Martin

Senior Director, Customer Success
& Professional Services

NAVEX Global

Kyle has over a decade of experience leading risk and compliance professionals across multiple industries. At NAVEX Global, Kyle interacts with all aspects of the Customer Success Organization, directly managing both the Customer Success and Professional Services teams. His cross-functional alignment with each department is critical to the success of his teams, and he takes on all challenges to continually improve customer experience.

Agenda

- Scope of the Problem
- Administrative Guidance
- Issues To Address if You Have Been Attacked
- Preventative Measures You Can Take
- Who owns this?

1. Understanding the Scope of the Problem

- **Ransomware attacks are on the rise.** Suspected ransomware payments nearly doubled in 2021
- **The ransom is only a fraction of the full cost** of a ransomware attack. Downtime, recovery, and reputational costs can be **10 – 15 times** the cost of the ransom itself
- **Primary Drivers** behind the surge include:
  - Increased vulnerability in the era of remote work and BYOD
  - Greater sophistication within the ransomware space, with contractors and subcontractors

2. Administrative Guidance

- **More required disclosures** of cyber attacks, especially for government contractors and critical infrastructure
- **Stronger cybersecurity measures** and migration to Zero Trust architecture
- **Increased enforcement** from OFAC and other agencies against businesses
- **Increased pursuit** of attackers by the Justice Department and other agencies

3. Issues To Address If You've Been Attacked

- **Key Questions**
  - Do you pay the ransom?
  - Do you disclose to law enforcement? Business partners? Customers?
- **3 Steps to Recovery:**
  - Develop and implement an incident recovery plan
  - Plan, implement and regularly test a data backup and restoration strategy
  - Maintain and up-to-date list of internal and external contacts
- **Conduct a Root Cause Analysis**

4. Preventative Measures You Can Take

- **Secure management commitment**
  - Financial resources
  - Facilitating a culture of compliance and risk awareness at all organizational levels
  - Assume that a successful attack is a matter of *when*, not *if*
- **Conduct an internal risk assessment**
  - What would happen to the business?
  - What are the key risk indicators?

4. Preventative Measures You Can Take (Continued)

- **Conduct a vendor risk assessment**
  - What kind of data does your vendor have access to?
  - How much access do they have?
  - How frequently do you update your assessment?
- **Implement internal controls**
  - Create polices and procedures that capture day-today operations and are easy to follow
  - Identify and correct weaknesses

4. Preventative Measures You Can Take (Continued)

- **Conduct testing and auditing**
  - Make it comprehensive and objective
  - Produce findings which are accountable and immediately addressable
- **Implement training**
  - Make it easily accessible
  - Take KRIs such as phishing test failures into account
  - Tailor it different employee levels

5. Determining Ownership

- Roles and responsibilities are cross-functional
- Start with a committee
  - Pull stakeholders from Compliance, Legal, Internal Audit, IT Security, etc.
- Extend responsibilities to third and fourth parties
- Bring in the experts to support key initiatives

NAVEX GLOBAL®

Security Through Integrity

How to Effectively Manage 3rd Party Information & Cybersecurity Risk

Matt Kelly, Editor & CEO| Radical Compliance

Linda Tuck Chapman, Chief Executive Officer | Third Party Risk Institute Ltd.

About the Presenters

MODERATOR

Matt Kelly

Editor & CEO, Radical Compliance

Founder of Radical Compliance, which provides consulting and commentary on corporate compliance, audit, governance, and risk management. Radical Compliance also serves at the personal blog for Matt Kelly, the long-time (and now former) editor of Compliance Week. Kelly writes and speaks frequently on corporate, audit, and governance, and now works with various private clients to understand those fields and to develop go-to-market strategies or provide other assistance in reaching audiences of compliance professionals.

RADICAL COMPLIANCE

SHARP THINKING ABOUT COMPLIANCE, AUDIT, AND RISK

About the Presenters

linda@3PRInstitute.com
+1- 416-452-4635

Linda Tuck Chapman C3PRMP

CEO, Third Party Risk Institute Ltd.

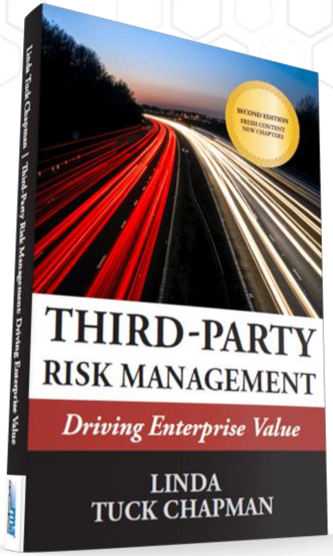
Linda is a leading expert in third-party risk management. As one of the first Chief Procurement Officers and Head Third Party Risk Management in the financial services sector, Linda helped create integrated best practices in strategic sourcing and third-party risk management.

In addition to her role as President, Ontala Performance Solutions Ltd., Linda leads Third Party Risk Institute Ltd.. A strategic advisor, relatable educator, and published author, Linda's students, clients, and global network benefit from her thought leadership.

Linda's best-selling book "Third Party Risk Management: Driving Enterprise Value" in its 2nd edition is available on Amazon.

Third Party Risk Institute Ltd. offers the gold standard certification program. **C3PRMP -** "Certified Third Party Risk Management Professional - is a 10-week video-based, faculty-led program *(66 CPE credits)*

Visit www.thirdpartyriskinstitute.com/training to register.



Career Highlights:

- BMO Financial Group: Chief Procurement Officer & Head Third Party Risk Management
- Ontario Education Marketplace: President & CEO
- Fifth Third Bank: Chief Procurement Officer & Head Third Party Risk Management
- Scotiabank Group: VP Procurement & Head, Supplier Risk Management

Agenda

- Basics of Third-Party Risk Management
- Getting Third-Party Risk Management Done
- Key Takeaways & Conclusion

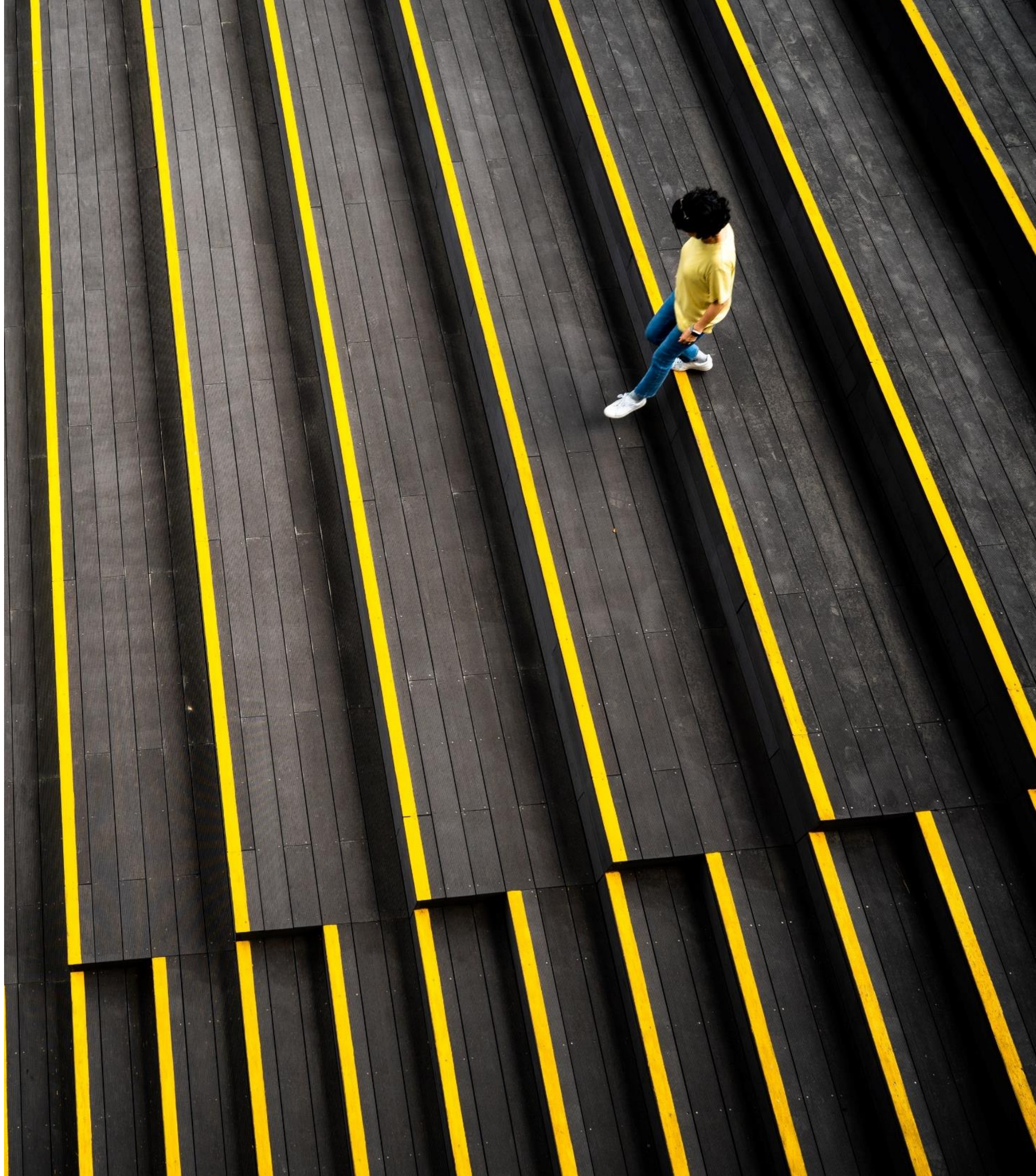
Basics of Third-Party Risk Management

Why It Has To Be Done

- Managing your extended enterprise
- Legal and regulatory obligations
- Financial and operational risks
- Protecting your reputation

What Is Involved

- Relationship segmentation
- Due diligence and selection
- Onboarding
- Risk monitoring
- Relationship management
- Responding to threats and risk events



Third-Party Assessment in Detail: What You Want To Know

- Relationship segmentation
- Evaluating the third party’s control environment
- Cybersecurity practices
- Financial health
- Business resilience
- Other risks

Getting Third-Party Risk Management Done

How To Assess a Third-Party/Vendor

- Procurement-related due diligence
- Pre-screening
- Defining requirements
- Questionnaires
- Reliance on 3rd party audits (e.g. SOC 2, SSAE)
- Evaluating controls
- Rating residual risks
- Risk acceptance

How To Monitor Third-Party Risk After Onboarding

- Relationship management versus risk monitoring
- Developing KRIs and risk thresholds
- Risk monitoring tools
- Escalation and exceptions
- Aggregated risk reporting
- Concentration risk

Workload Management Techniques

- Technology-enabled processes
- 3rd party tools
- Technology-enabled workflow
- Data management and governance
- AI for third-party risk management
- Data-driven decisions

How To Avoid Problems

- Tone at the top
- A compelling value proposition
- Stakeholder engagement
- Appropriate roles and responsibilities
- Risk-adjusted practices
- Effective risk oversight
- Root cause analysis for risk events and to mature your program

Lessons Learned

- Third-party risk management is a team sport, and everyone has a role to play
- Visible C-Suite support and a compelling value proposition is essential for success
- Effective Challenge is one of the most important tools in your toolkit
- Failing to invest in technology means valued resources will be tied up with “task management”, not “risk management”