

**RAUSCH**  
ADVISORY SERVICES

# Third-Party Risk Management Internal Audits Role



The Institute of  
Internal Auditors

# Agenda for Third-Party Risk Management

- Introduction to your speaker
- Third-Party Risk Management
- Recent 3<sup>rd</sup> Party Breaches
- Internal Audits Role
- Frameworks & Incident Response
- RAS



# Michael Lisenby, CRISC, CDPSE

Managing Partner for Rausch Advisory Services

Mike has significant experience helping businesses manage their technology resources and compliance needs effectively. His experience includes consulting and co-sourcing, IT Security, IT audits, Regulatory compliance, and technology security assessments, risk identification, assessment and evaluation, risk response, risk monitoring, IT Security & Governance control design and implementation, and IT control monitoring and maintenance.

Prior to Rausch Advisory Services, held leadership roles with Arthur Andersen and several other National Consulting Firms and has prior experience with Fortune Brands and Philip Morris. Mike designed a Virtual Security Technology Center for a National Consulting Firm and ran an ethical hacking / penetration testing team for Arthur Andersen.

He currently serves on the Board of Directors for the Institute of Internal Auditors Atlanta Chapter and formally served on the Board of Directors for Information Systems Audit and Control Association (ISACA/Atlanta & Milwaukee), and he holds a CRISC (Certified in Risk and Information Systems Control) Certification and a CDPSE (Certified Data Privacy Solutions Engineer).

Michael continues to speak nationally at events and has been published on information security topics to include: IT Audit & Governance, Malware, Ransomware and Spear Phishing. In 2018 he was awarded the William Mulcahy Excellence through leadership Award by the Institute of Internal Auditors. Recently Michael was published in the AHIA's New Perspectives and Internal Auditor Magazines.



## Six Types of Vendor Risk

1. Cybersecurity risk
2. Compliance risk
3. Reputational risk
4. Financial risk
5. Operational risk
6. Strategic risk



Third-Party Risk is the potential risk that arises from organizations relying on outside parties to perform business services or activities on their behalf.

Organizations are faced with a growing awareness that risk and compliance challenges no longer stop at traditional organizational boundaries.

Establishing the wrong business relationships—or allowing current ones to sour through poor management—can force an organization to confront reputational and existential threats.

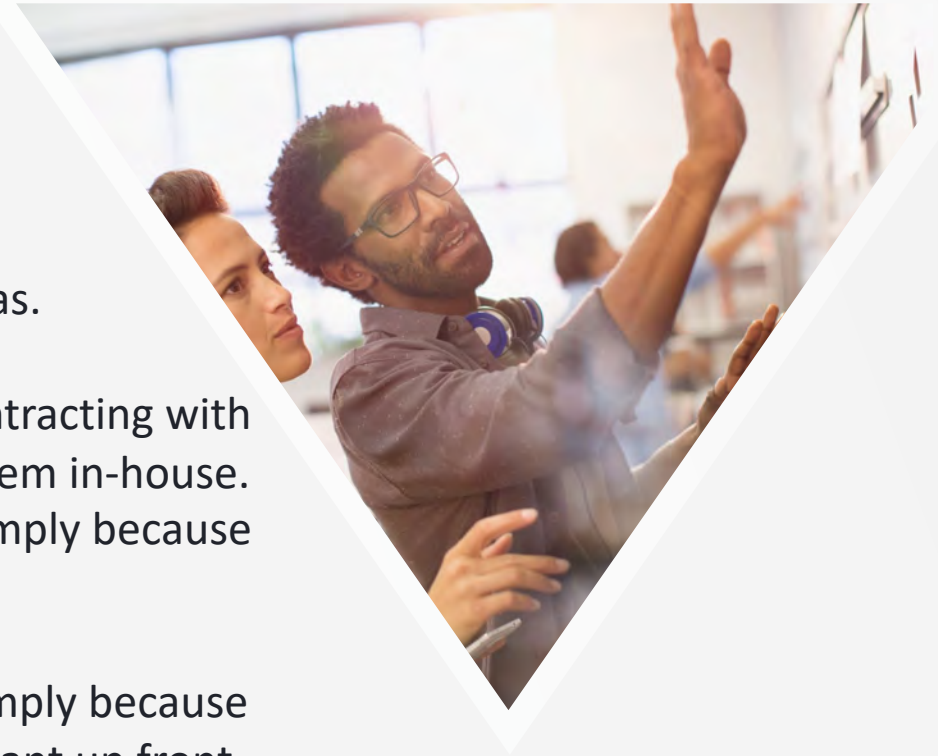
# 3<sup>rd</sup> Risk Management



## **Polling Questions 1:**

Does your audit department currently participate in the Vendor Risk Management Process?

# Why Are Vendors and Third Parties Important to Business?



The competitive advantages offered by vendors fall into a few key areas.

**Specialization:** Some products and services are so specialized that contracting with a dedicated company can be better than trying to make or perform them in-house. It's also impractical for some companies to perform every function, simply because there are so many. Vendors allow for focus on core competencies.

**Cost Savings:** Many companies use vendors to fulfill essential roles simply because it's cheaper than trying to do so in-house, which might require significant up front investments.

**Globalization:** With the rising tide of world commerce, it's practically required to have vendors that can help companies compete overseas. Things like legal services, translations, and marketing require people who are knowledgeable in other countries and can bridge the many gaps.

For all the benefits they offer, third parties have some significant drawbacks. A few key risks are listed below.

## Downsides of Third-Party Relationships



**Financial Risk:** Risk that a third party could damage financial performance. For instance, the company could fall short of revenue goals after a supplier provides a faulty component, impairing sales.

**Reputational Risk:** The risk arising from negative public opinion created by a third party. Dissatisfied customers, inappropriate interactions, poor recommendations, security breaches, and legal violations are all examples that could harm a company's reputation and standing.

**Regulatory/Compliance Risk:** Risk that a third party will impact compliance with laws, rules, or regulations, or from noncompliance with internal policies or procedures. For example, if a supplier violates labor or environmental laws, the principle organization can still be found liable and face fines.

**Operational Risk:** Risk that a third party could cause loss from disrupted business operations. Examples include a software vendor being hacked, leaving a company with a downed system, or a supplier being impacted by a natural disaster.

**Strategic Risk:** Strategic risk is the risk arising from adverse business decisions, or the failure to implement appropriate business decisions in a manner that is consistent with the institution's strategic goals. The use of a third party to perform critical functions can expose an institution to strategic risk.

# Cybersecurity Risk

- ❖ Compliance risk
- ❖ Reputational risk
- ❖ Financial risk
- ❖ Operational risk
- ❖ Strategic risk



Often organizations are breached due to the security weaknesses introduced by third parties that possess sensitive information or are granted access to systems or intellectual property.

Cybercriminals have become extremely sophisticated and specific when targeting organizations and their users, as they often work to identify weak links that will enable access to privileged and highly confidential data, such as **financials, customer data** or **intellectual property**.

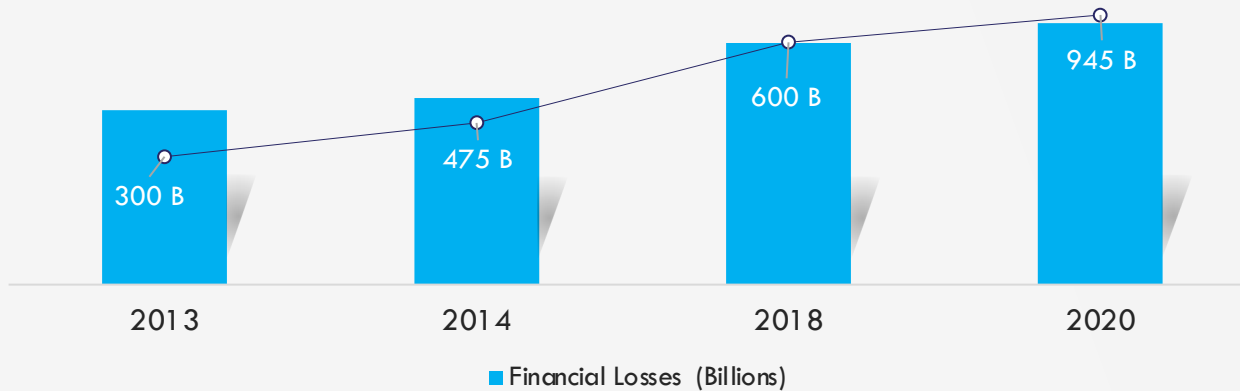
**3<sup>rd</sup> Risk  
Management**



# Financial Losses are ALWAYS on the rise due to Cybercrime

This slide portrays information regarding the concerns that are currently existing in the organizations. It is essential for top level management to keep check on existing concerns as they have severe impact on the growth in terms of huge financial losses and bad public image.

### Reported Financial Losses due to Increase In Cybercrimes



### 2020 Ponemon Institute

- Over the past two years, 53% of organizations have experienced at least one third-party-caused data breach, with remediation costs averaging \$7.5 million.

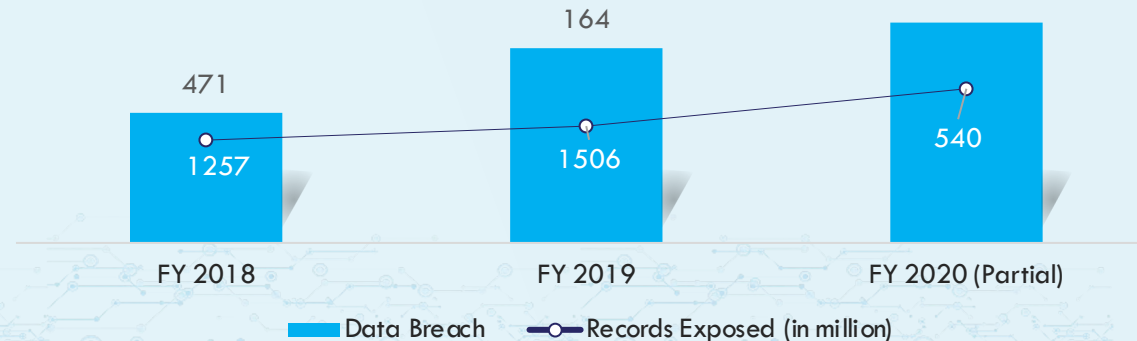
### Key Takeaways

- Observing rise in data breach incidents
- Risk of records of millions get exposed containing confidential and sensitive information has also been increased with breach incidents
- No real-time breach notification leads to breach incidents and reputational uncertainty

R

>>>>

### Data Breaches and Records Exposed

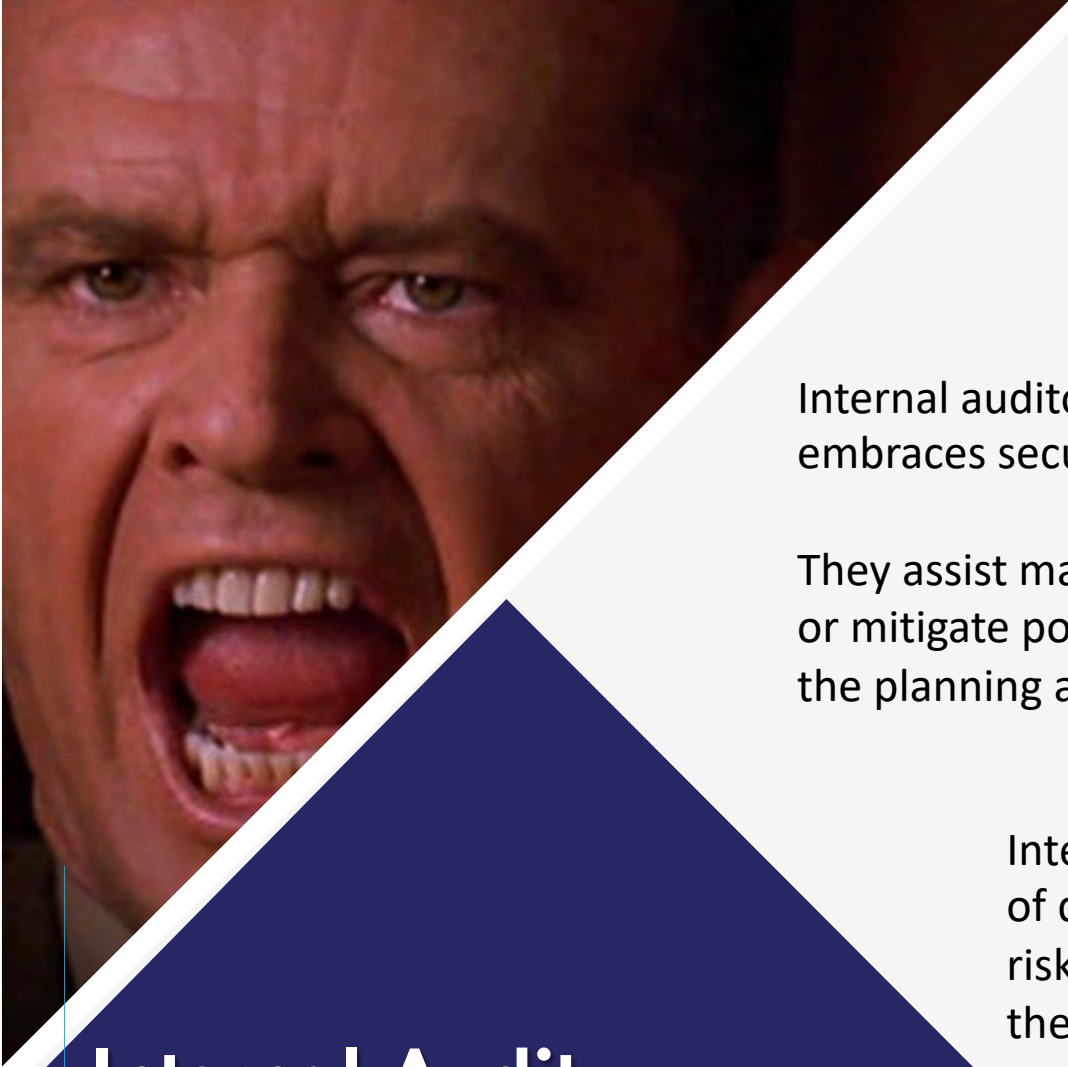


# Third-Party Nation State Cyber Breach

"I think from a software engineering perspective, it's probably fair to say that this is the largest and most sophisticated attack the world has ever seen," - Brad Smith, President of Microsoft said during an interview that aired on Sunday on the CBS program "60 Minutes."

# solarwinds





## **Internal Auditor: You want me on that wall! You need me on that wall!**

Internal auditors support management's efforts to establish a culture that embraces security, responsiveness and compliance.

They assist management with the evaluation of internal controls used to detect or mitigate potential threats to the organization and should be involved during the planning and execution of an Incident Response Plan.

Internal Audit is uniquely positioned as the organization's third line of defense. An independent internal audit function will, through a risk-based approach to its work, provide assurance to the organization's board of directors and senior management.

**Internal Audit**  
**Risk Mitigation Expertise**



## **Polling Questions 2:**

What is the number 1 risk area for your company as it relates to vendor third party risk?



Security frameworks make it possible for organizations to speed up the adoption of strong cybersecurity measures. They don't need to start from scratch when working on their security practices within their company. Some of these frameworks are mandated by the industry that they operate in, while others are voluntary to offer a security foundation.

- HIPAA
- PCI DSS
- NIST SP 800-53
- NIST Cybersecurity Framework
- HITRUST
- ISO 27000 Series
- NERC 1300
- ANSI/ISA 62443
- COSO
- COBIT 5



- How does the Company Handle Cybersecurity Risks?
  - Optimizing Cybersecurity Framework Roadmap
  - Categorization of Cyber Risks
  - Risk Assessment Matrix
  - Cybersecurity Risk Management Worksheet
  - Cybersecurity Incident Response Plan

# Initiating Cyber Risk Management Program

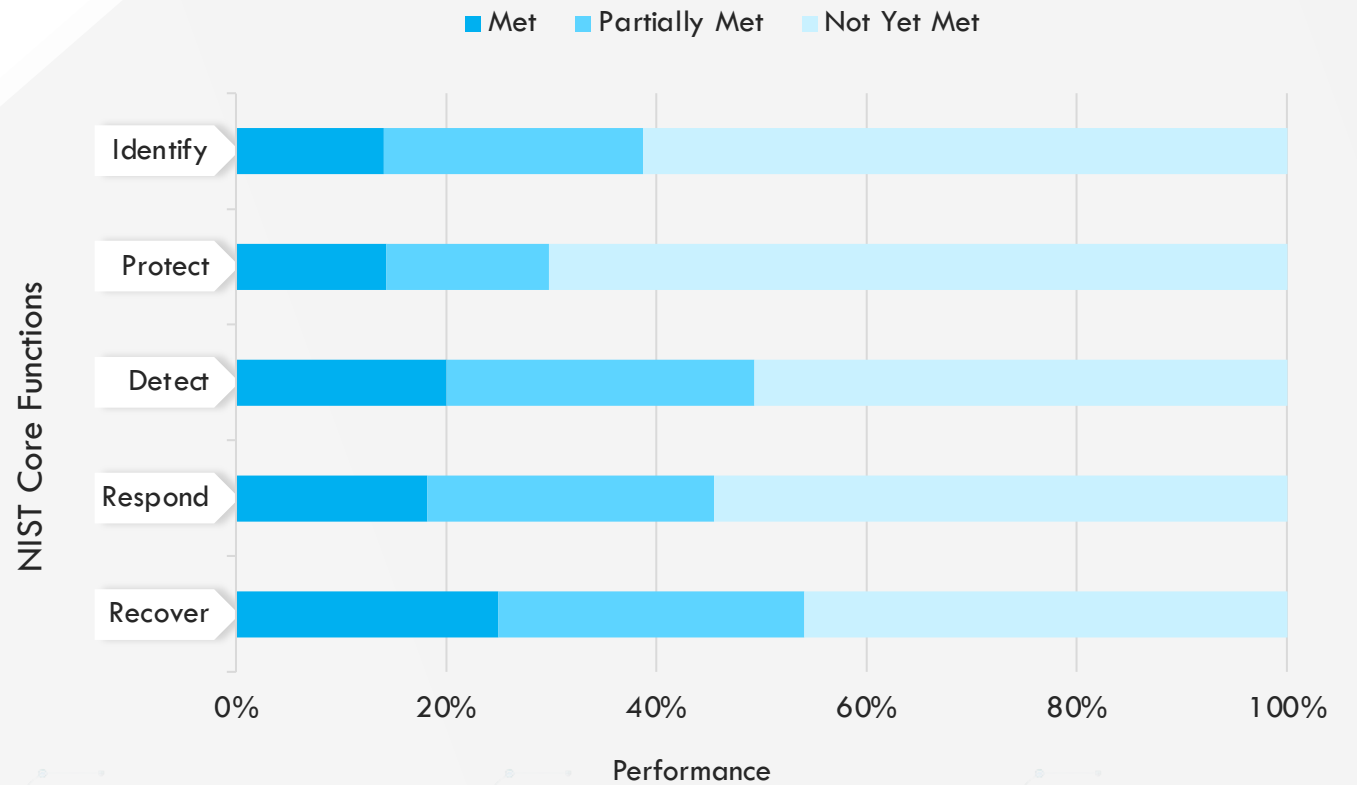


**Note –**  
The current cybersecurity framework will be judged on certain parameters mentioned below

- Identify – Asset management, governance
- Protect – Data security
- Detect – Threat intelligence
- Recover – Incident response planning
- Recover – Incident recovery

# Analyzing IT Department on NIST Cybersecurity Framework

This slide portrays information regarding how an auditor might analyze the company's current cybersecurity framework.








\*NIST – National Institute of Standard and Technology



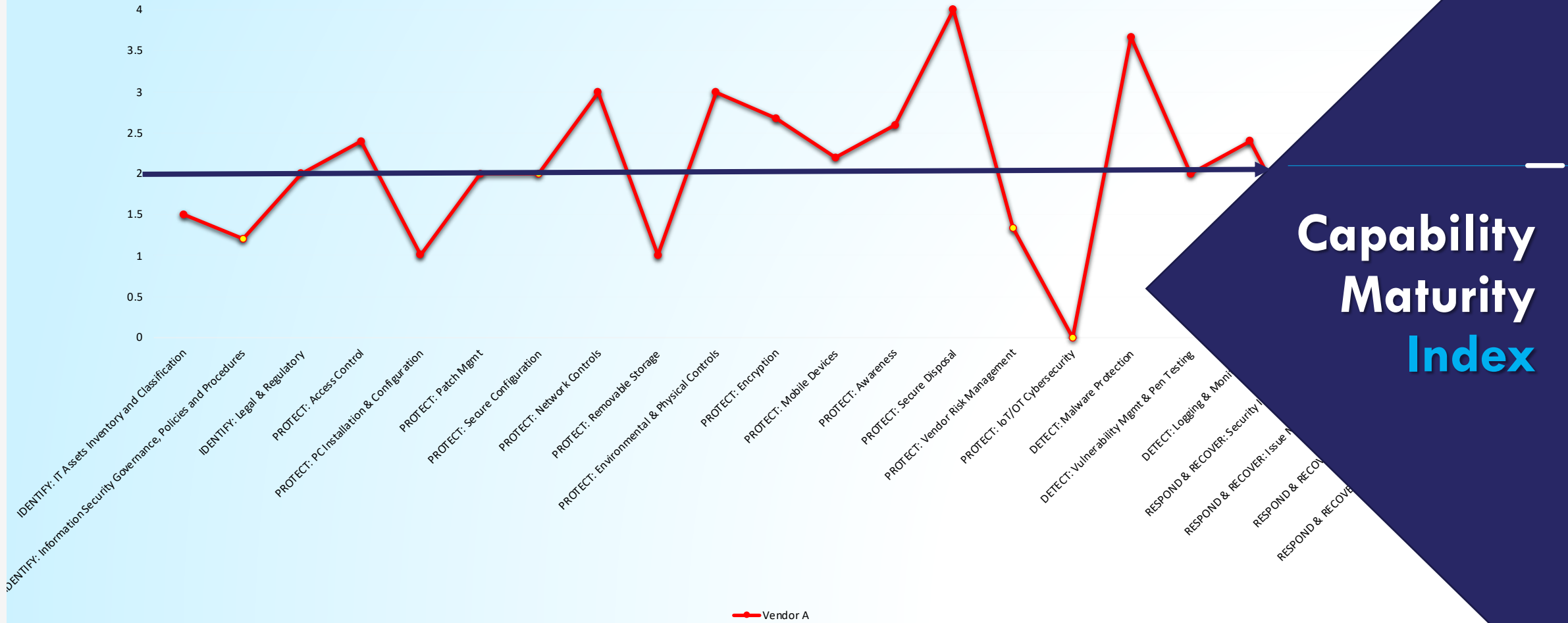
# Determining an organizations current Capabilities

This slide portrays information regarding assessment of current cybersecurity framework on certain standards.

	Description	Key Enablers	Minimum Standard	Evolving Strength	Best in Class
 <b>Identify</b>	Assessing cybersecurity risk & their impact on firm and employees	Asset Management		<input checked="" type="checkbox"/>	
		Governance	<input checked="" type="checkbox"/>		
		Business environment	<input checked="" type="checkbox"/>		
 <b>Protect</b>	Safeguarding critical infrastructure service delivery	Data Security	<input checked="" type="checkbox"/>		
		Access Control	<input checked="" type="checkbox"/>		
		Protective Technologies			<input checked="" type="checkbox"/>
 <b>Detect</b>	Event occurrence identification	Threat Intelligence	<input checked="" type="checkbox"/>		
		Continuous Monitoring	<input checked="" type="checkbox"/>		
		DLP			
 <b>Response</b>	Appropriate action to detected cybersecurity event	Communication		<input checked="" type="checkbox"/>	
		Response Planning	<input checked="" type="checkbox"/>		
		Compliance Response			<input checked="" type="checkbox"/>
 <b>Recovery</b>	Recovering capabilities impaired by cybersecurity event	Incident recovery management	<input checked="" type="checkbox"/>		
		Ransomware	<input checked="" type="checkbox"/>		
		Ability to respond to clients			<input checked="" type="checkbox"/>

The capability index is an effective tool that helps in evaluating cyber risk by establishing a base-line and plotting how a vendors control environment does in comparison.

**Audited Vendor A vs Company's Minimum Standards**

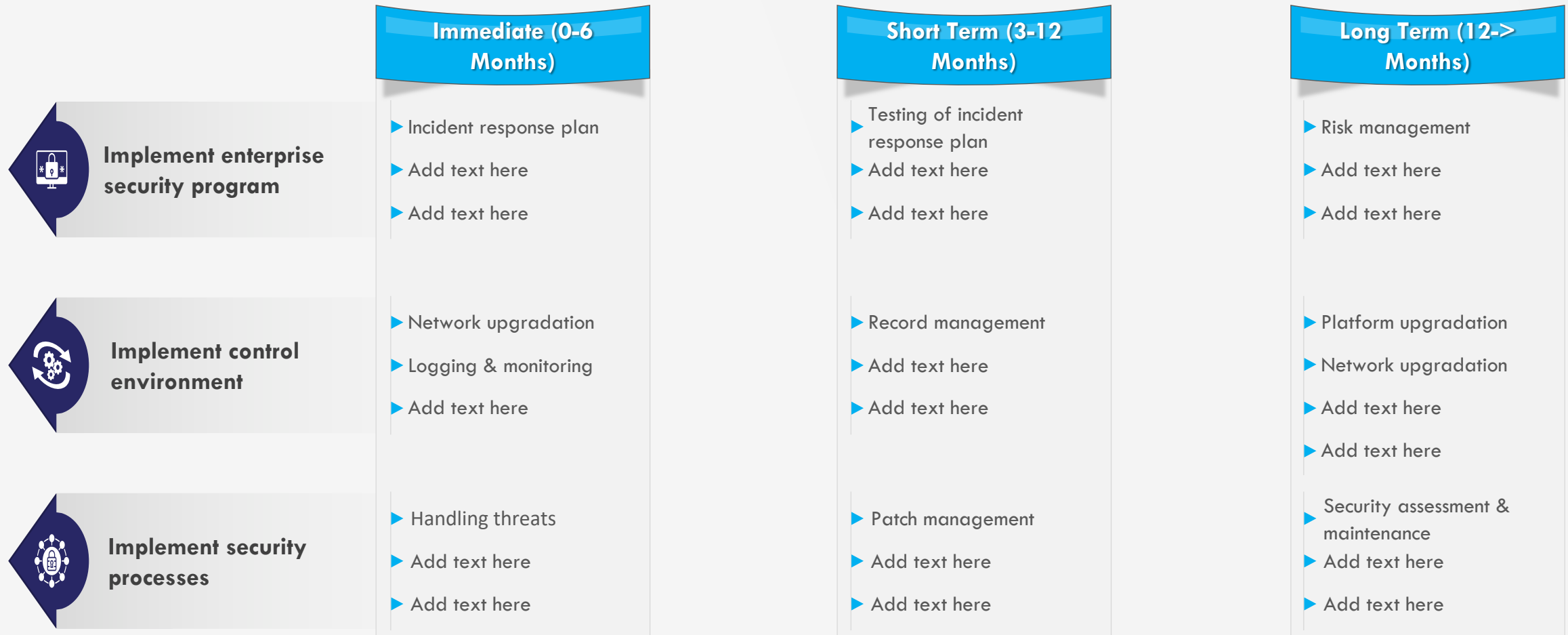


**Capability  
Maturity  
Index**



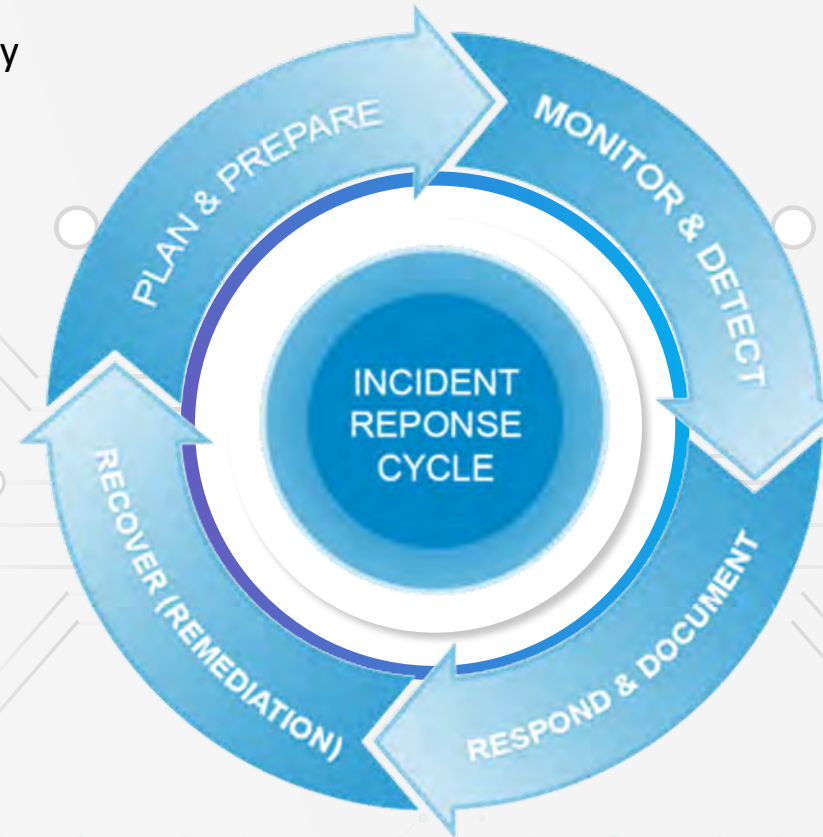
# Optimizing Cybersecurity Framework Roadmap

This slide portrays information regarding optimization of current cybersecurity framework. The IT department will require to fulfill crucial activities in specific timeframe.



- Governance strategy planning
- Skills development planning and training

- Incident Response Plan (IRP), Most organizations today would do well to expand their efforts to mitigate the consequences of inevitable breaches, which likely affect infrastructure systems and compromise key data such as personally identifiable information. An incident-response (IR) plan guides the response to such breaches. The primary objective of an IR plan
  - Manage an incident in a way that limits damage
  - increases the confidence of external stakeholders
  - reduces recovery time and costs.



# Incident Response Plan

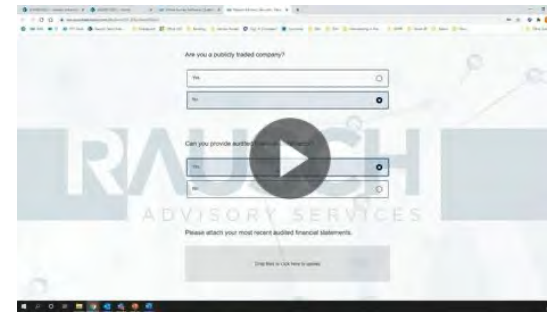


## **Polling Questions 3:**

How does your company track vendor risk?



# COMPLIANCE MADE EASY.



- Rausch designed the Rausch Assessment Solution “RAS” to provide a SaaS based platform to perform advanced risk assessments, provide consistency and reduce fees significantly.
- Utilizing RAS has further reduced the impact to the process owners. This allows them to self-assess their environment and simply provide data uploads such as SOC reports, COI, evidence of controls directly into the platform reducing time as the evidence is automatically mapped to the work papers and vendor portal.
- An auditee can sign-in securely to a client branded assessment and take their time answering questions and uploading documents when directed. They can simply close the browser and when signing back in pick back up where they left off.
- RAS provides learning capabilities for the auditee as the programs are all mapped back to internationally recognized standards such as NIST, CoBit 5, COSO and ISO.



# RAS

## COMPLIANCE MADE EASY



In all of our service offerings the RAS platform fosters standardization and consistency by leveraging recognized frameworks or existing client methodologies to help facilitate the efficient collection of documents, control information or auditee responses. Additionally, Rausch leverages data analytics to further expedite the audit process where possible.



Shannon Collins, VP of Compliance – W.S. Badcock  
“The Rausch team has been wonderful to work with and helped us create a robust vendor risk assessment solution that meets all the requirements for which we were looking. Because we are a finance company, we had some special compliance requirements that needed to be included in the risk assessment. Without hesitation, the Rausch team jumped into action and made sure that all of our requirements were met, and expectations exceeded. “



# CHOOSE RAUSCH

TO DELIVER THROUGH LEADERSHIP, RESOURCE MANAGEMENT  
AND POSITIVE RETURN ON INVESTMENT IN THE AREAS OF:  
FINANCE & ACCOUNTING · INTERNAL AUDIT · INFORMATION SECURITY



**Atlanta Office**  
5825 Glenridge Drive  
Building 1-212  
Atlanta GA 30328  
404-775-1151

**RAS**  
Compliance Made Easy  
info@rauschadvisory.com  
www.rauschadvisory.com

**San Francisco Office**  
1390 Market Street  
Suite 200  
San Francisco, CA 94102  
415-965-6776