



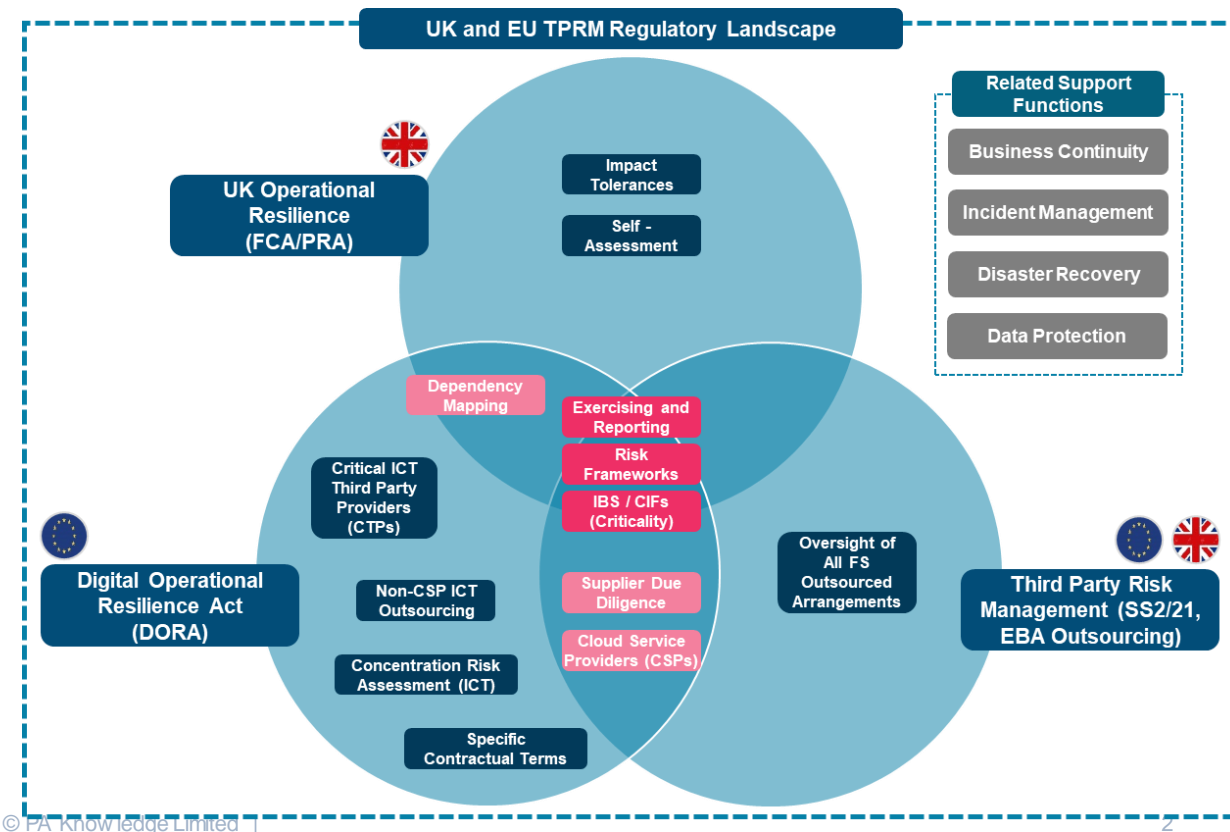
Themes across resilience regulation

Using the Digital Operational Resilience Act
as a blueprint



Bringing Ingenuity to Life.
paconsulting.com

Regulatory Background

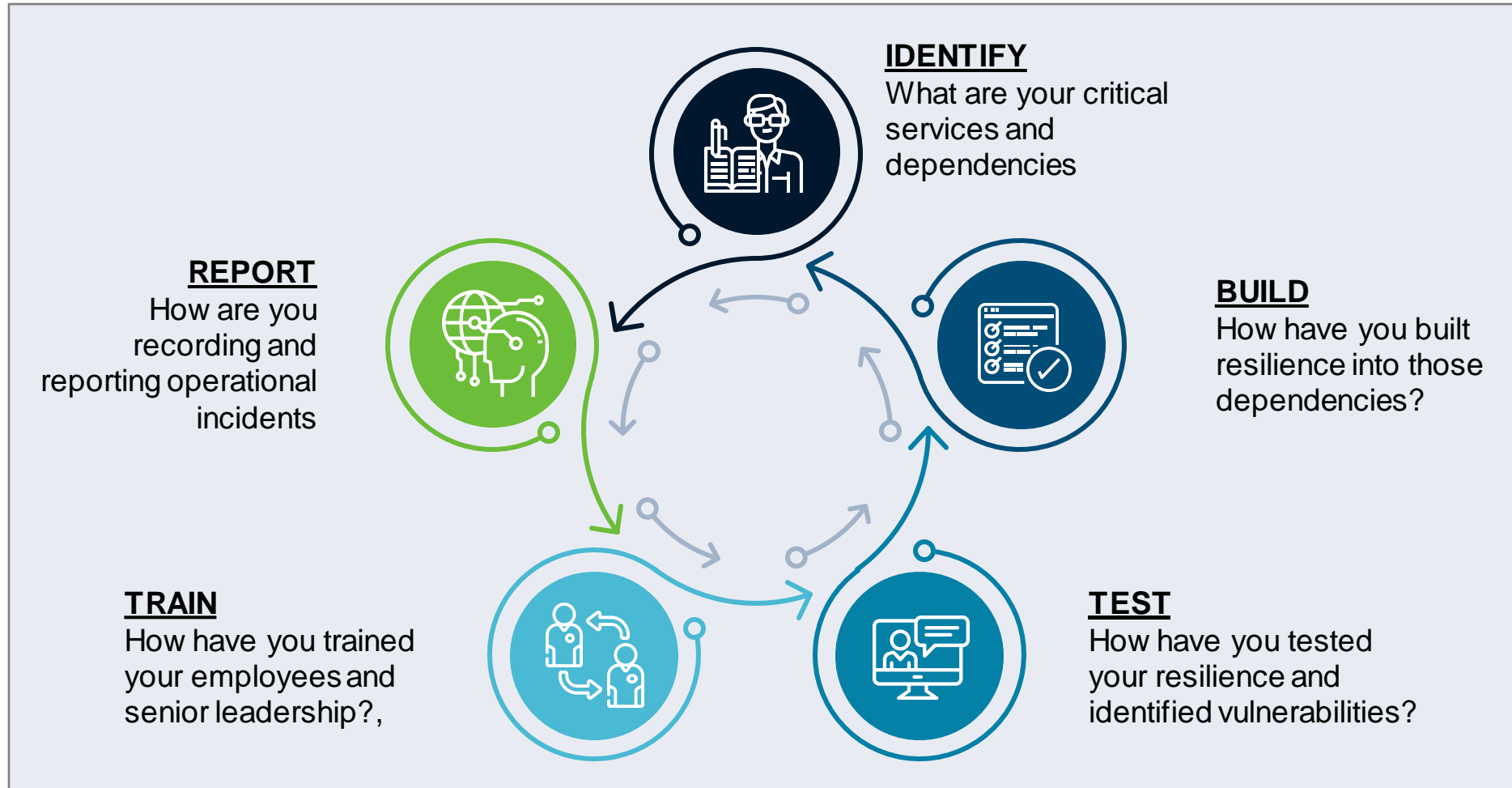
The Digital Operational Resilience Act (DORA) and existing regulatory guidance around Operational Resilience and Third-Party Risk Management all have similarities, as they focus on ensuring the stability, security, and continuity of financial services. These regulatory frameworks share common objectives related to resilience, risk management, customer protection, and testing and exercising. However, they differ in their specific focus areas and the types of entities they regulate. Where Operational Resilience focuses on ensuring service continuity, DORA addresses digital service providers' Operational Resilience in the context of digital services.



Global Regulatory Developments

- 
 Monetary Authority of Singapore (MAS) (August 2022: **Operational Risk Management – Management of Third-Party Arrangements**)
 - No significant change to the existing requirements under the MAS Guidelines on Outsourcing.
 - Additional guidance on enhancing concentration risk analysis, TPRM technology and implementation of the 3LoD model.
- 
 June 2023: **US Interagency Guidance for Third Party Relationships (Risk Management)**.
 - Largely aligned with initial Proposed Guidance from 2021.
 - Key changes include reference to maintaining a complete inventory of all third-party relationships and an expansion of the scope, that now covers FinTechs which interact directly with customers.

Identifying your key dependencies – how to define **critical**

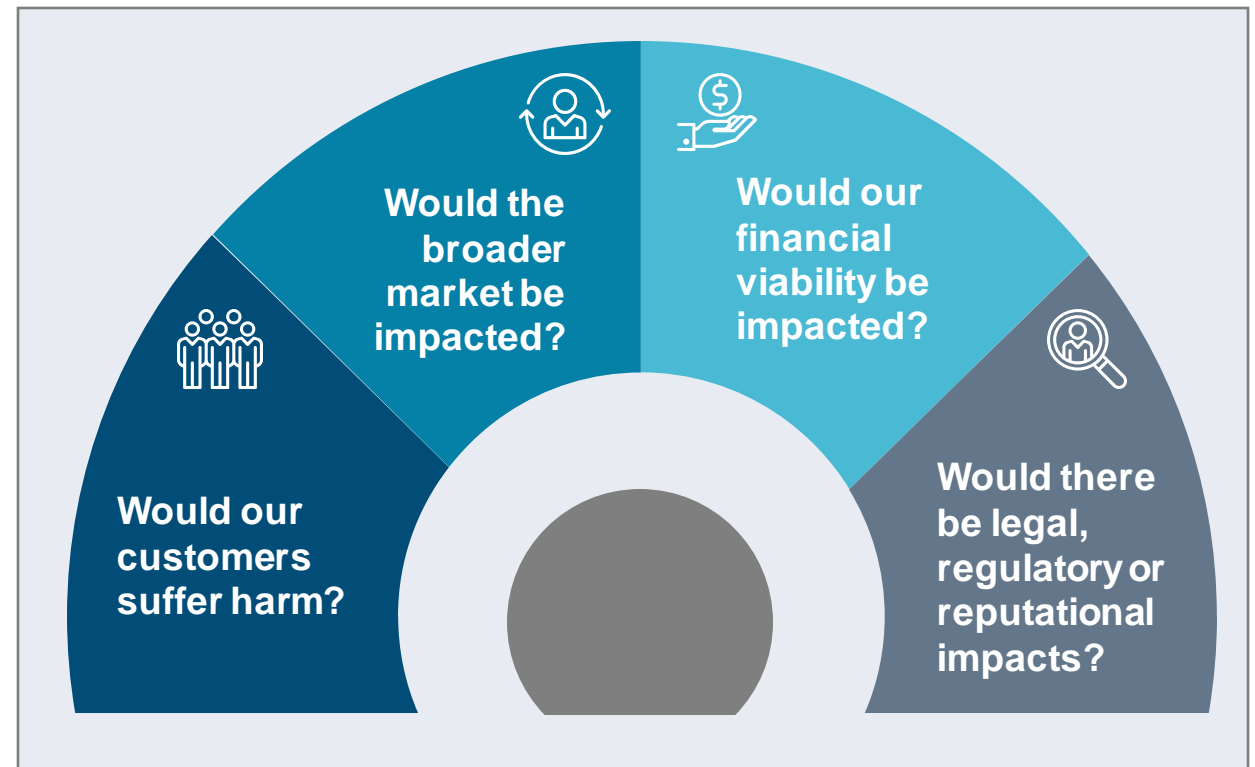


Identifying your key services – how to define critical

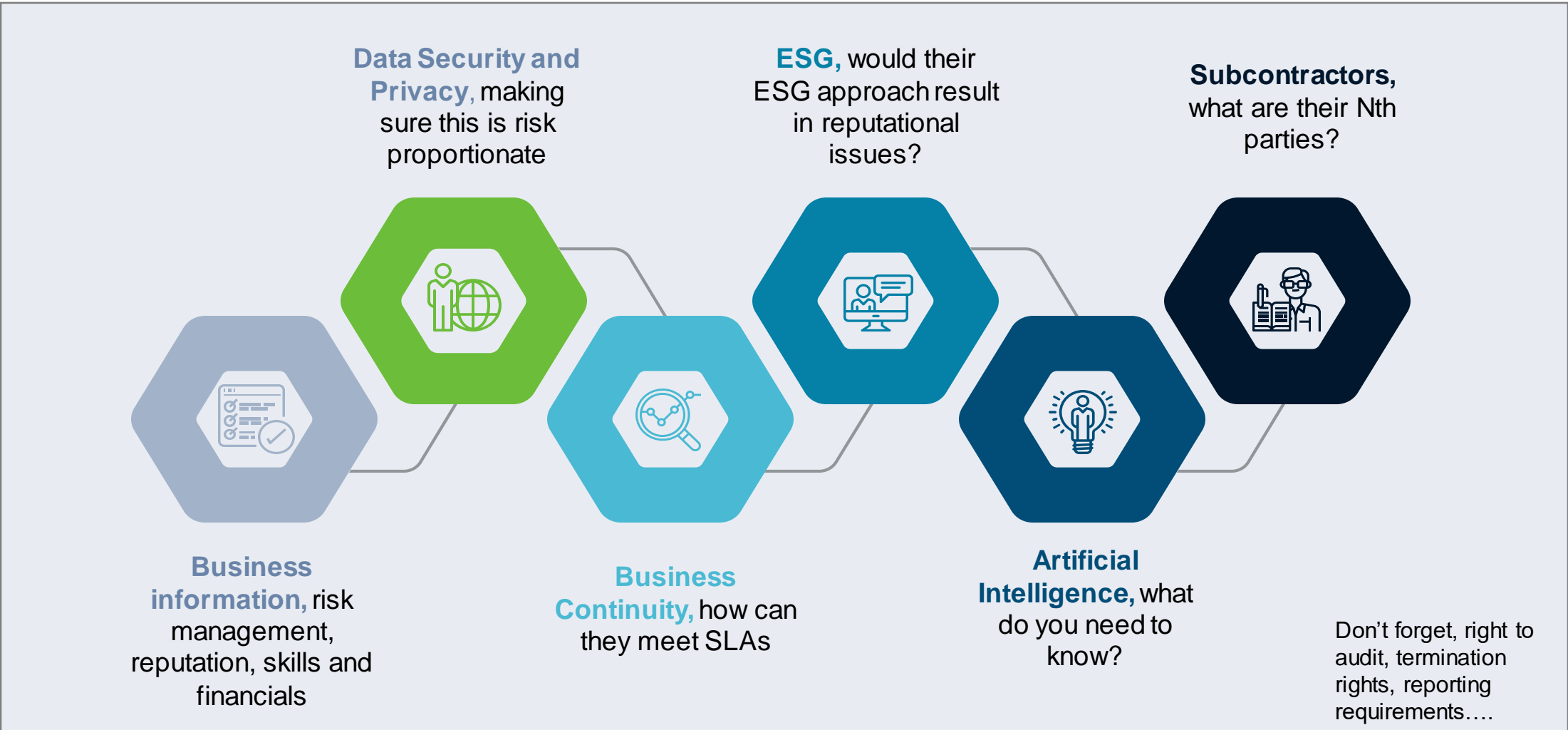
There are slightly deviating definitions of critical or important across the current regulatory landscape.

However, at the highest-level firms should use their existing Business Impact Assessments and resilience documentation to determine the following

If the service was disrupted....

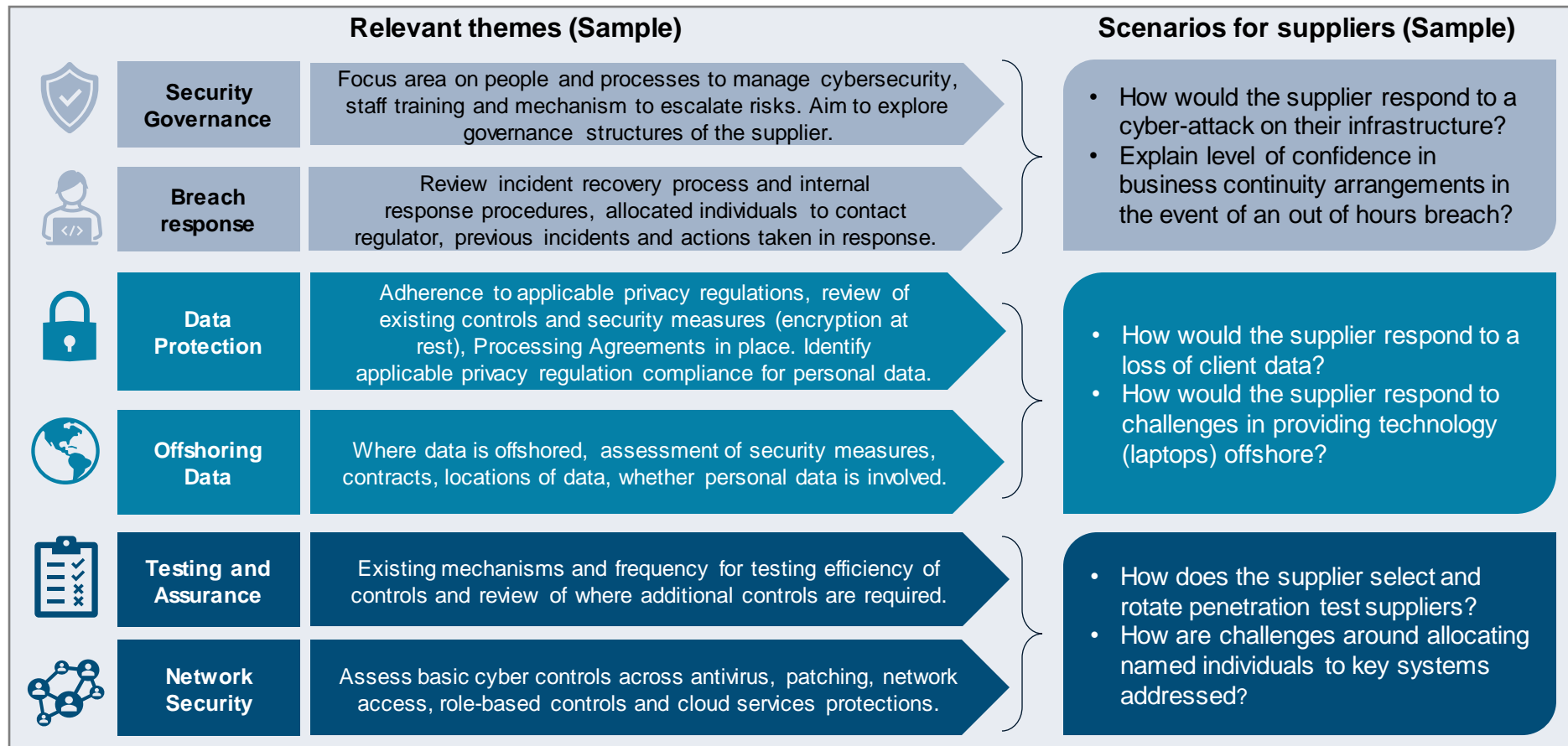


Building in resilience at the off-set: Due Diligence



Testing to identify vulnerabilities

Scenarios are driven by **themes** that are aligned to the service(s) being provided. Suppliers are asked to **provide details of how they would respond to the scenario(s)**. This provides **practical insights** into the **suppliers' preparedness** and their **ability to respond to disruption**.








Recording and Reporting incidents

Reporting to the regulators is not a new concept in Financial Services, however the pre-defined reports may require firms to carry out a feasibility assessment on their ability to report.

More broadly SEC 8K requirements also place more pressure on firms to report

Making an assessment of Root Cause:

 <p>Malicious Actions</p> <ul style="list-style-type: none"> • Deliberate internal actions • Deliberate physical damage or theft • Fraudulent actions • Cyber security 	 <p>System failure malfunction</p> <ul style="list-style-type: none"> • Hardware capacity & performance • Hardware maintenance • Hardware obsolescence • Software compatibility/configuration • Software performance • Network configuration 	 <p>Process Failure</p> <ul style="list-style-type: none"> • Insufficient/failure of monitoring & control • Insufficient roles & responsibilities • ICT risk management process failure • Insufficient/failure of ICT operations • Insufficient/failure of ICT project management • Inadequate internal policies • Inadequate ICT Systems Acquisition, Development, and Maintenance
 <p>Human Error</p> <ul style="list-style-type: none"> • Omission • Mistake • Skills & knowledge • Inadequate resources • Miscommunication 	 <p>External event</p> <ul style="list-style-type: none"> • Natural Disaster • Third party failure 	

Within 4 hours



Firms will report via a templated form that includes mandatory fields.



Initial Report: Information on impact to other entities, how the incident was discovered, BCP activation.



Intermediate Report: Information about affected business areas, infrastructure components, communications, temporary actions taken, CVE/loC details.

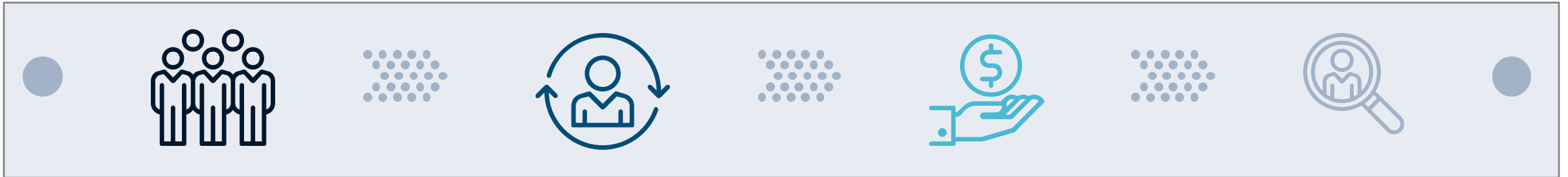


Final Report: Information on root cause, breach of SLAs or contractual agreements, information about measures taken for remediation and recovery, lessons learnt, information on direct and indirect costs and losses due to the incident

Within 72 hours

Within 1 month

Training your accountable people



Firm wide culture

Embedding resilience principles similar to security and privacy to build a resilient culture

Across the business, individuals need to report security issues, privacy gaps and take ownership for building resilience by design

Senior Leadership

Many regulations focus on senior accountability, and resilience being set from the top

Making resilience a key part of business strategy and seen as an enabler not a compliance hindrance

Tailored training

Many first line roles have day to day responsibility for building firm resilience

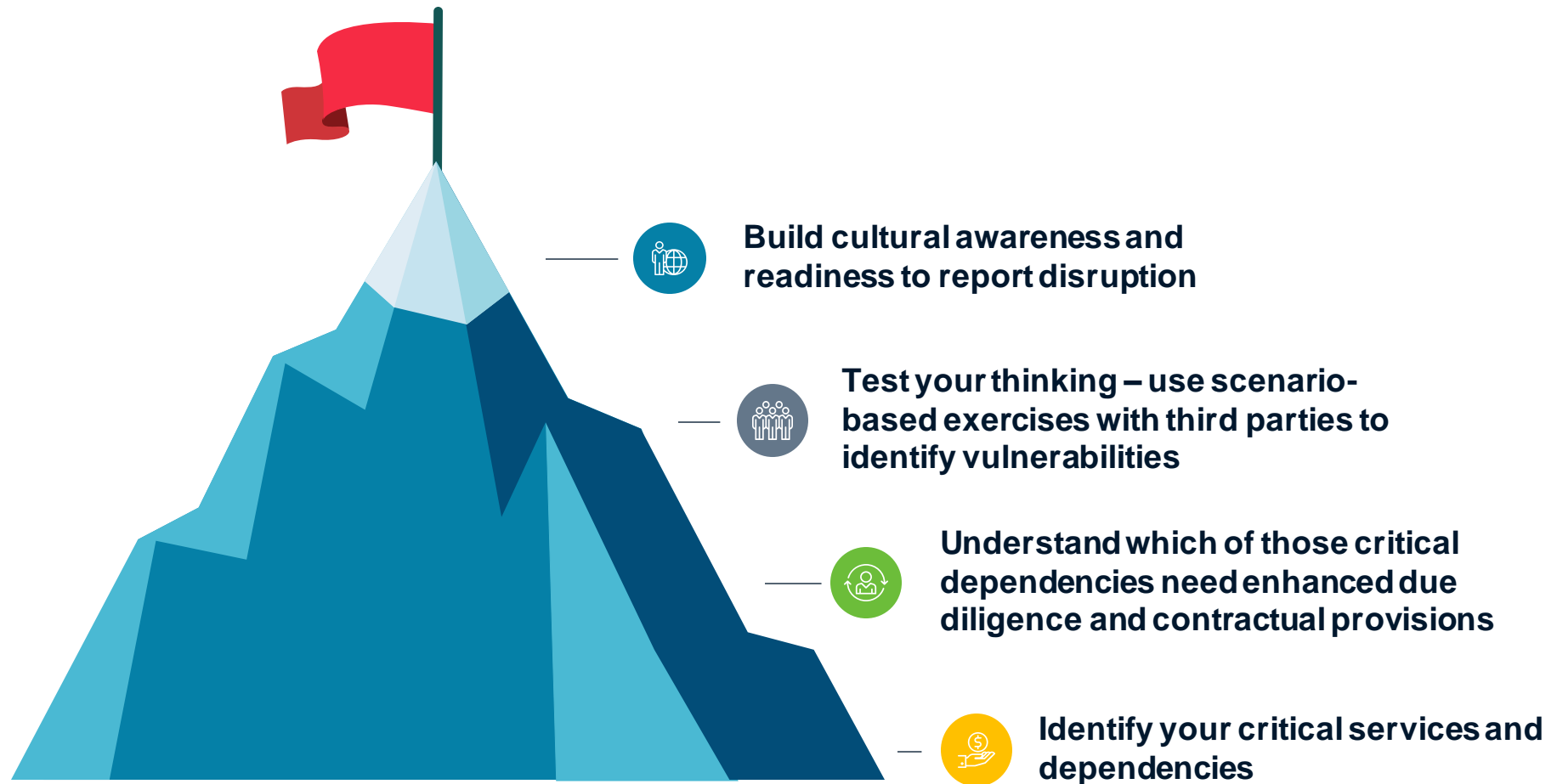
Vendor managers for example need to understand the importance third parties play to the overall success of the business

Lessons Learnt

Post incident or exercise, sharing lessons learnt supports building cultural awareness.

This could be through a community of practice or town hall, where themes are shared

Steps to take to align with resilience



**Bringing
Ingenuity
to Life.**



New York Office

PA Consulting Group Inc.
45th Floor
The Chrysler Building
405 Lexington Avenue
New York
NY 10174
USA
+1 212 973 5900

About PA.

We believe in the power of ingenuity to build a positive human future.

As strategies, technologies, and innovation collide, we create opportunity from complexity.

Our diverse teams of experts combine innovative thinking and breakthrough technologies to progress further, faster. Our clients adapt and transform, and together we achieve enduring results.

We are over 4,000 strategists, innovators, designers, consultants, digital experts, scientists, engineers, and technologists. And we have deep expertise in consumer and manufacturing, defense and security, energy and utilities, financial services, government and public services, health and life sciences, and transport.

Our teams operate globally from offices across the US, UK, Ireland, Nordics, and Netherlands.

PA. Bringing Ingenuity to Life.

Discover more at paconsulting.com and connect with PA on [LinkedIn](#) and [Twitter](#)

This document has been prepared by PA Consulting Group. The contents of this document do not constitute any form of commitment or recommendation on the part of PA and speaks as at the date of publication.

paconsulting.com

All rights reserved © PA Knowledge Limited 2024

No part of this documentation may be reproduced, stored in a retrieval system or transmitted in any form or by any means, electronic, mechanical or otherwise, without the prior written permission of PA Consulting Group.