



# Cybersecurity in Critical Infrastructure – Operational Technology

August 11, 2020

PwC | Operational Technology (OT) Cybersecurity Practice



# NOTES



**Anti-Trust  
Compliance**



**Please do not place the  
call on hold to avoid  
music disrupting the  
call.**



**Everyone will remain  
muted.**



**PESA will share a  
post-event summary.**



**During Q&A: If you have  
questions/comments, use chat  
function or please unmute  
yourself.**

# Cybersecurity in critical infrastructure – Operational technology

Harshul Joshi & Brad Bauch



August  
2020



# With you today



**Harshul Joshi**

PwC - Cybersecurity & Privacy Partner  
harshul.joshi@pwc.com



**Brad Bauch**

PwC - Cybersecurity & Privacy Partner  
brad.bauch@pwc.com



# Business case – The imperative for OT cybersecurity



# What is Operational Technology (OT) and where is it found?

Operational Technology (OT) systems are combinations of hardware and software that **detect or cause a change to a physical device or process**. OT is **pervasive, and expanding** as firms continue to digitally transform and depend on automation the information generated by these systems. Below are examples of OT across a variety of industries:

## Energy, Utilities, & Resources

**Oil & Gas** - Boilers, Pressure Sensors, Drilling/Drilling Telemetry, Rig Stabilization, Leak Detection  
**Power & Utilities** - Wind turbines, Water Dams, Solar Farms, Nuclear, Natural Gas, Coal  
**Chemicals** - Furnaces, Pressure Sensors, Gas/Meteorological Sensors, Pipelines  
**Mining** - Autonomous Vehicles, Drills, Collapse Sensors/Alarms, Air/Water Quality Sensors, Lighting



## Manufacturing

**Food & Beverage** - Ovens, Fryers, Boilers, Actuators, Bottlers/Canners, Conveyor Belts, Palletizers  
**Automotive/Industrial** - Robotic Assembly, Painters, Conveyors, Material Handling Robots  
**Electronics** - Clean Room BMS, HMI's and Controllers



## Healthcare

**Medical Devices** - Pacemakers, Insulin Pumps, Patient Monitors  
**Pharmaceuticals** - Robotic Arms, Refrigerators, Packagers  
**Building Management Systems** - HVAC/Air Filtration, Lighting, Fire Suppression, Physical Access Control  
**Laboratory/Surgical Equipment** - Robotic Surgical Instruments, Imaging Scanners, Pharmaceutical Dispensers



## Transportation & Logistics

**Locomotive** - Train Track Switching, Defect Detectors, Height/Width Sensors, Weight Distribution Sensors, Locomotive Control System, Braking  
**Aerospace/Maritime** - Autopilot, Safety Control, Steering Control, Propulsion, Buoyancy Control, Port Management  
**Retail/Warehouse** - Conveyors, Palletizers, Material Handlers, Pickers, Refrigerators, Building Management Systems



# How has digitization increased OT risk to organizations?

## Historical Context






Operational technology predates the information systems era and initially consisted of isolated systems running proprietary control functions on specialized hardware/software and communication protocols. These have been replaced with the same products, systems and services already in use in the information technology domain: Windows operating systems running on Intel-based hardware and connected via TCP/IP networks.

Digital transformation, coupled with enterprise **need for data, specifically around resource planning**, led to a need to connect systems and transfer data more effectively. For OT systems, connecting legacy systems that had not previously been exposed to the enterprise network exposes new risk.

### OT Data Generated From Supporting Critical Processes

-  Production Data
-  Production Quality Assurance
-  Inventory
-  Supply Chain
-  Maintenance Planning

### Enterprise Resource Planning (ERP) Data

-  Sales
-  CRM
-  Purchasing
-  Financials
-  Human Resources

OT Site Data

ERP

Save Money  
Increase Efficiency



**Impact:** This connectivity and move to commodity hardware and software, viewed more urgently after several OT related incidents around the world, has **acted as a driver for increased security in the OT space**. Many organizations are viewing this challenge as an opportunity to align Operations, IT, and Information Security in order to increase the security posture of the OT environment and reduce risk to the organization.

# What major OT security issues do companies face today?

Due to the sensitive nature of OT systems, stringent uptime requirements, and with a decades-long system lifecycle, OT systems pose a significantly different security challenge than traditional IT systems.

## Driving Security in Unregulated Industries

- Unregulated industries have not been compelled to secure operational systems, leading to a lack of security controls across many industries and sectors.
- Corporate boards are increasingly cautious of providing funding, initial or follow up, for expensive remediation without quantifiable metrics to measure risk reduction.

## OT System Vendor Coordination

- Vendors of OT systems maintain control of the configuration and maintenance of systems.
- Vendors dictate approved architecture, software, and patches. Vendors can prohibit AV on endpoints and cause lengthy delays in patching.
- Existing vendor contracts may not require timely remediation of vulnerabilities, patches, etc. leading to increased risk exposure.

## Decades of Technology Debt

- Organizations have often grown or shrank through decades of mergers, acquisitions, and divestitures. This leads to disparate systems and architectures across the same organization.
- OT systems have traditionally been seen as static, and not been updated. Many systems may no longer be updated/patched by the vendor.

## OT Security Program Governance

- IT and OT resources have not historically been required to collaborate on the deployment and ongoing 'run' activities of security.
- Extending traditional IT security capabilities and controls to OT environments requires careful coordination to limit risk of unexpected downtime, and to effectively realize value in terms of risk reduction.

## Lack of Workforce/Resources

- Few resources exist with a background including Operations, IT, Security, and Risk Management.
- Many companies are looking to assess and remediate entire fleets of sites, requiring a large number of resources, sometimes across the world.
- Successful OT security initiatives require coordination of cross functional teams of subject matter specialists from a variety of domains and often involve internal and external resources.

## Business Implications of an OT Cyber Attack

- Remediation costs for sizeable organizations can easily fall in the tens of millions of dollars.
- The impact of a widespread cyber attack on a company's OT environment could **halt production and revenue generation**, thus compounding the the expense of responding to and remediating the incident.



# What are the trends in OT?

As companies continue their digital transformations and further blur the lines between their IT and OT systems they need to be prepared to defend their networks against emerging threats.

## Attacks Impacting Both IT & OT

Most cyber attacks impacting OT environments also impact IT environments, resulting in incidents that require both groups to collaborate and respond, however 61% of companies report they have no cross training between the two.



## IT/OT Convergence

As OT transitions from highly specialized hardware & software to more traditional IT technology stacks there are opportunities for cost savings, increased visibility, and improving security, yet 24% of companies say their IT & OT departments have little to no interaction.



## Increased Intensity of Attacks

Cyber attacks targeting OT assets have increased in both volume and sophistication. While past attacks focused on data gathering, modern attacks are capable of not only operational disruption, but can even cause physical damage.



## Evolving Defences

The growing need to protect OT assets has led to investment from the private and public sectors to build new defences in the form of new trainings, methodologies, and tools.

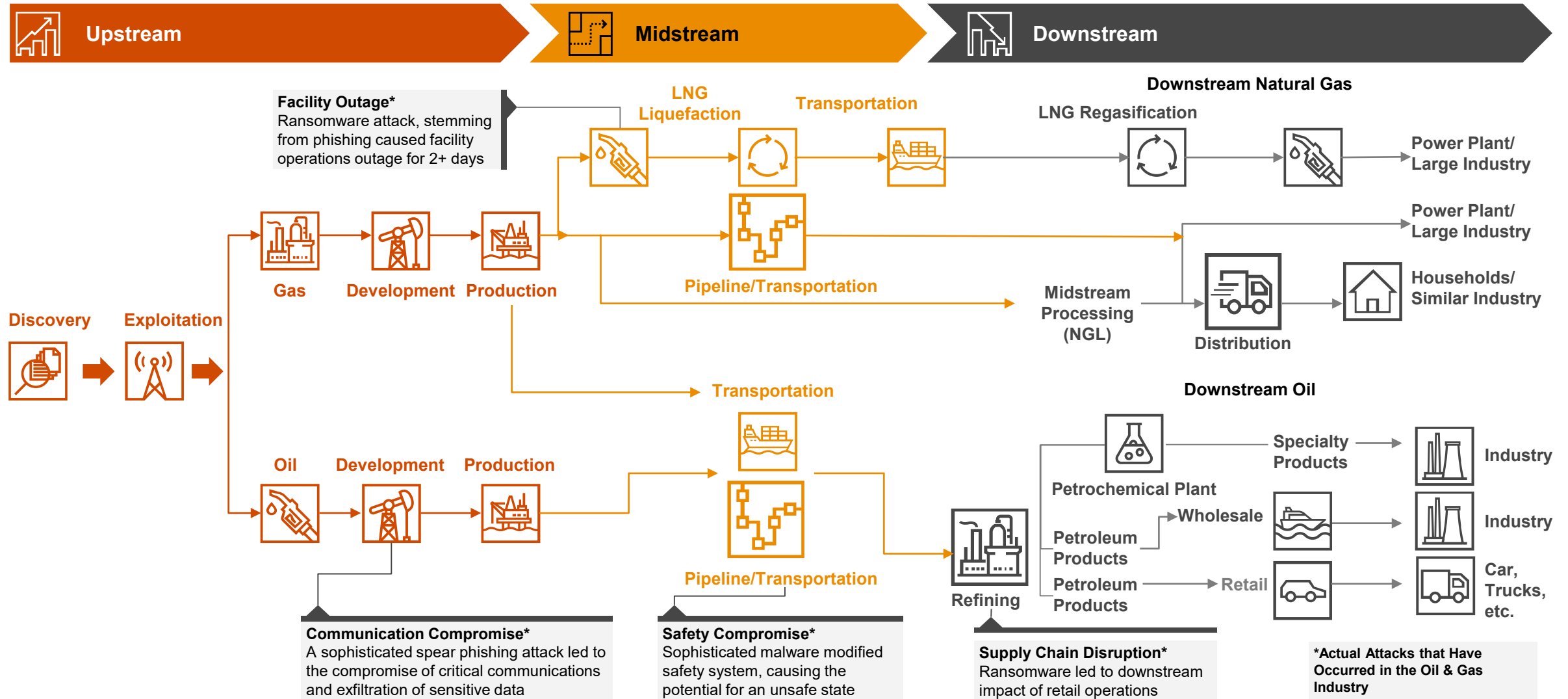


## Focus on Risk Management

Regulated & unregulated industries alike are putting a renewed effort into improving cyber risk management to help drive change & prioritize limited resources. Additionally, new approaches are taking a more holistic approach to consequence reduction to help reduce risk.



# Example value chain – Oil & gas – What’s at risk?

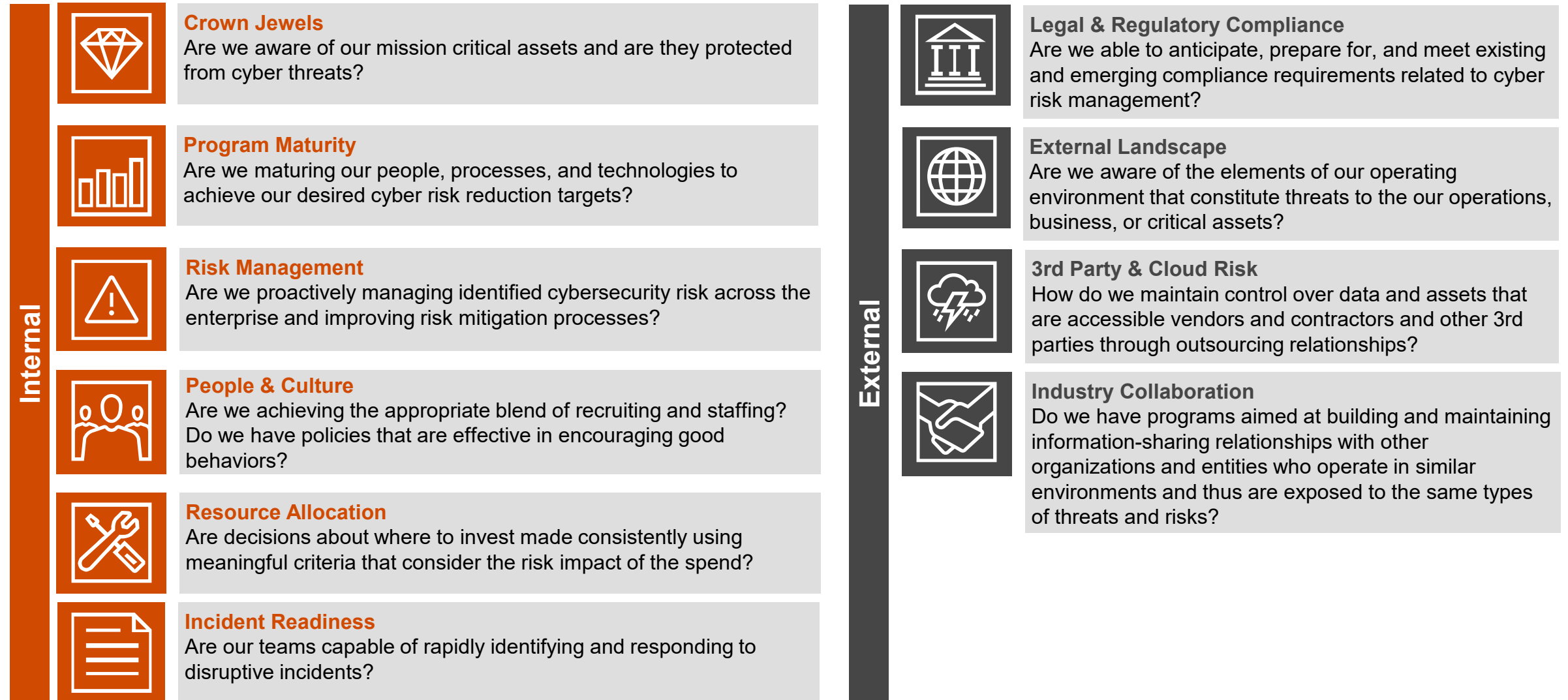


# Cybersecurity in critical infrastructure – Board level issue



# 10 strategic lenses for board & executive reporting

Lenses provide answers to a key question about strategy and risk, each supported by multiple data points.



# Cyber resilience & supplier cyber security in critical infrastructure

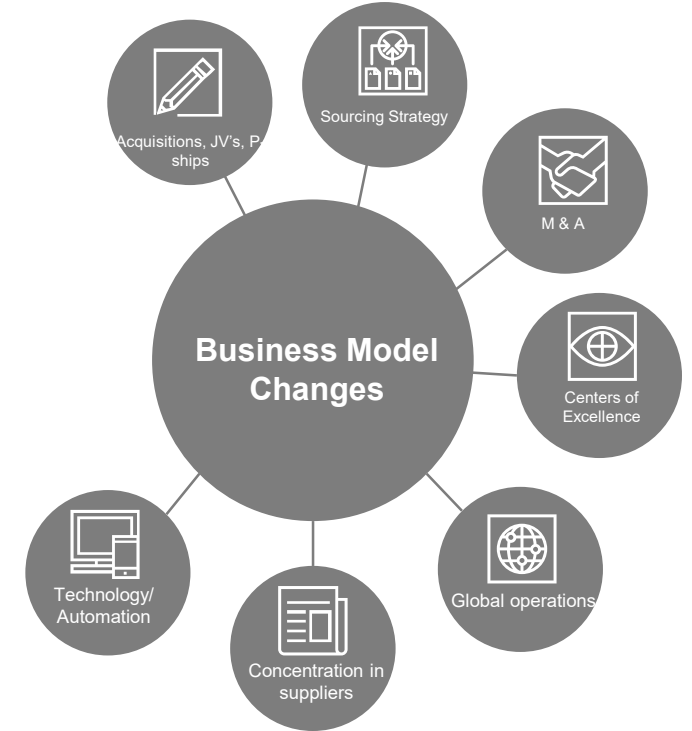
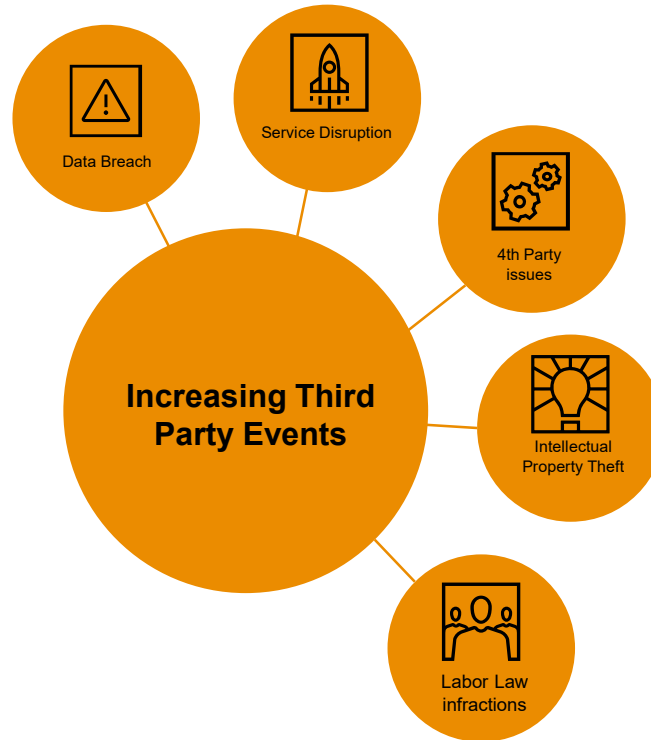


# Improving and sustaining third party risk management is essential amid raising regulatory and client expectations



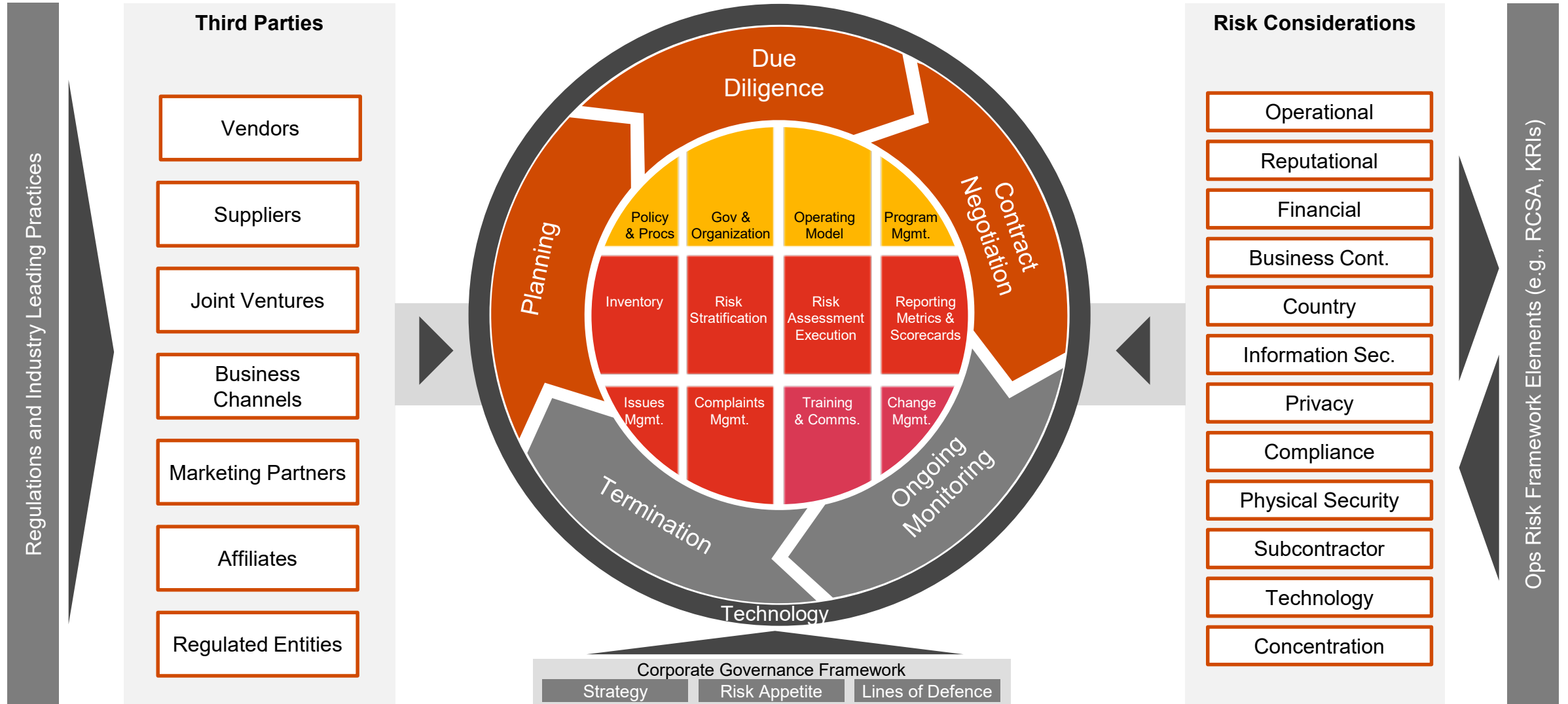
**Regulatory guidance related to Third Party Risk Management (TPRM)** continues to evolve and expand, requiring a strategic approach and framework to maintain compliance.

**Increased Third Party events and incidents** lead to customer churn, regulatory penalties and fines, and reputational impact, requiring enhanced due diligence and ongoing monitoring for potential vulnerabilities.



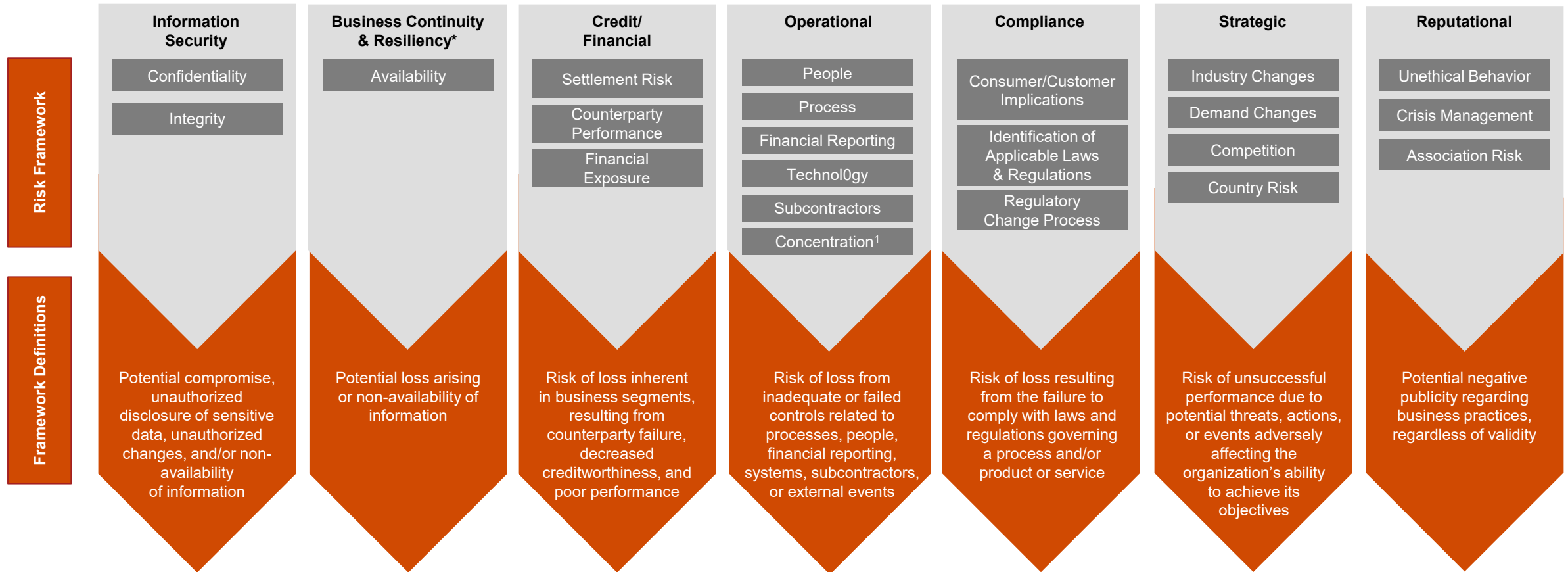
**Changes in business strategies and operating models** lead to new types of Third Party arrangements and exposures to risk, requiring organizations to carefully consider the risks prior to execution.

# A holistic TPRM Framework facilitates a consistent approach to identification, mitigation, and management of Third Party risks



# Significant enterprise risk dimensions impacting Third Party Risk Management

Presented below are significant enterprise risk dimensions that must be identified and managed throughout the TPRM lifecycle.



\*Business Continuity Management includes Business Contingency ("BC") planning and Disaster Recovery ("DR")

<sup>1</sup>Assess the risks associated with third parties/subcontractors having too many services, too many services being performed in a single location, or a third party/subcontractor being over reliant on a single client.



# The following presents current trends in the Third Party Risk Management landscape



Regulators across the globe are introducing **new regulations and increasing expectations**.



**Globalization and digital transformation** have created integrated, digitally connected, and borderless third party marketplaces.



Multiple organizations are relying on the same third parties in and across industries increasing **concentration risk concern**.



Enterprises are looking for enhanced partnership and **integration between the Risk and Procurement organizations** to balance risk/value.



Traditional third party assessment processes are good but reflect a **point in time and are difficult to scale**.



Ensuring third parties are complying with **rapidly changing regulations** is a key concern of executives.



Organizations are increasingly using **risk data, predictive modeling, statistics and visualization** to generate insights that help make better decisions.



Regulators have increased **focus on fourth, fifth and nth party risk** and how organizations are managing risk throughout their supply chain.



As the TPRM industry follows the accelerating digital wave, manual processes and spreadsheets will give way to **automation and analytics**.

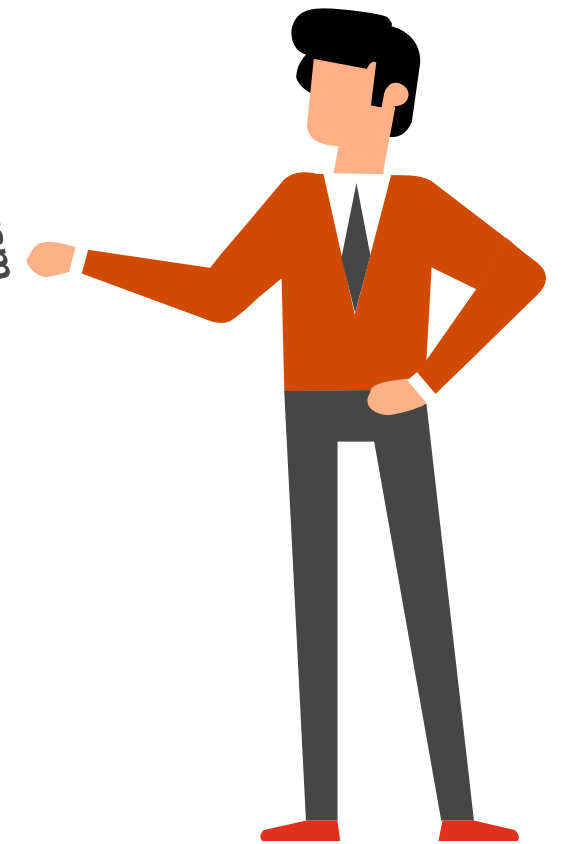


**Consortiums and alliances** are providing third party risk management capabilities that multiple participating organizations can leverage.

# Operating components of a leading edge third party **security** risk management program

Operating components define how the TPRM program will operate while taking into account regulatory guidance and industry leading practices, while maintaining alignment with the organizations' operational risk tolerances

A strong third party security risk management program contains **three** core components: **program management**, **risk assessment**, and **intelligence-led monitoring**. Each of these components contains **four capabilities**, totalling the 12 core capabilities that make up a **security-focused** third-party risk management program.

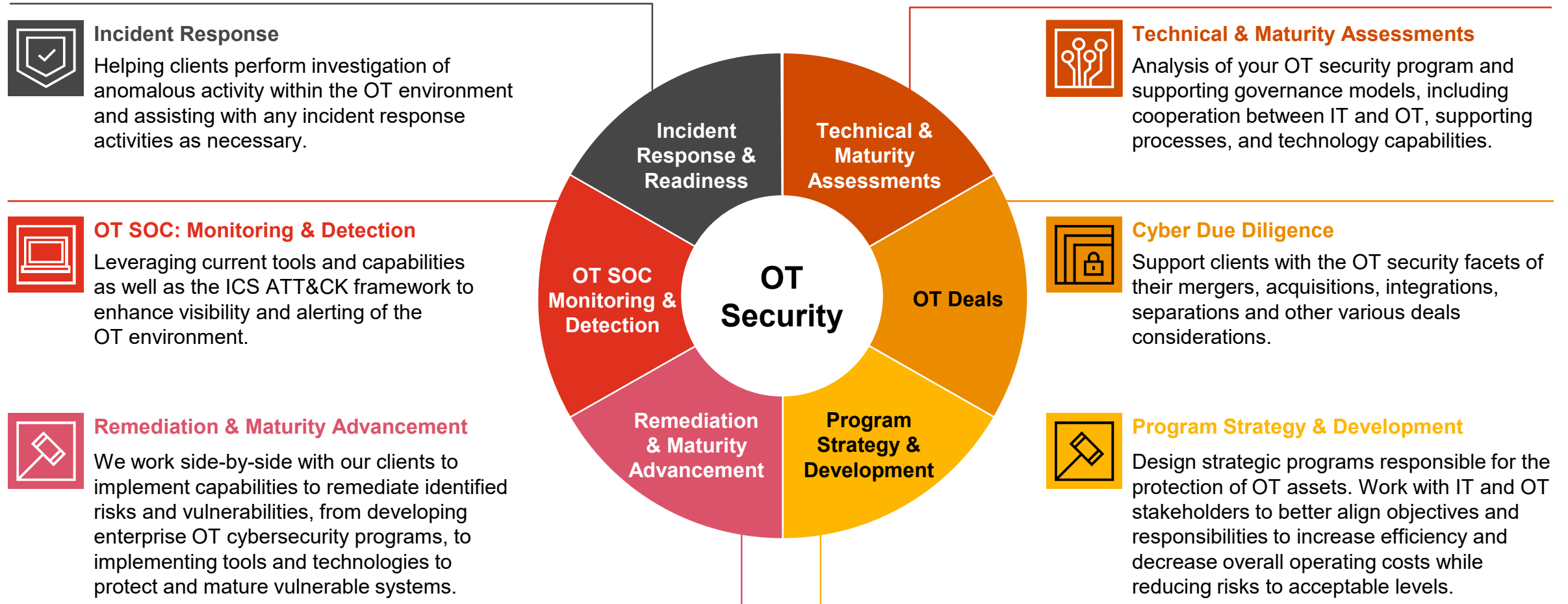


# Taking action

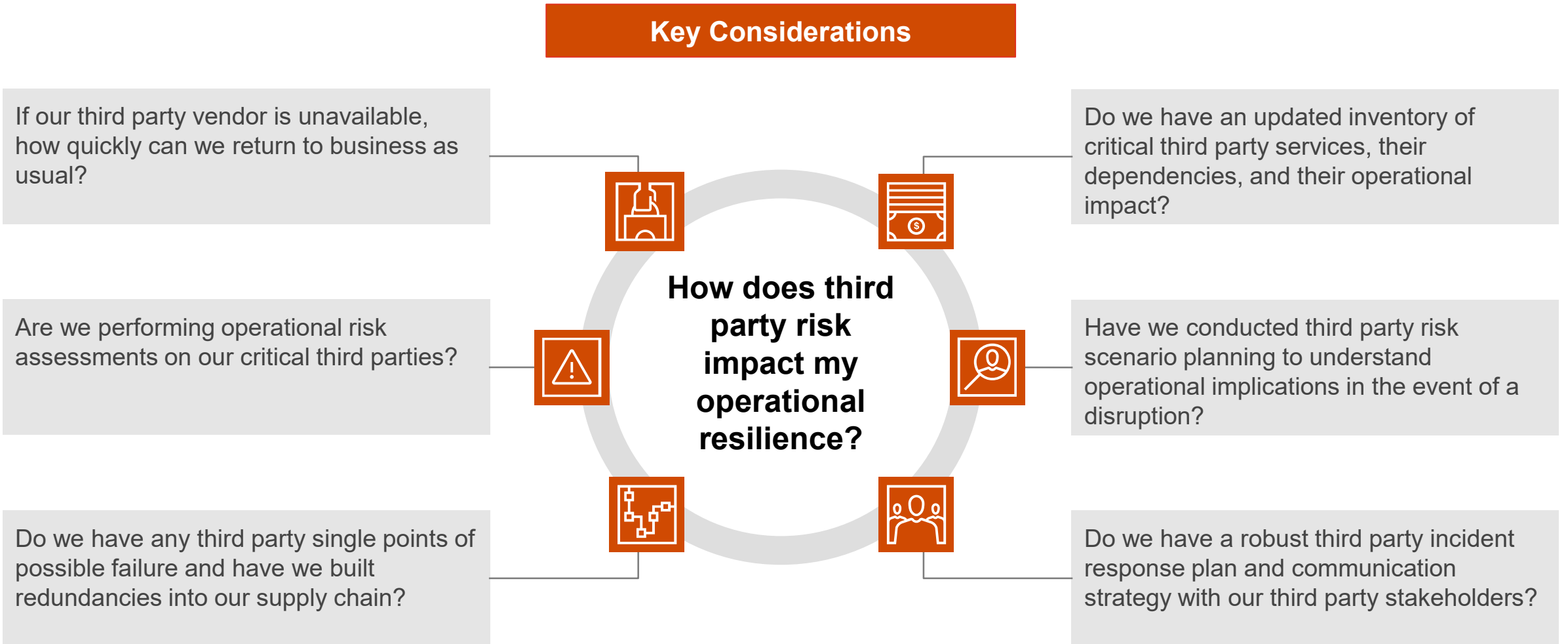


# OT security – Holistic Approach

**Organizations must adopt a proactive security posture** in order to programmatically manage cybersecurity risk to operational systems. PwC Cybersecurity and Privacy offers a variety of services to enable integrated IT and OT security programs and reduce risk to organizations.



# Third party risk management and operational resilience



# How can I enhance my third party resilience?

01

## **Evaluate Your Overall Operational Resilience**

Understand the resilience posture of your workforce, technology, infrastructure, operations, and incident response capabilities that may also be needed to withstand third party disruptions.

02

## **Improve Third Party Visibility**

Identify and maintain an updated inventory of third parties and services that are critical to your day to day operations.

03

## **Understand your Mission Critical Dependencies**

Identify mission critical processes, systems, resources, and underlying dependencies to help understand risks that drive continuity strategies.

04

## **Assess Third Party Risk and Impact to your Business**

Perform operational third party risk assessments and conduct scenario planning exercises to help understand operational implications and mitigation strategies.

05

## **Develop and Test Crisis Management Plans**

Prepare crisis management plans and conduct testing to enhance your readiness to respond and withstand a potential major third party disruption.



# Thank you

[pwc.com](https://www.pwc.com)

© 2020 PwC. All rights reserved. PwC refers to the US member firm or one of its subsidiaries or affiliates, and may sometimes refer to the PwC network. Each member firm is a separate legal entity. Please see [www.pwc.com/structure](https://www.pwc.com/structure) for further details.