
How can you improve your ability to identify, respond and adapt to significant operational interruptions?
EY
Building a better working world

Agenda

I	**Introductions and objectives**
II	Why is resilience important
III	Typical issues — be aware
IV	What do you need to do
V	Summary and questions

Introductions and objectives

Ali Kazmi

Executive Director — IT Risk Transformation

John Milne

Director — IT Risk Transformation

James Turpie

Senior Manager — IT Risk Transformation

Objectives for this session

- To understand why resilience is important
- To understand common challenges amongst building societies, mutuals and the wider FS sector
- To explore the path towards operational and cyber resilience

Please feel free to ask questions throughout this session

Defining resilience

- Operational Risk is defined in Basel II as the 'risk of loss resulting from inadequate or failed internal processes, people and systems or from external events'.
- Operational Risk functions are tasked with identifying, measuring and assessing these operational risks.

- Operational Resilience is the organisation's set of people, processes and technology marshalled to reduce operational risks down to an acceptable level and react effectively when they do crystallise.

Polling question 1

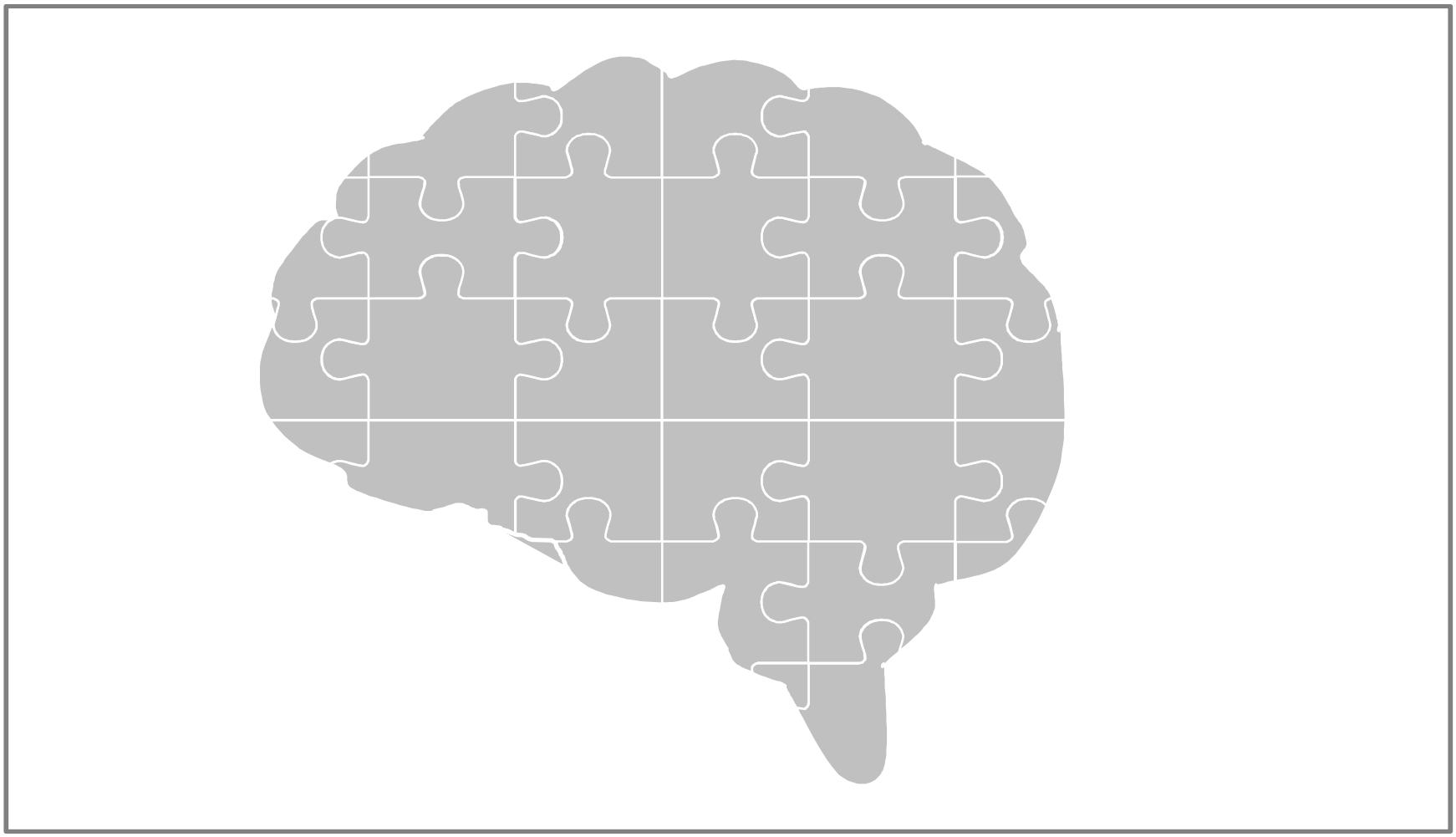
How aware of resilience are you?

We regularly read about service disruptions and cyber attacks which bring down critical services. Taking proactive preventative action now can reduce the risk of disruption.

Polling question: How hot a topic is resilience within your organisation?

- **What is resilience?**
- **Resilience is occasionally discussed.**
- **We have an active resilience programme.**
- **Resilience is discussed at senior management and board levels on a regular basis.**

Resilience is in the mind of the consumer



How can you improve your ability to identify, respond and adapt to significant operational interruptions?

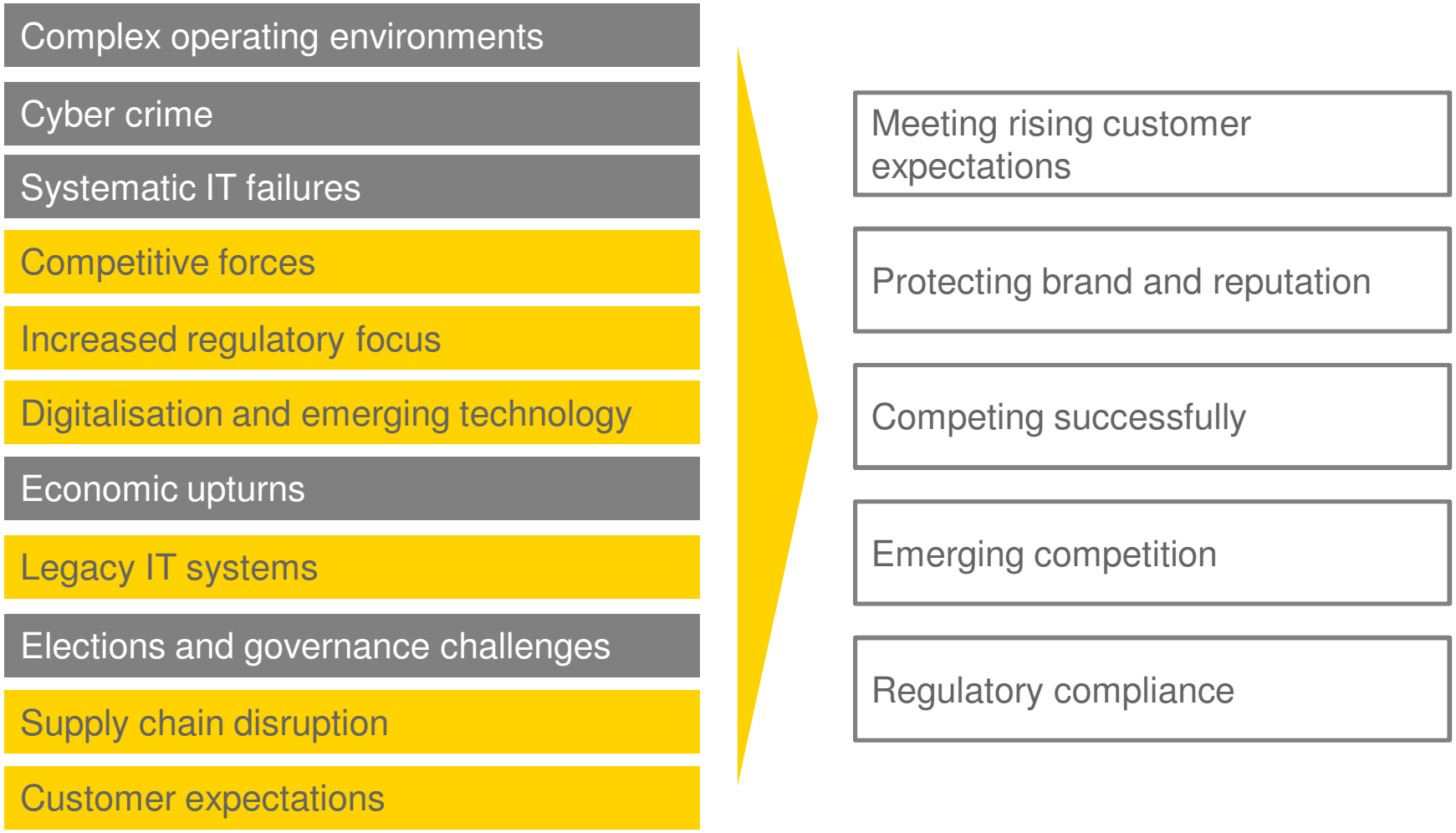
Media headlines

- **There are many famous and infamous examples of when systems outages and cyber attacks affect customers and hit the headlines.**

Agenda

I	Introductions and objectives
II	**Why is resilience important**
III	Typical issues — be aware
IV	What do you need to do
V	Summary and questions

Why does resilience matter to you?



How can you improve your ability to identify, respond and adapt to significant operational interruptions?

The regulatory dimension

Main regulatory drivers

- High profile operational events and follow-up
- Prevalence of legacy IT systems
- Emergence of cyber attack as an increasing threat
- Progress on financial resilience Recovery and Resolution Planning ("Living Wills")
- More aggressive regulatory culture ("prove it to me")

Main regulatory tools

- Forensic testing (CBEST)
- More "deep dives"
- Wider use of skilled persons reports (s166)
- Improved operational data - benchmarking
- Regular collective exercises
- Non-binding Guidance/Dear CEO
- SMR

Main regulatory focus

- Governance - resilience is a Board issue
- Critical Economic Functions – identifying "crown jewels"
- Risk Appetite - clear statement of tolerance for loss of key business capabilities against a wider range of criteria
- Accountability – individual responsibilities should be clearly defined and set against an unambiguous chain of command
- 3 Lines of Defence – each line should be independent and be equipped to provide effective challenge
- Resilience culture – continuous improvement not "fix on fail"
- Resilient behaviours – effective and proactive training and awareness

Industry response

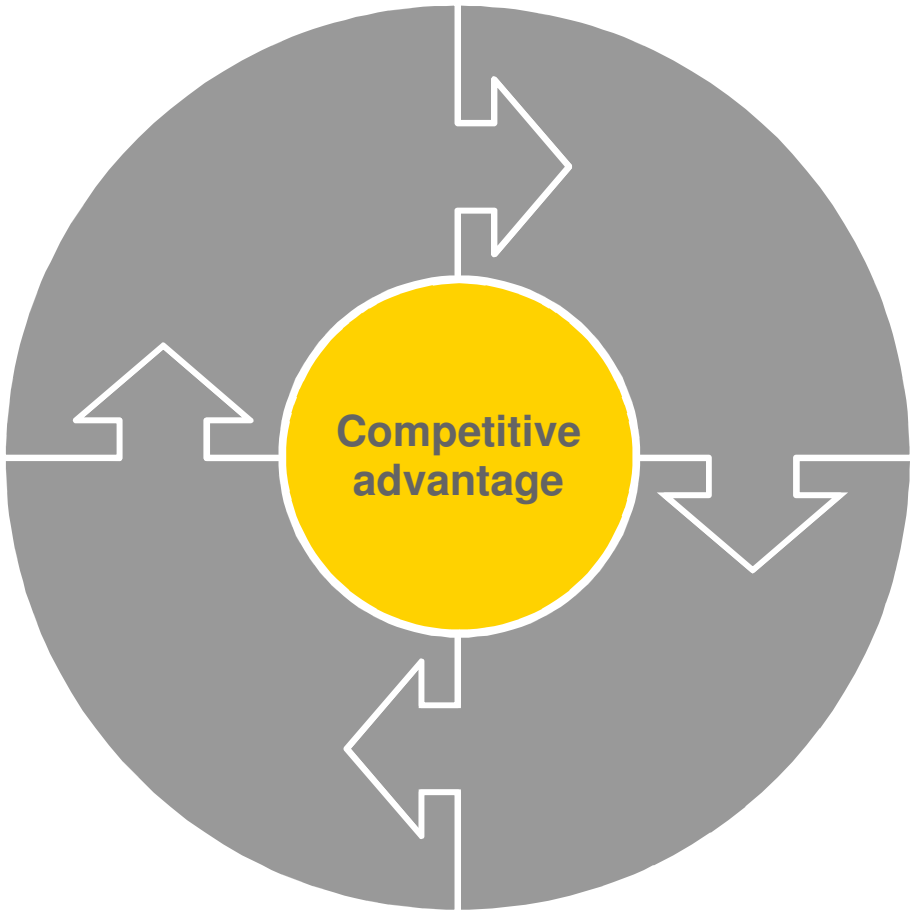
- Recognition that resilience is a mainstream risk
- Increasing application of traditional risk-management techniques
- Increasing senior management engagement and oversight up to and including Board
- Better articulation of Risk Appetite against not just quantitative but also qualitative criteria
- Clearer definition of roles and responsibilities (SMR)
- More disciplined application of 3 Lines of Defence
- Improved and more regular MI
- Increased investment in training to promote resilient behaviours
- Promoting a resilience culture
- Enhanced testing/simulation

How can you improve your ability to identify, respond and adapt to significant operational interruptions?

Advantages held by resilient organisations

Confidence

Coherence



Competition

Agility

How can you improve your ability to identify, respond and adapt to significant operational interruptions?

Agenda

I	Introductions and objectives
II	Why is resilience important
III	**Typical issues — be aware**
IV	What do you need to do
V	Summary and questions

Polling question 2

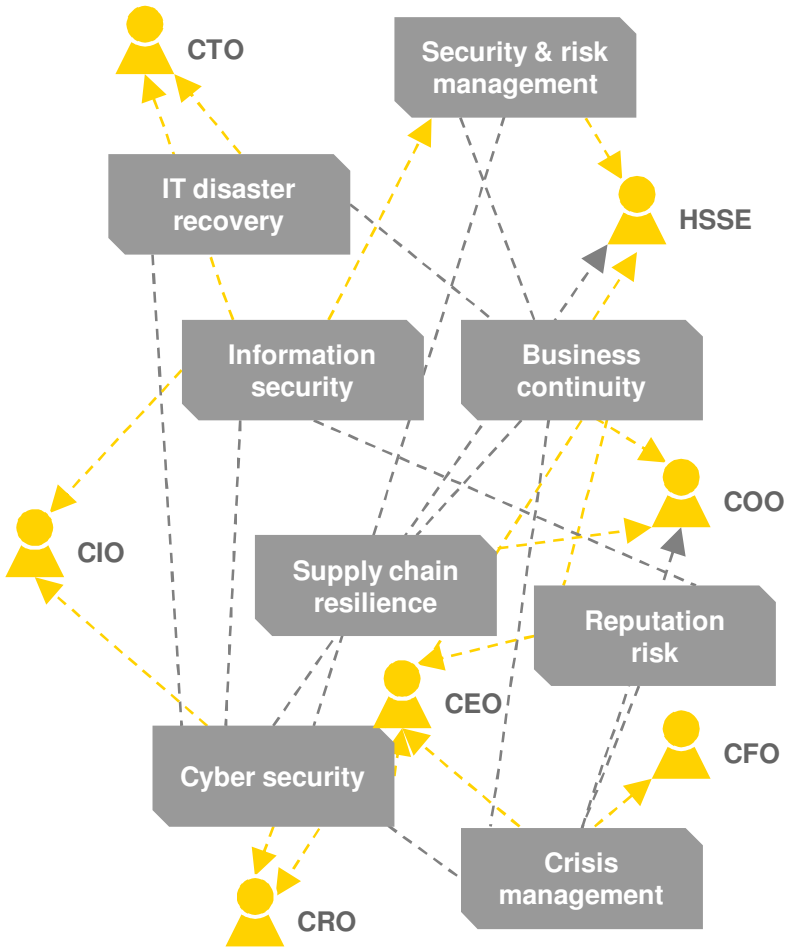
The ownership challenge

Polling Question: Who is ultimately responsible for resilience within your organisation?

- **Chief Executive Officer**
- **Chief Risk Officer**
- **Chief Information Officer**
- **Chief Operating Officer**
- **Head of Risk**
- **Board**
- **Chief Resilience Officer / Head of Resilience**
- **Other**

Resilience challenges

- Dynamic landscape
- Customer expectations
- Poor leadership
- Limited strategy
- Piecemeal approach
- Organisational change
- Skills gap and resource limitations
- Underinvestment
- Inconsistency of technology
- Inaccessible information
- Cost
- Ineffective controls



How can you improve your ability to identify, respond and adapt to significant operational interruptions?

Agenda

I	Introductions and objectives
II	Why is resilience important
III	Typical issues — be aware
IV	**What do you need to do**
V	Summary and questions

Polling question 3

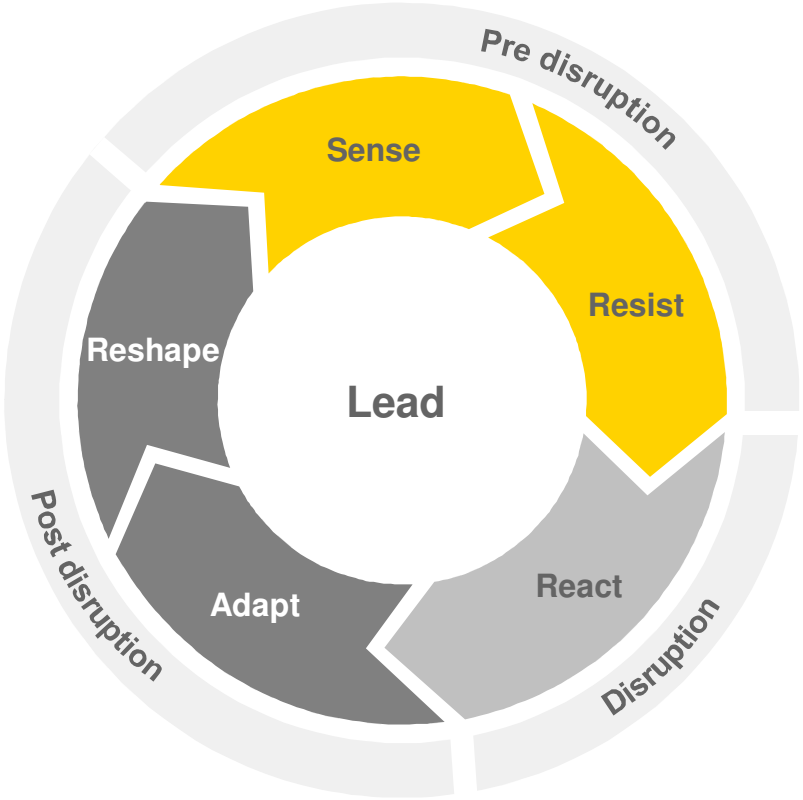
Resilience strategy

Polling Question: Does your organisation have a resilience strategy in place?

- **Yes**
- **No**

Strategic approach to resilience

Sense, **Resist** and **React** to disruptive events, while **Adapting** and **Reshaping** operations in environments characterised by both foreseeable and unforeseeable risk



How can you improve your ability to identify, respond and adapt to significant operational interruptions?

Polling question 4

Testing your readiness

Polling Question A: How often do you test your resilience capabilities?

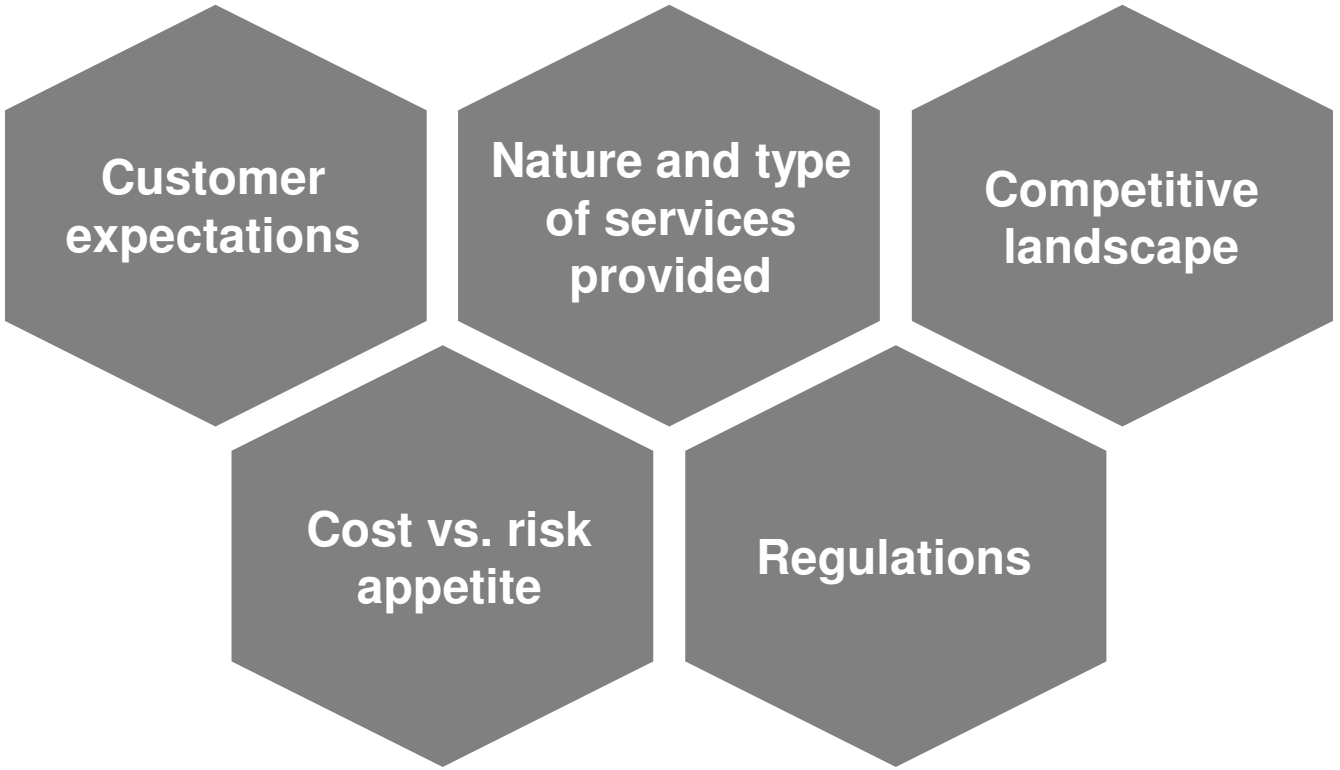
- Monthly
- Bi-annually
- Annually
- Occasionally
- Never

Polling Question B: What is the nature of the testing that you perform?

- Only single functions
- End to end business processes
- Including suppliers
- Cross-industry
- We do not test our resilience capabilities

How much resilience is enough resilience?

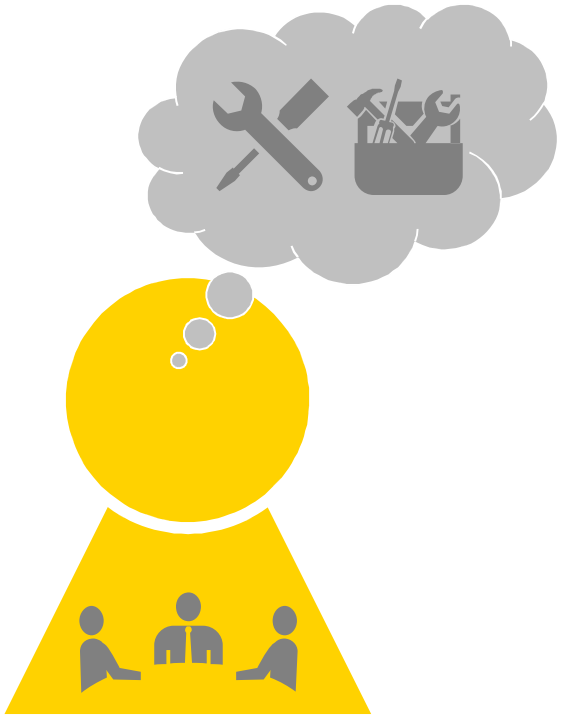
Investment in resilience is informed by a number of factors including:



How can you improve your ability to identify, respond and adapt to significant operational interruptions?

Components of an effective resilience strategy

1. Strategy needs to be dynamic
2. Strategy needs to include key dependencies
3. Have the right governance in place
4. People are key
5. Have a resilient culture



How can you improve your ability to identify, respond and adapt to significant operational interruptions?

Three key steps to reduce risk

How can you improve your ability to identify, respond and adapt to significant operational interruptions?

Agenda

I	Introductions and objectives
II	Why is resilience important
III	Typical issues — be aware
IV	What do you need to do
V	**Summary and questions**

Key take-aways

Readiness

- Do we have the relevant skills and experience on the Board to know if we're doing enough?
- Do the risk committee and Board sufficiently debate the cyber agenda and resilience of the organisation?
- How do we compare to peer organisations?
- Have we exercised our ability to respond to a cyber attack – up to Board level?

Re-shape the agenda and set-up an effective strategy

- Do we know understand our 'crown jewels' that are at greatest risk of cyber attack?
- Have we defined a cyber risk appetite which is meaningful for our organisation?
- Is our cybersecurity strategy aligned with your business objectives? Is cyber security embedded in our digital transformation agenda?

Skills and resources

- Is our cyber security function appropriately organised, trained, equipped, staffed and funded?
- Do we have a cyber security strategy that covers people, processes and technology AND identify, protect, detect, respond and recover aspects ? Is Governance clear and does this cover 3rd parties?

Assurance

- How do we measure the effectiveness of our cyber capabilities?
- How quickly would we know if we were being attacked and if our assets were compromised?

Polling question 5

Wrap-up

Polling Question: Considering everything we have discussed today, how confident are you in the resilience position of your organisation?

- **Not at all confident**
- **Unconfident**
- **Confident**
- **Absolutely confident**
- **Not sure**

Did we meet our objectives … ?

- To understand why resilience is important
- To understand the path to resilience
- To understand common challenges in the market

If you have any questions then please feel free to contact us:

Ali Kazmi — akazmi@uk.ey.com
John Milne — jmilne1@uk.ey.com
James Turpie — jturpie@uk.ey.com

Finally — we would like to request your feedback!

Thank you

How can you improve your ability to identify, respond and adapt to significant operational interruptions?

Important information

Accordingly, Ernst & Young accepts no responsibility for loss arising from any action taken or not taken by anyone using this pack.

The information in this pack will have been supplemented by matters arising from any oral presentation by us, and should be considered in the light of this additional information.

If you require any further information or explanations, or specific advice, please contact us and we will be happy to discuss matters further.