# MARYLAND HOSPITAL CYBERSECURITY SYMPOSIUM

## Cyber Liability:

*Fail Points in Policy,*
*Vendor Accountability and*
*Cyber Insurance*

Sept. 2016

pwc

# *Discussion Points*

- **“Cyber Liability”**
- **Policy Fail Points**
- **Vendor Accountability**
- **Cyber Insurance**

# *What is Cyber Liability?*

- **Cyber Risk** is any risk of financial loss, disruption or damage to the reputation of an organization from some sort of failure of its information technology systems[1].
- **Cyber Liability** addresses both the *first- and third-party risk* associated with e-business, the Internet, networks, data and informational assets.
  - Includes the risk that arises from the unauthorized use of, or unauthorized access to, electronic data or software within your network or business.
  - Can extend to risk of liability claims for spreading a virus or malicious code, computer theft, extortion, or any unintentional act, mistake, error, or omission made by your employees while performing their job.

[1] – Institute of Risk Management, https://www.theirm.org/knowledge-and-resources/thought-leadership/**cyber-risk**/

# Policy Fail Points

*In terms of Business Resilience, here is what trips up most organizations relating to Cybersecurity:*

- Unclear Roles and Responsibilities
- Static P&Ps
- Lack of Critical Asset Inventory
- Poor Vulnerability Management
- Immature Threat Analysis and Breach Detection Processes
- Poor Employee Training/Monitoring
- Poor Vendor Management
- Lack of Tested Incident Response Plan (and BCP and DRP…)

# How does this relate to your Vendors or Contractors?

## Healthcare: Sample headlines involving Third Parties

**$1.55 million settlement underscores the importance of executing HIPAA business associate agreements**

OCR's investigation indicated that the hospital **failed to have in place an appropriate business associate agreement**, as required under the HIPAA Privacy and Security Rules, so that its business associate could perform certain payment and health care operations activities on its behalf.

– U.S. Dept of HHS on *March 16, 2016*

**Improper disclosure of research participants' protected health information results in $3.9 million HIPAA Settlement**

A **laptop** computer containing the **electronic protected health information** (ePHI) of approximately 13,00 patients and research participants was **stolen** from an employee's car.

– U.S. Dept of HHS on *March 17, 2016*

**FTC Data Security Settlement Highlights Need for Third Party Vendor Management and Oversight**

Federal Trade Commission (FTC) announced a settlement with a translation services providers following the public **exposure of thousands of medical transcript files** containing personal medical information.

– *HL Chronicle of Data Protection, January 2014*

**Vendor mistake causes breach of 32,000 patients' data.**

The vendor was hired to transcribe care notes on what was supposed to be a secure website. However, the information remained publicly accessible because the vendor apparently **failed to activate a firewall.**

– *Healthcare Business & Technology, August 2013*

**$750, 000 HIPAA settlement underscores the need for organization-wide risk analysis**

90,000 individuals **ePHI was access after an email attachment with malicious malware was downloaded.** Affiliated covered entities must have in place appropriate policies and processes to assure HIPAA compliance with respect to each entities that are a part of the affiliated group.

– U.S. Dept of HHS on *December 14, 2015*

# Healthcare Regulatory Drivers

*Companies in the healthcare industries need to monitor their third party relationships for compliance with regulatory requirements, including:*

***Incidents attributed to current third-party business partners jumped 56% in 2015, an increase that prompted some large US healthcare payers to institute strong policies around required attestations (HITRUST, SOC 2, etc.) for their critical vendors.[1]***

- **Health Insurance Portability and Accountability Act (HIPAA):** Companies in the health industries can be held responsible for vendors' lack of adherence to HIPAA regulations related to Protected Health Information (PHI). The HIPAA rules generally require that covered entities having a formal Business Associate relationship with a vendor, maintain a Business Associate Agreement (BAA) to ensure that the business associates will appropriately safeguard PHI
- **HIPAA Omnibus Rule:** The Omnibus Rule revised the existing business associate agreement (BAA) requirements to now require a business associate to comply with the Security Rule, to ensure any subcontractors enter into a contract or other arrangement to protect the security of e-PHI, and report to the covered entity breaches of unsecured PHI
- **Health Information Technology Act (HITECH):** Among other requirements, HITECH extended the liability of Covered Entities under HIPAA to their Service Providers
- **Food and Drug Administration (FDA):** Organizations regulated by the FDA are required to have strong vendor controls in place for a range of sectors including Drugs, Medical Devices, Food, Cosmetics and Tobacco Products
- **Good x Practice(GxP):** A series of quality guidelines and regulations used in sectors such as pharmaceuticals, medical device, cosmetics and food. Manufacturers must establish and maintain procedures to ensure that all products conform to traceability and accountability requirements for all parties that contributed to the development and production of the products

*[1] PwC, CSO, CIO, The Global State of Information Security® Survey 2016*

# Healthcare Key Points of Focus

**Expanding and evolving regulatory landscape**

Regulatory and compliance pressures (e.g., HIPAA and HITECH Act) continue to drive healthcare organizations to manage third party risk

**Increasing reliance on third parties**

Healthcare organizations have substantial reliance on third parties (including decentralized IT), and like most industries, continue to look for third party support to streamline operations and reduce cost

**Lack of a formal TPRM governance function**

Healthcare organizations lack a clear understanding of the inventory of the third parties, flow of sensitive data, and sustainable process for ongoing monitoring of risk, including shadow IT

**Absence of a formal third party risk management process**

Healthcare organizations lack a consistent third party risk assessment process -- including frequency based on risk as well as how to track and remediate based on findings

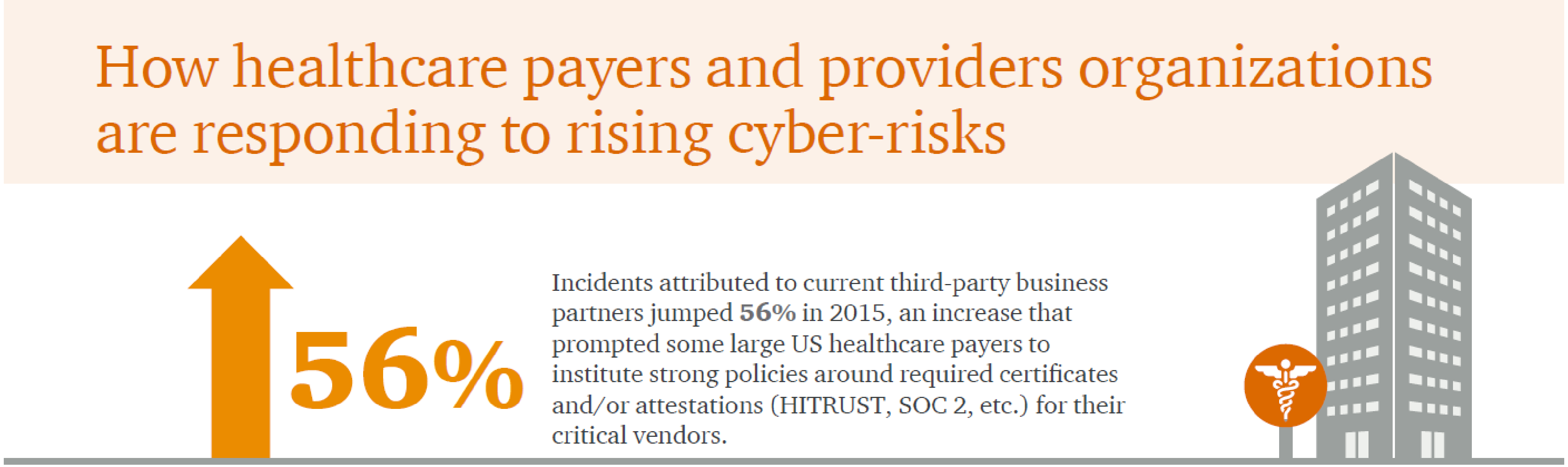
**Sourcing decisions made without evaluating risk**

Various areas of Healthcare organizations are making sourcing decisions before evaluating/classifying risk to data (privacy) and the control environment (security)

# *2016 PwC Global State of Information Security Survey**

## Key findings from the GSISS Relating to Healthcare Payers and Providers

## *Incidents Attributed to Third-Parties* Include:



How healthcare payers and providers organizations are responding to rising cyber-risks

56%

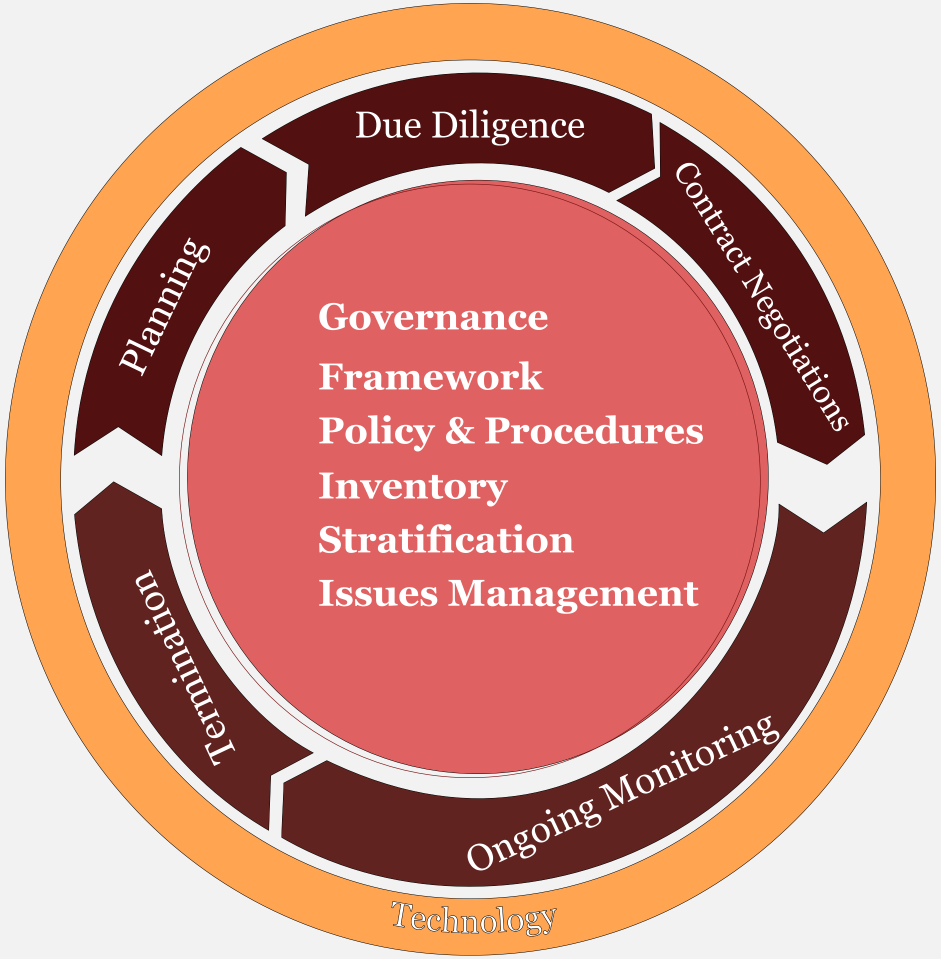
Incidents attributed to current third-party business partners jumped **56%** in 2015, an increase that prompted some large US healthcare payers to institute strong policies around required certificates and/or attestations (HITRUST, SOC 2, etc.) for their critical vendors.

* Source: PwC, CSO, CIO, *The Global State of Information Security® Survey 2016*

# *A High-level Perspective on Managing Third-Parties*

**Third parties**

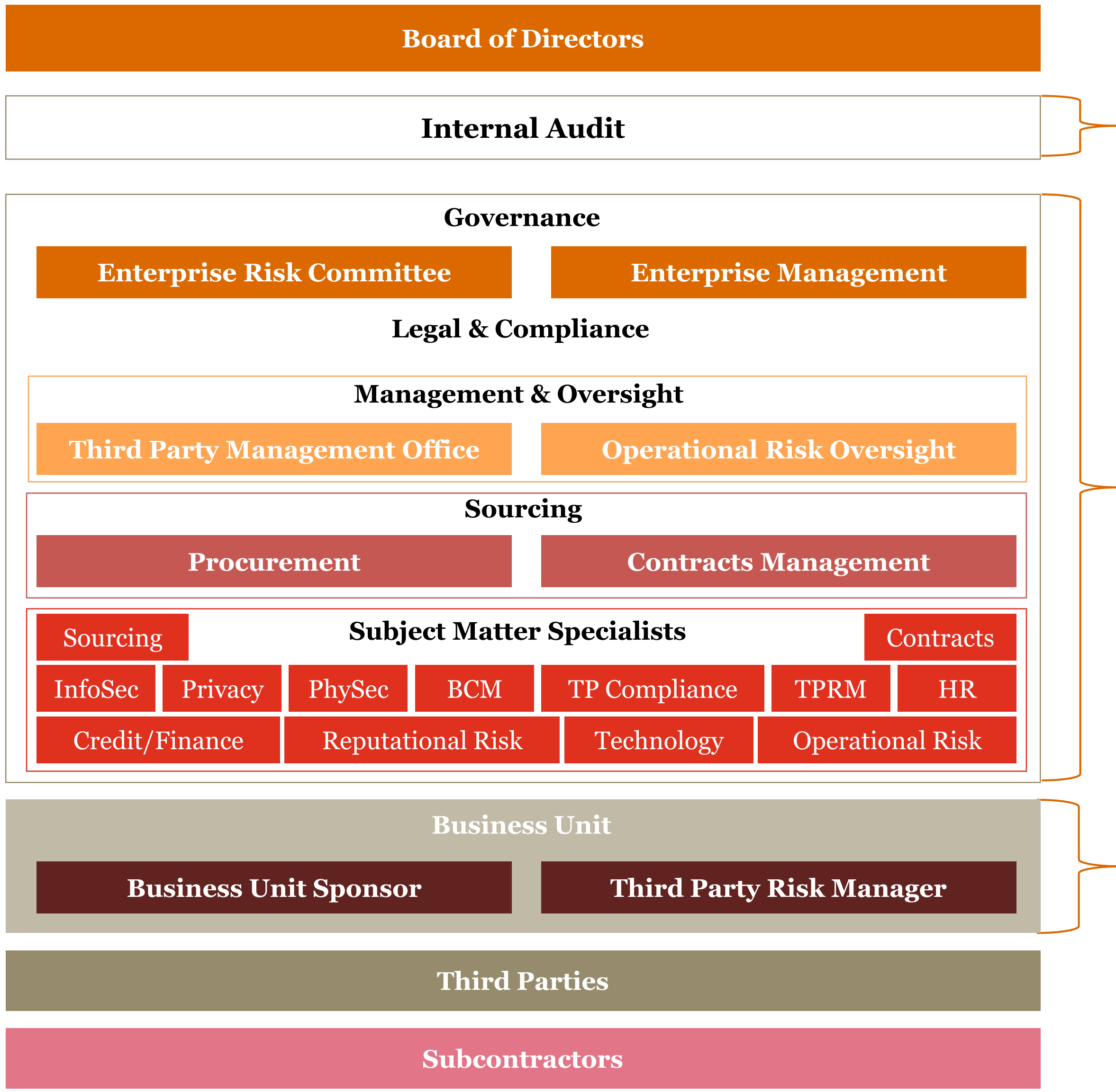
- Vendors
- Suppliers
- Joint Ventures
- Business Channels
- Marketing Partners
- Affiliates
- Business Associates
- Regulated Entities



**Risk Considerations**

- Reputational
- Operational
- Credit/Financial
- Business Continuity and Resiliency
- Strategic/Country
- Subcontractor
- Technology
- Info Security & Privacy
- Compliance

# Program Governance



Board of Directors

Internal Audit

Governance

Enterprise Risk Committee | Enterprise Management

Legal & Compliance

Management & Oversight

Third Party Management Office | Operational Risk Oversight

Sourcing

Procurement | Contracts Management

Subject Matter Specialists

Sourcing | Contracts

InfoSec | Privacy | PhySec | BCM | TP Compliance | TPRM | HR

Credit/Finance | Reputational Risk | Technology | Operational Risk

Business Unit

Business Unit Sponsor | Third Party Risk Manager

Third Parties

Subcontractors

**Third Line of Defense**

- Independent assurance
- Independently test, verify and evaluate risk management controls against internal policies
- Report upon effectiveness of the program

**Second Line of Defense**

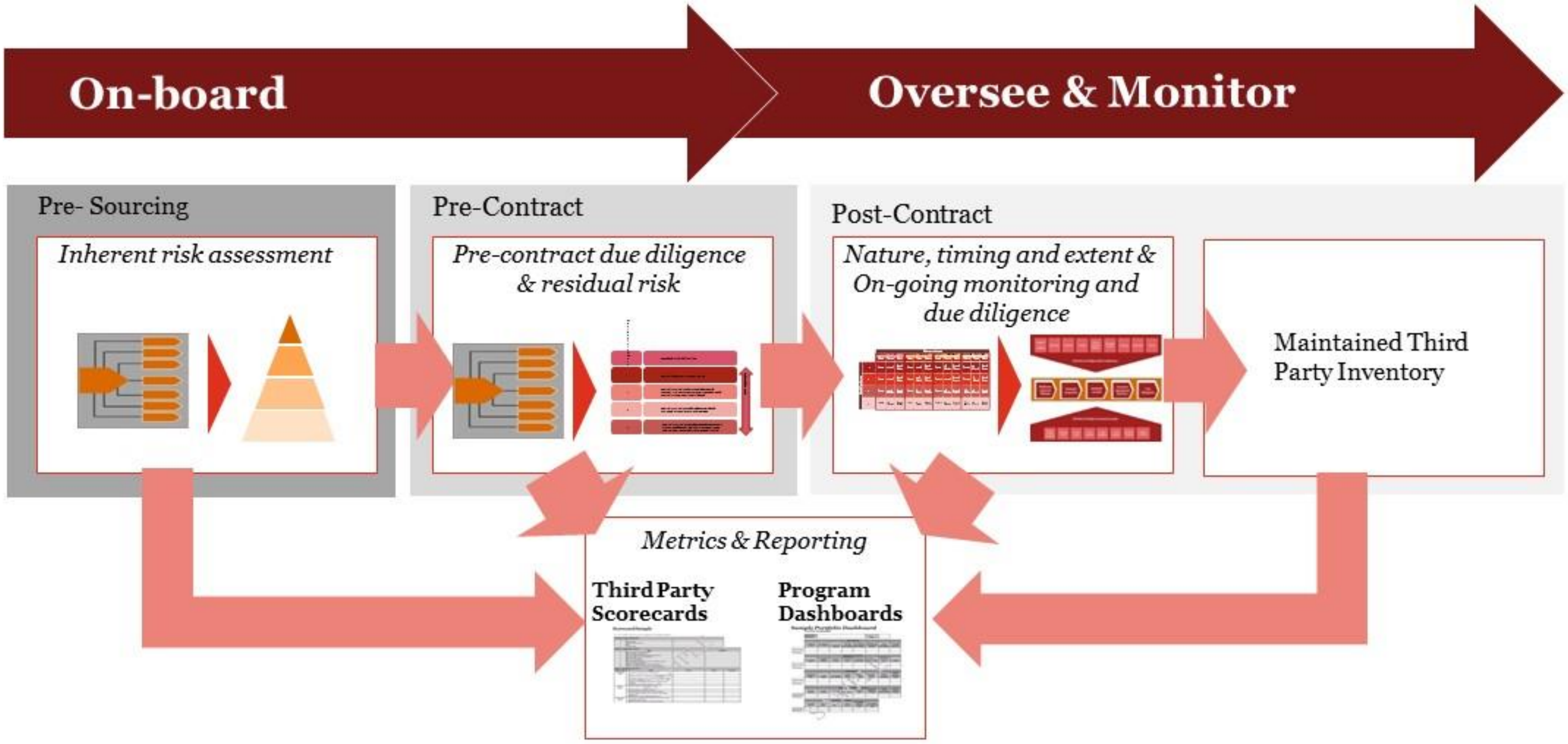
- Independent compliance framework, policy & oversight
- Business partners work with the BU's to identify, assess and mitigate all risks
- Design and assist in implementing company-wide risk framework and oversee enterprise risks
- Provide independent risk oversight across all risk types, business units and locations
- Perform quality assurance reviews and other targeted oversight practices to ensure that the line of business is compliant with internal policies/ external regulations

**First Line of Defense**

- Primary responsibility for compliance and owner of risk
- BU managers and third party relationship owners are responsible for identifying, assessing and mitigating risk associated with their business
- Implement internal controls and practices are consistent with company-wide policies & procedures
- Promote a strong risk culture and sustainable risk-return decision making

# Planning

Planning and Inherent Risk Stratification facilitates maintenance of the third party inventory, and enables management to focus resources and efforts on those services that present greater risk to the organization.



On-board

Oversee & Monitor

Pre- Sourcing

*Inherent risk assessment*

Pre-Contract

*Pre-contract due diligence & residual risk*

Post-Contract

*Nature, timing and extent & On-going monitoring and due diligence*

Maintained Third Party Inventory

*Metrics & Reporting*

**Third Party Scorecards**

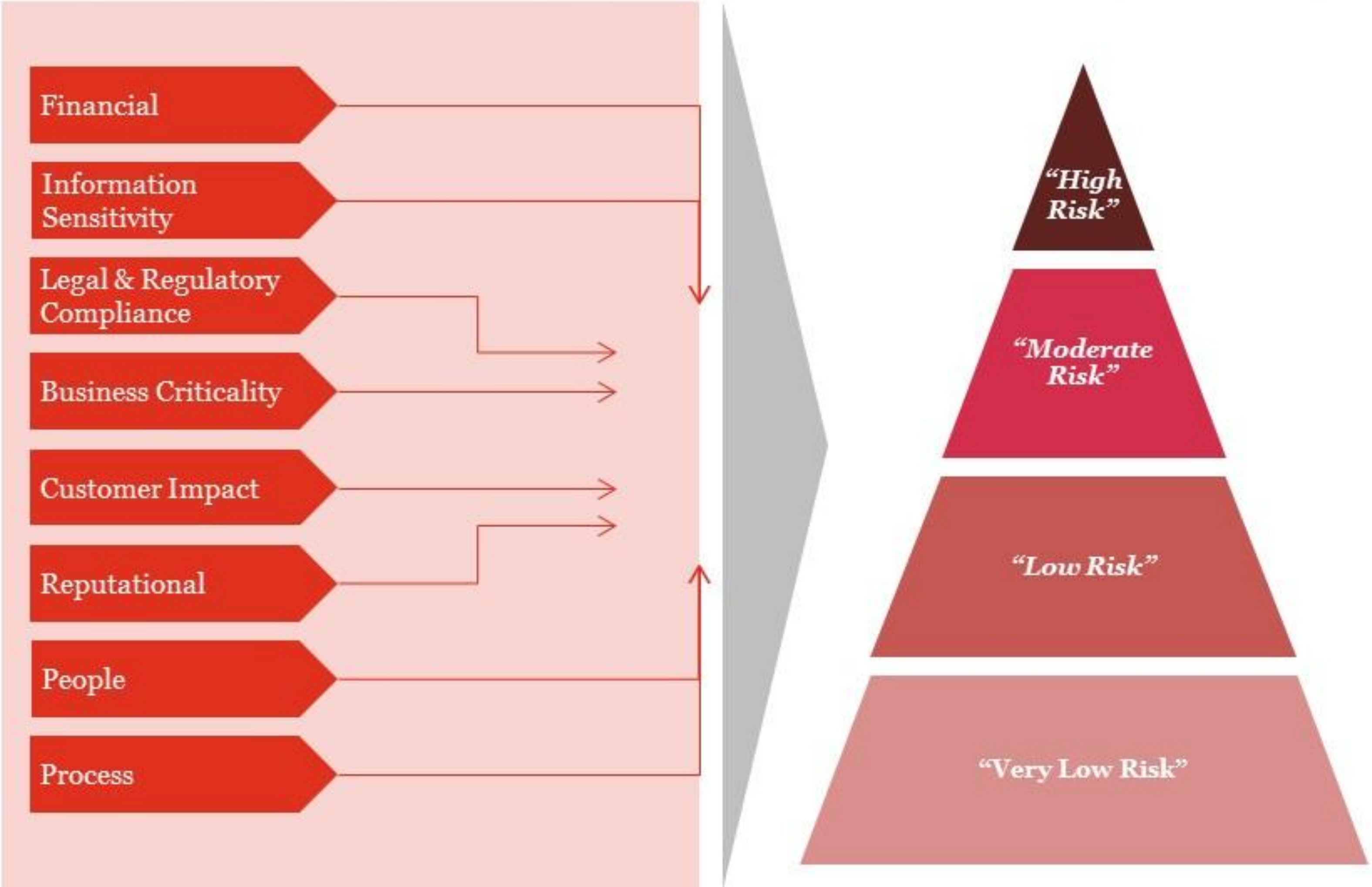
**Program Dashboards**

# Planning: Inherent Risk Methodology

*The inherent risk assessment process allows for the sorting of third party services/products by inherent risk scores and inherent risk ratings.*

*Example Inherent Risk (IR) Methodology*

*Example Risk Stratification Structure*



**1 – "High Risk"** These third parties are handling high risk services, have a critical level of disruption, access to highly restricted types of data and are client facing.

**2 – "Moderate Risk"** These third parties are handling high or medium risk services, have high level of disruption, access to restricted data and may be client facing.

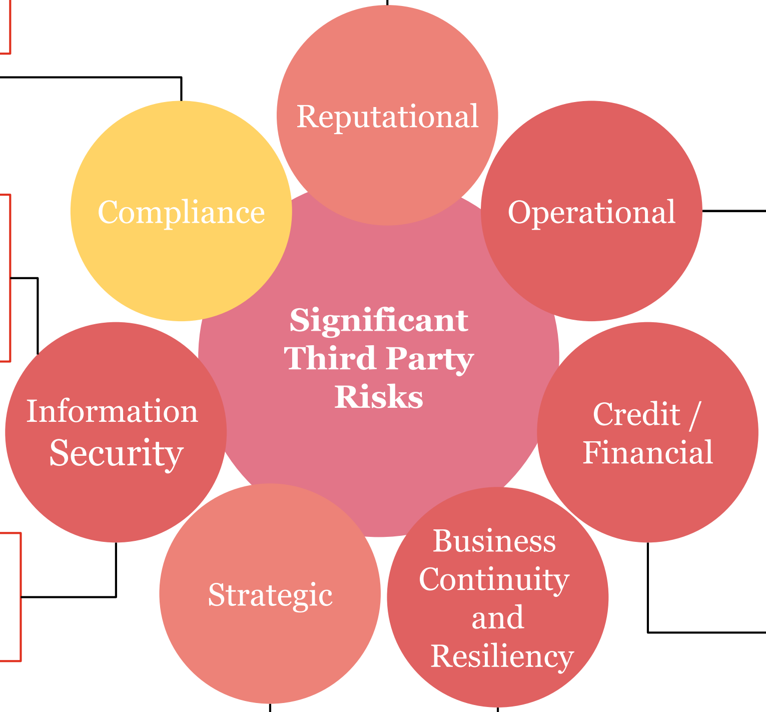
**3 – "Low Risk"** These third parties are handling medium risk services, have a moderate level of disruption, have access to restricted data and are not client facing.

**4 –"Very Low Risk"** These third parties are handling low risk services, have a low level of disruption, do not have access to restricted data and are not client facing.

# Due Diligence

The following correlates significant third party risks to the assessments utilized by organizations to evaluate the effectiveness of third party controls in place to mitigate risks.

***Legend:***
□ *Assessment*
○ *Risk*



**Compliance:**
Assesses the third-party’s ability/control framework in place to comply with laws/regulations.

**Reputational:**
Assesses the impact to the organizations reputation based on services provided by a third-party.

**Information Security & Privacy:**
Assesses third party controls over the availability, confidentiality, and integrity of third party data .

**Operational Competency:**
Assesses the ability of the third party to deliver the contracted products/services.

**Subcontractor:**
Assesses the risk management processes surrounding the use of subcontractors by third parties.

**Technology:**
Assesses the adequacy and appropriateness of the third party’s systems and applications to provide the product/service.

**Physical Security:**
Assesses facility access and security measures implemented by the third party.

**Financial:**
Assesses financial stability for the third party to continue provide the product/service.

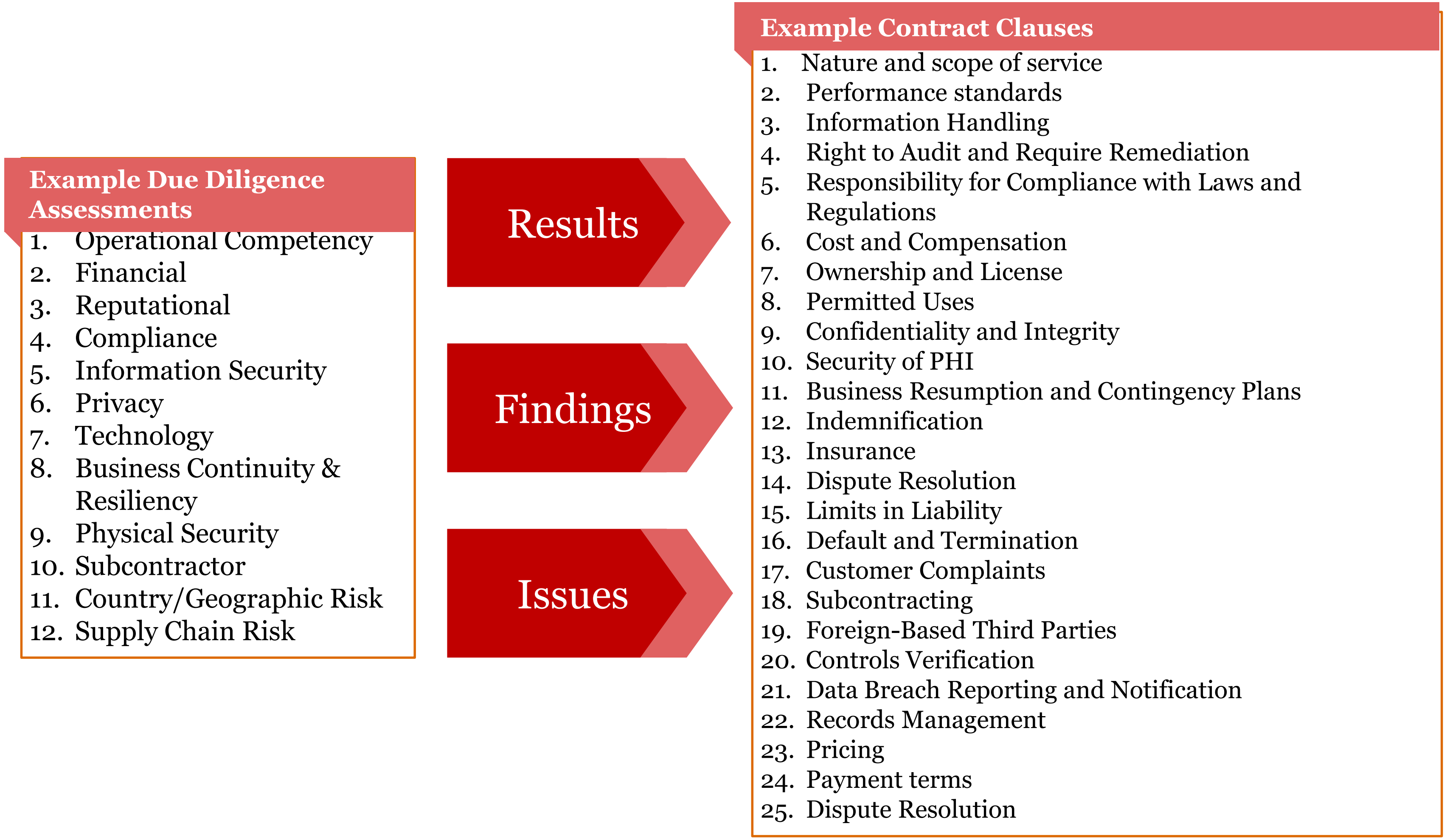
**Country Risk:**
Assesses political, geographic, regulatory, legal, and economic risks of sourcing to a country or region.

**Business Continuity & Resiliency:**
Assesses the third party’s ability to perform in the event of a process failure or catastrophic event.

# Contracting

The service risk profile should assist in driving the following internal actions:

- Inherent Risk should drive the required contract approval levels;
- Contracts should be reviewed periodically, particularly those involving critical activities and sensitive or personal information, to ensure they continue to provide obligations related to pertinent risk controls and legal protections; and
- Where problems are identified, the organization should seek to renegotiate at the earliest opportunity.



**Example Due Diligence Assessments**

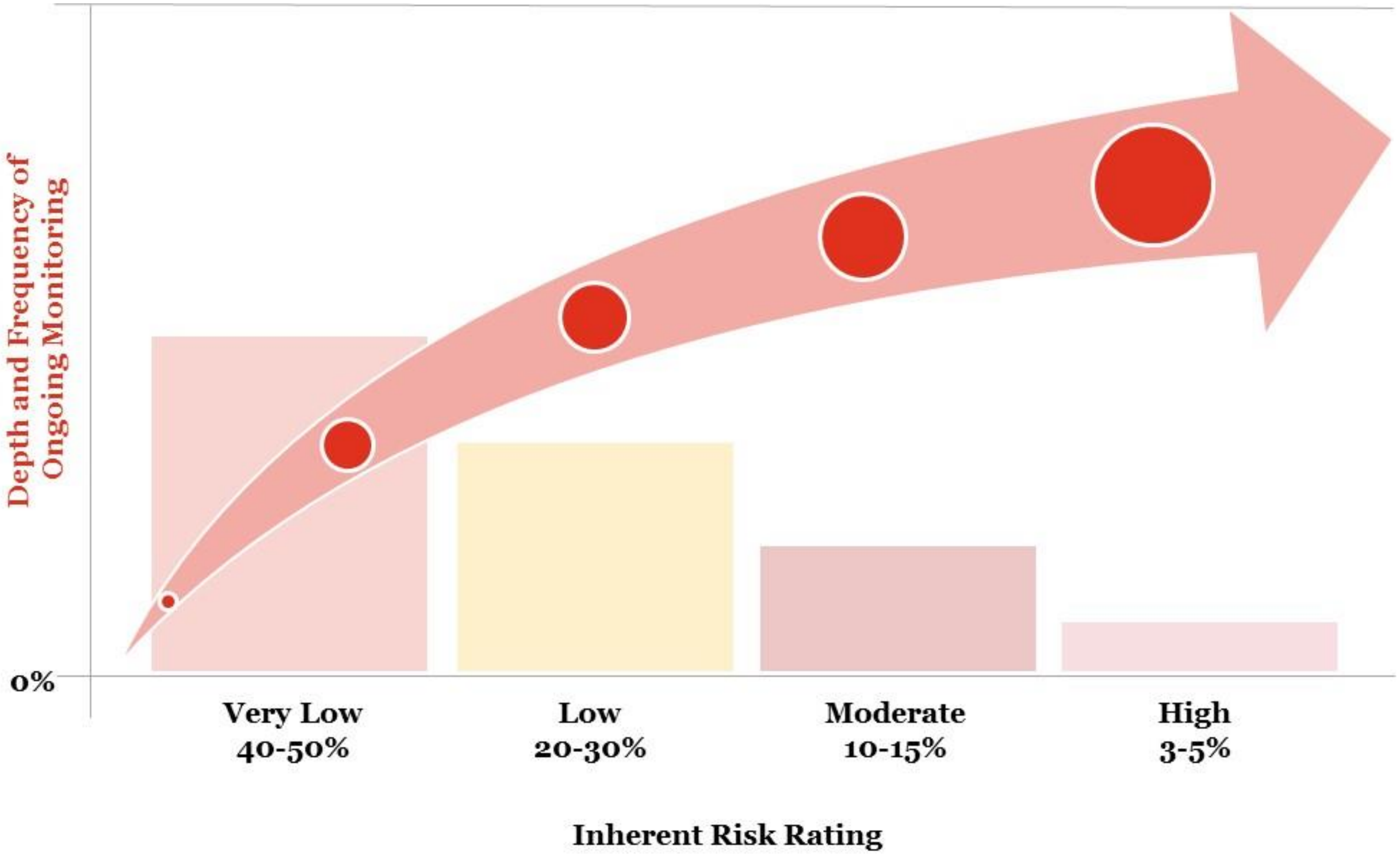
1. Operational Competency
2. Financial
3. Reputational
4. Compliance
5. Information Security
6. Privacy
7. Technology
8. Business Continuity & Resiliency
9. Physical Security
10. Subcontractor
11. Country/Geographic Risk
12. Supply Chain Risk

**Example Contract Clauses**

1. Nature and scope of service
2. Performance standards
3. Information Handling
4. Right to Audit and Require Remediation
5. Responsibility for Compliance with Laws and Regulations
6. Cost and Compensation
7. Ownership and License
8. Permitted Uses
9. Confidentiality and Integrity
10. Security of PHI
11. Business Resumption and Contingency Plans
12. Indemnification
13. Insurance
14. Dispute Resolution
15. Limits in Liability
16. Default and Termination
17. Customer Complaints
18. Subcontracting
19. Foreign-Based Third Parties
20. Controls Verification
21. Data Breach Reporting and Notification
22. Records Management
23. Pricing
24. Payment terms
25. Dispute Resolution

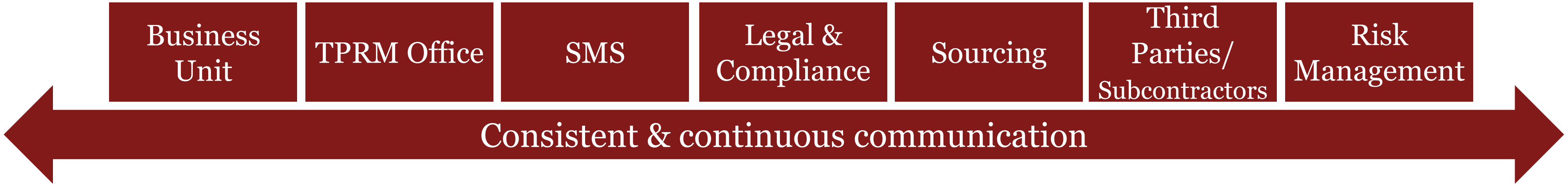
# Ongoing Monitoring

Results of the inherent risk should drive the nature, timing and extent of activities used to monitor, oversee, and re-assess third party relationships. Due to the higher costs associated with more in-depth assessment activities, a risk based approach should be leveraged ensuring higher risk relationships receive more active risk management than lower risk relationships.



# *Termination*

Each third party termination will be unique; however, there are common decisions, considerations, and results that should be addressed with key stakeholders and executed with a defined plan and checklist.


Business Unit

TPRM Office

SMS

Legal & Compliance

Sourcing

Third Parties/ Subcontractors

Risk Management

Consistent & continuous communication

### Termination decision

- Service Failure/Significant Customer Complaints
- Data Breach/Security Incident
- Regulatory/Legislative
- End of Contract
- Business Decision
- Product/Service Discontinued

### Termination considerations

- Product/Service Brought In-House
- Product/Service Transitioned to Alternate Third Party
- Customer Impact
- Operational Impact
- Patient Safety
- Contingency Procedures
- Oral & Implied Contracts
- Internal Employee Impact

### Termination result

- Interim Processes
  - NDA
  - Transfer Process Knowledge
  - Migrate or Destroy
- Information
  - Return or destruction
  - Ongoing safeguards
  - Ownership and control
- Costs
  - Monetary
  - Non-monetary
- Migrate/Sell Assets
  - Software/Intellectual Property
  - Hardware
  - Facilities
- Notification to Customers and Internal Employees

# *Cyber Insurance*

- **What is it?**
- **Why do we need it? (Isn't this covered in Technology E&O or Business Liability Insurance?)**
- **Key Considerations**

# *Cyber Insurance**

## First-Party (Direct Losses) Cyber Insurance covers:

- Crisis Management & Identity Theft Response
- Cyber Extortion
- Data Asset Protection
- Network Business Interruption

## Third-Party (Third-party losses by others) Cyber Insurance covers :

- Network Security Liability
- Privacy Liability

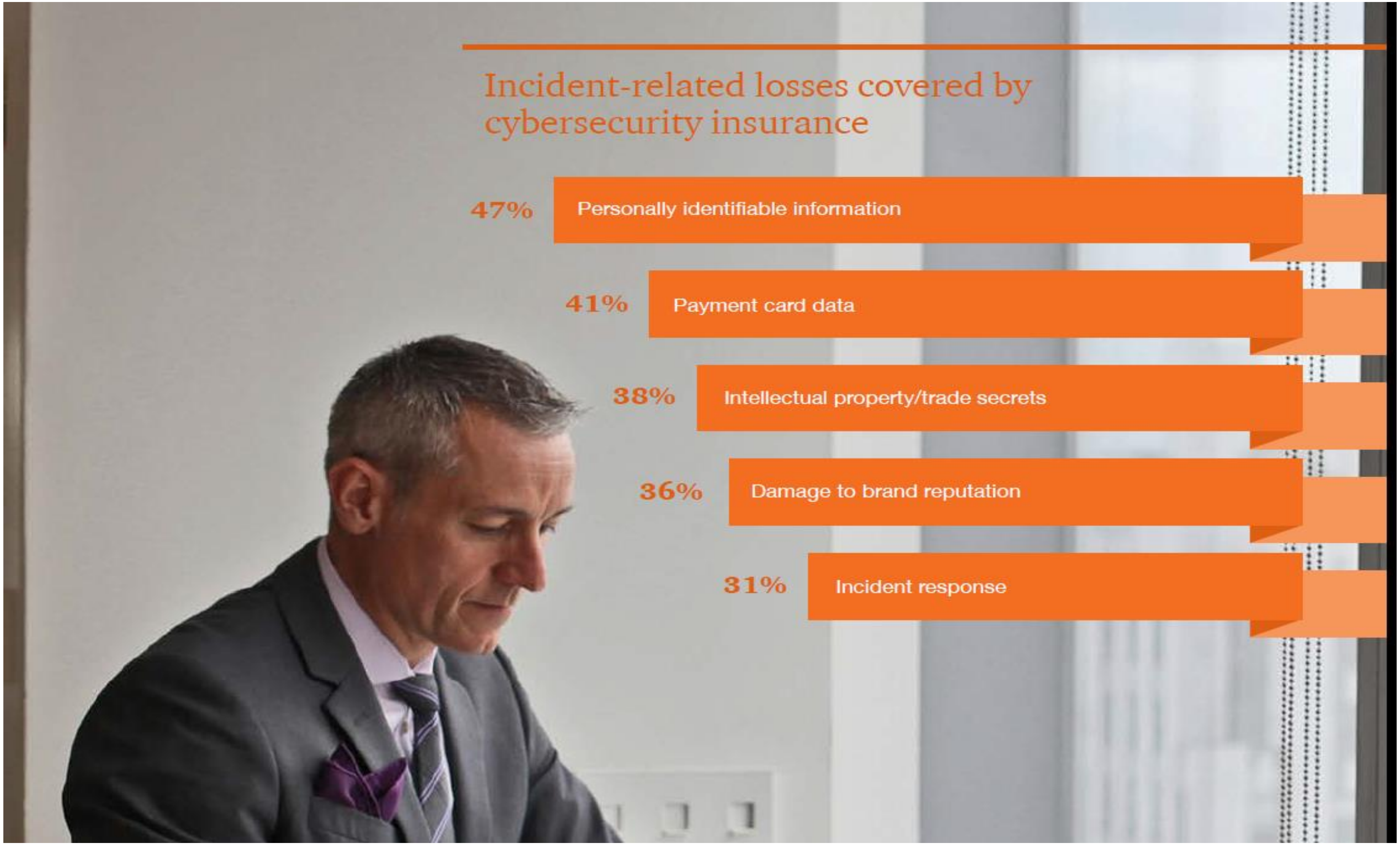
* - Financial Services Sector Coordinating Council – Purchaser's Guide to Cyber Insurance Products

# *Questions and Considerations*

- **Isn’t this covered in Technology E&O or Business Liability Insurance?**
  - Not included in these policies
  - Can be an add on or separate policy

- **How much does my organization need?**
  - No formula or one-size-fits-all guidance
  - Factors:
  - Organizational residual risk and business considerations (size, sector, maturity, risk tolerance)
  - Market supply

# *What is Typically Covered Today?*



Incident-related losses covered by cybersecurity insurance

# *Additional Hidden Value to Your Organization**

- Insurance places a dollar value on an organization's cyber risk.
- The underwriting process can help organizations identify cybersecurity gaps and opportunities for improvement.
- In addition to providing the traditional risk transfer function, many cyber insurance policies bring supplemental value through the inclusion of risk mitigation tools, as well as significant incident response assistance following a cyber incident.

* - Financial Services Sector Coordinating Council – Purchaser's Guide to Cyber Insurance Products

# *Prepare Before You Seek Cyber Insurance*

## Underwriters will want to know about*:

- Dedicated Security Resources
- Security P&P's
- Security Controls
- Incident Response Plan (and BCP and DRP)
- Employee Training and Compliance
- Third-Party Vendor/Contractor Management
- Board Oversight

* - Financial Services Sector Coordinating Council – Purchaser's Guide to Cyber Insurance Products

# *What to Look for in Cyber Insurance Policies**

## Policy Construction:

- When Is Coverage Triggered?
- What are the Requirements around Notice to Insurer?
- What is Process for Approval of Organization’s Breach Counsel and/or Forensics Firm?

## Key Exclusions:

- Portable/mobile devices
- Intentional Acts/Negligence
- Nation-state actors, Terrorism, Acts of God
- Territorial Limits
- Breach at Third-party Vendor
- Post-breach Services
- Credit Monitoring Costs

* - Financial Services Sector Coordinating Council – Purchaser’s Guide to Cyber Insurance Products

# *What to Look for in Cyber Insurance Policies (Cont.)**

## Other:

- Insider Threat
- Data on Unencrypted Devices/BYOD
- Information/Data Managed by Third-party Vendors
- Replacement Costs
- Coverage for Potential Regulatory Investigations, Fines, etc.
- Damages to Corporate Clients

* - Financial Services Sector Coordinating Council – Purchaser's Guide to Cyber Insurance Products

# *Questions?*

***Lisa Gallagher***
***PwC, Managing Director, Health Sector P&S***
***703-581-2014***
***Lisa.A.Gallagher@pwc.com***

***visit www.pwc.com/gsiss2015***

This document was not intended or written to be used, and it cannot be used, for the purpose of avoiding U.S. federal, state or local tax penalties. This includes penalties that may apply if the transaction that is the subject of this document is found to lack economic substance or fails to satisfy any other similar rule of law.

This presentation has been prepared for general guidance on matters of interest only, and does not constitute professional advice. You should not act upon the information contained in this publication without obtaining specific professional advice. No representation or warranty (express or implied) is given as to the accuracy or completeness of the information contained in this publication, and, to the extent permitted by law.