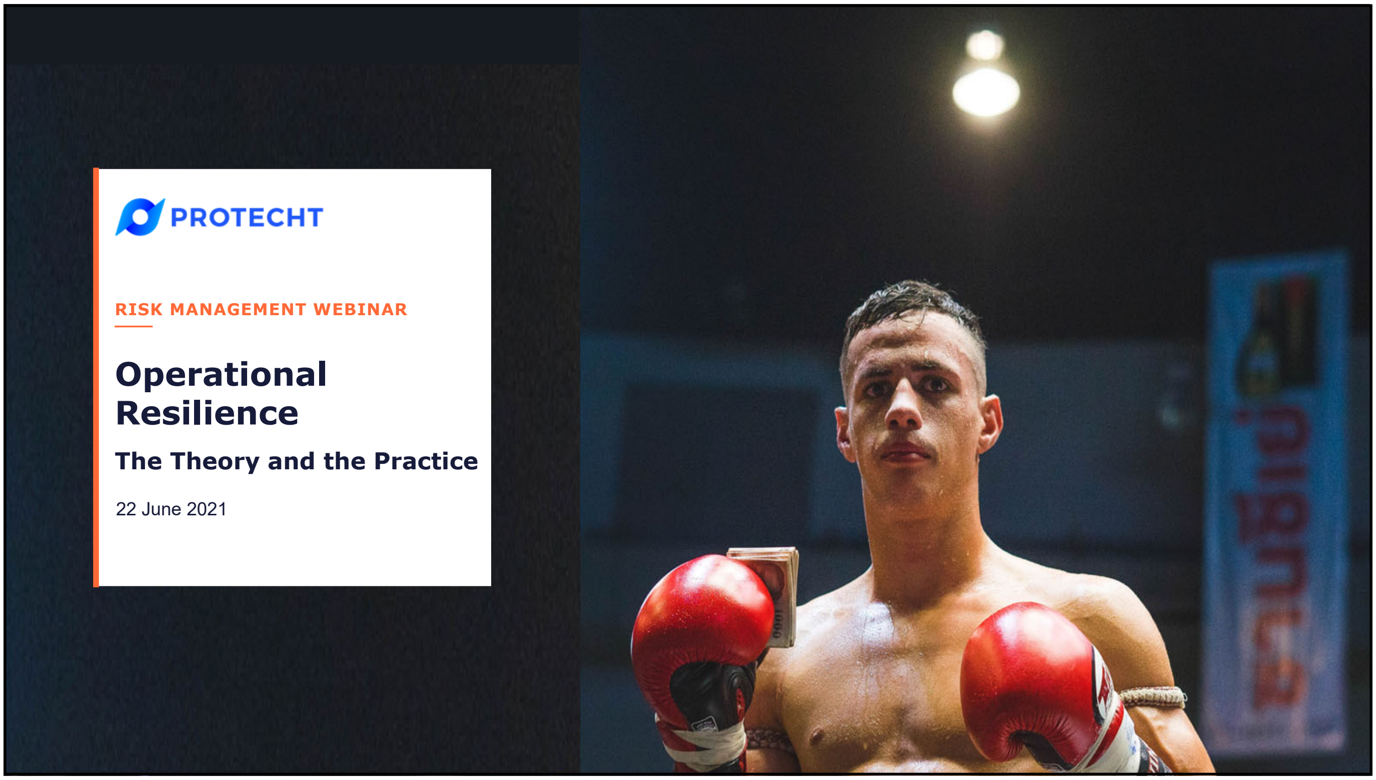


PROTECHT

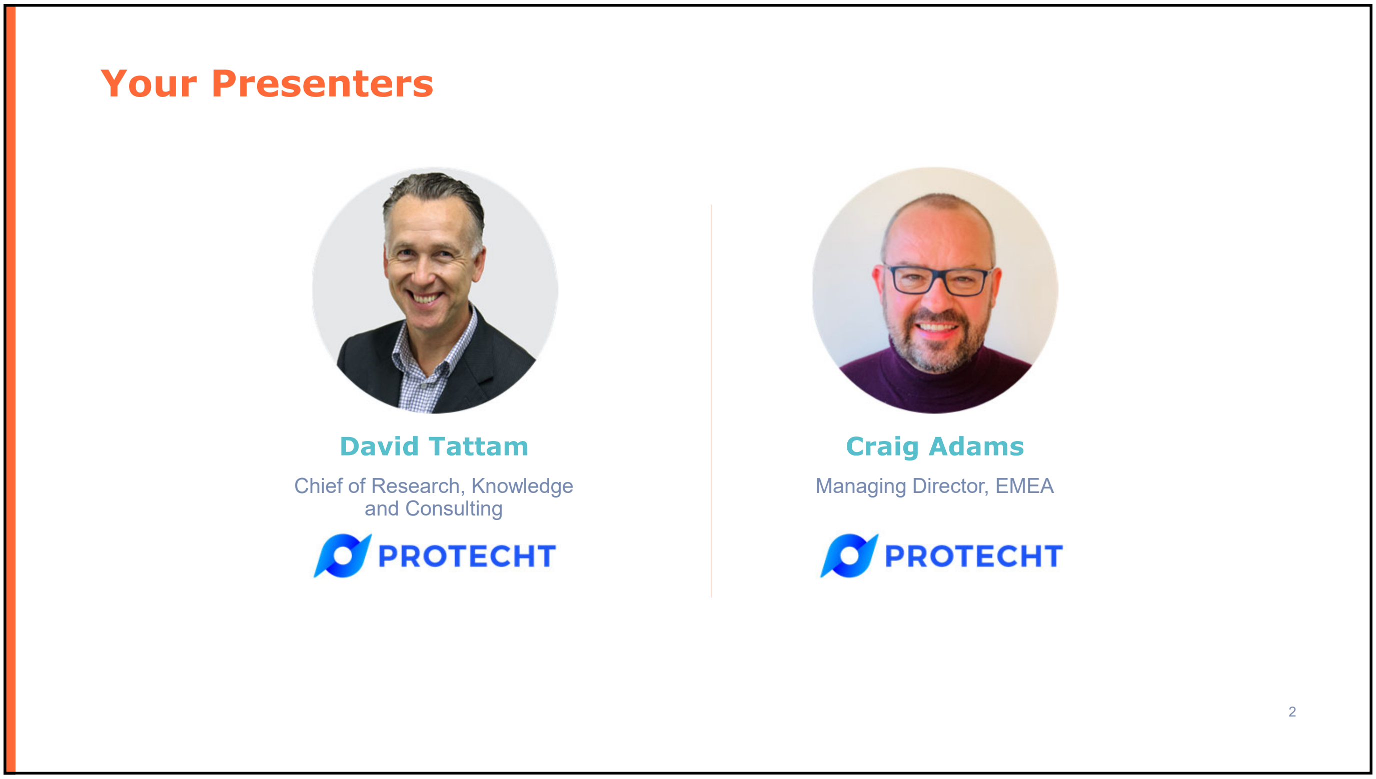
RISK MANAGEMENT WEBINAR

Operational Resilience

The Theory and the Practice

22 June 2021

1



Your Presenters

David Tattam

Chief of Research, Knowledge and Consulting

PROTECHT

Craig Adams

Managing Director, EMEA

PROTECHT

2

2

PROTECHT.ERM

Risk Management Software

A Complete and Flexible Risk Management Solution

- RISK ASSESSMENT
- COMPLIANCE MANAGEMENT
- INTERNAL AUDIT
- KEY RISK INDICATORS
- INCIDENT MANAGEMENT
- ACTIONS MANAGEMENT
- CUSTOM REGISTERS

PROTECHT Redefining Risk

Risk and Controls Self-Assessment: Protecht.ERM delivers centralised divisional and group risk assessments as well as control testing to support control effectiveness ratings.

PROTECHT TRAINING | PROTECHT ERM | PROTECHT ADVISORY | PROTECHT CONSULTING

3

3

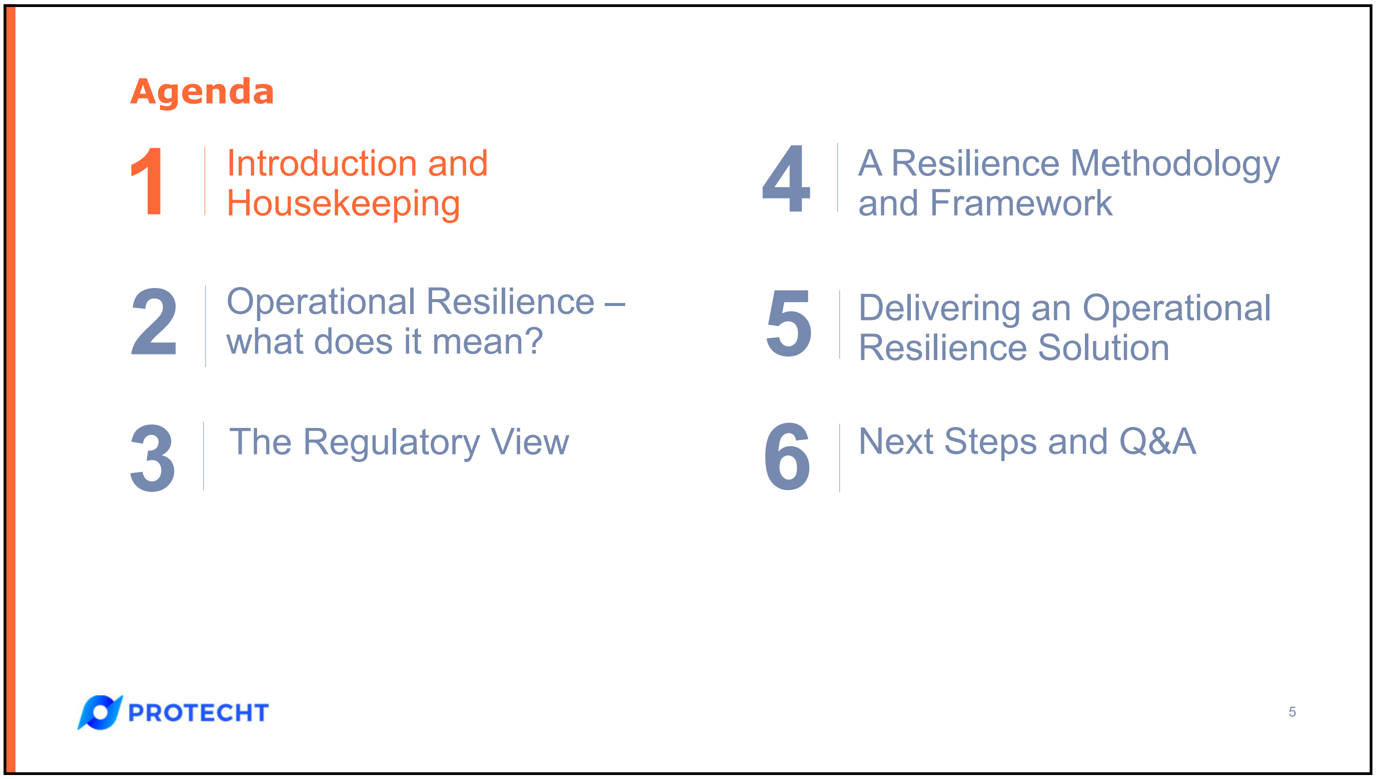
Life doesn’t get easier or more forgiving, we get stronger and more resilient.

Steve Maraboli, Life, the Truth, and Being Free

PROTECHT

4

4



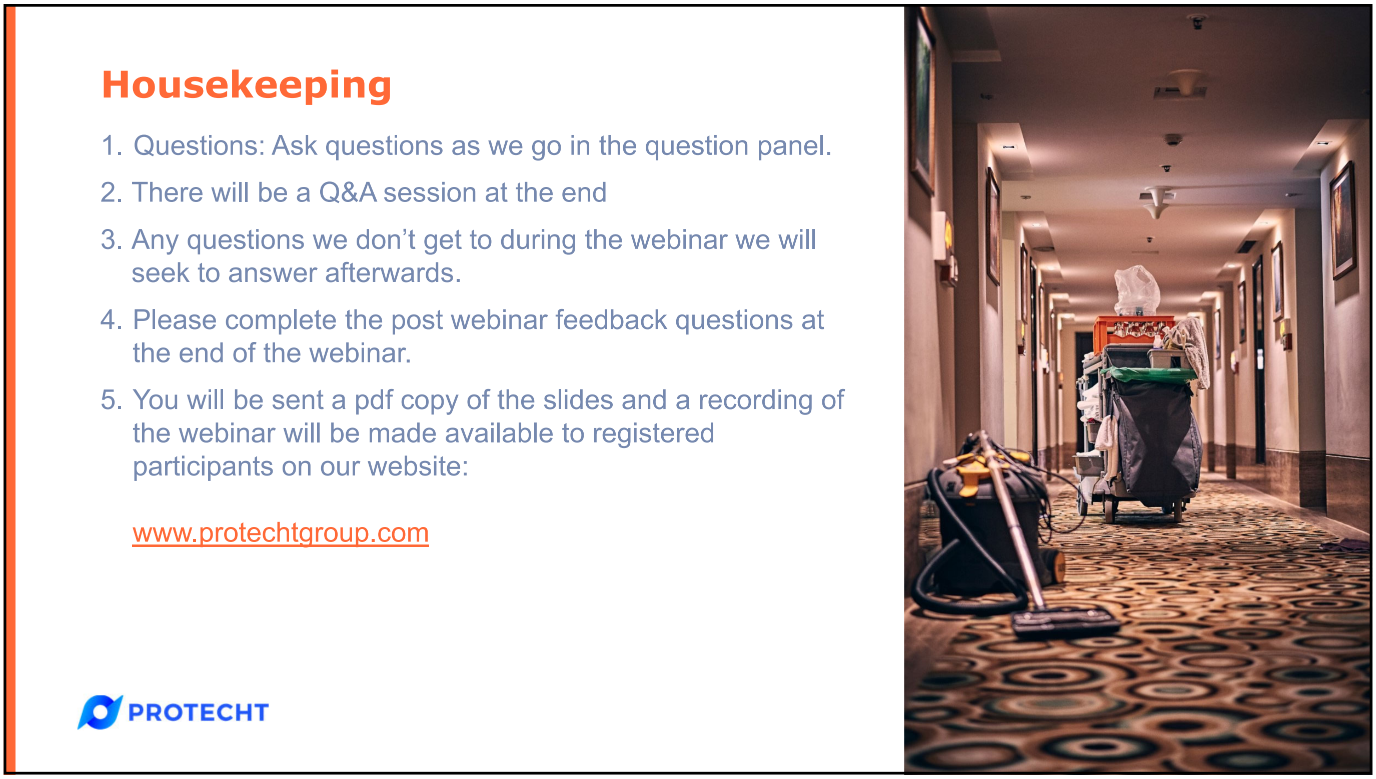
Agenda

1. Introduction and Housekeeping
2. Operational Resilience – what does it mean?
3. The Regulatory View
4. A Resilience Methodology and Framework
5. Delivering an Operational Resilience Solution
6. Next Steps and Q&A

PROTECHT

5

5



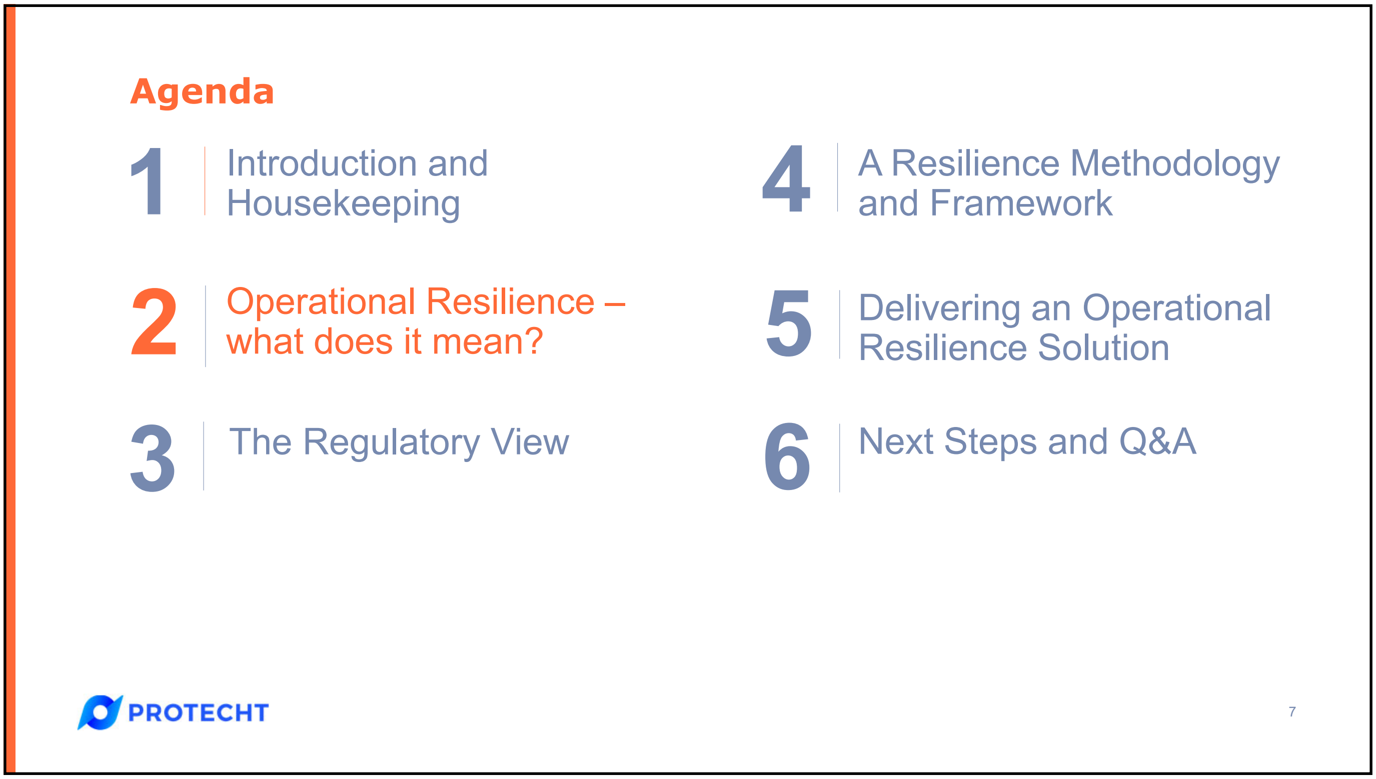
Housekeeping

1. Questions: Ask questions as we go in the question panel.
2. There will be a Q&A session at the end
3. Any questions we don't get to during the webinar we will seek to answer afterwards.
4. Please complete the post webinar feedback questions at the end of the webinar.
5. You will be sent a pdf copy of the slides and a recording of the webinar will be made available to registered participants on our website:

   www.protechtgroup.com

PROTECHT

6



Agenda

1 Introduction and Housekeeping

2 Operational Resilience – what does it mean?

3 The Regulatory View

4 A Resilience Methodology and Framework

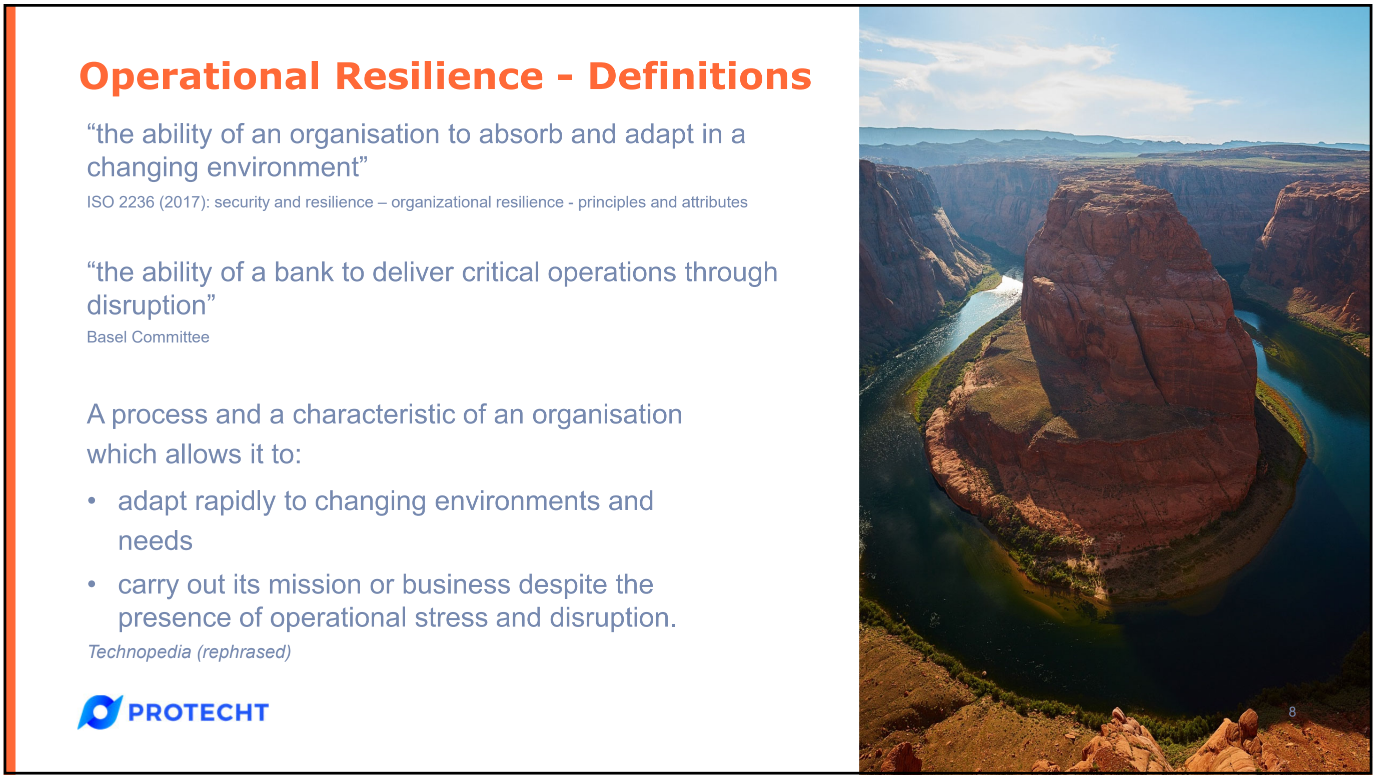
5 Delivering an Operational Resilience Solution

6 Next Steps and Q&A

PROTECHT

7

7



Operational Resilience - Definitions

"the ability of an organisation to absorb and adapt in a changing environment"

ISO 2236 (2017): security and resilience – organizational resilience - principles and attributes

"the ability of a bank to deliver critical operations through disruption"

Basel Committee

A process and a characteristic of an organisation which allows it to:

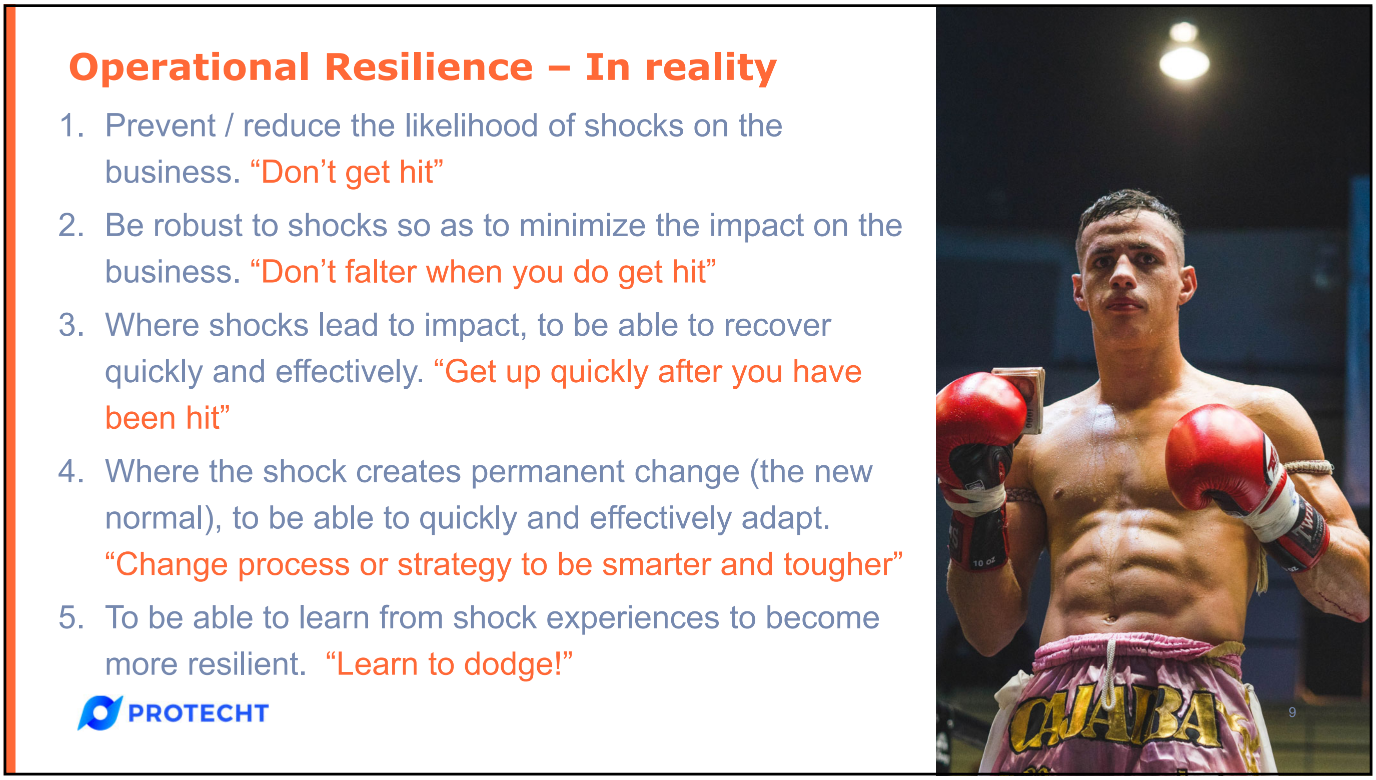
- adapt rapidly to changing environments and needs
- carry out its mission or business despite the presence of operational stress and disruption.

Technopedia (rephrased)

PROTECHT

8

8

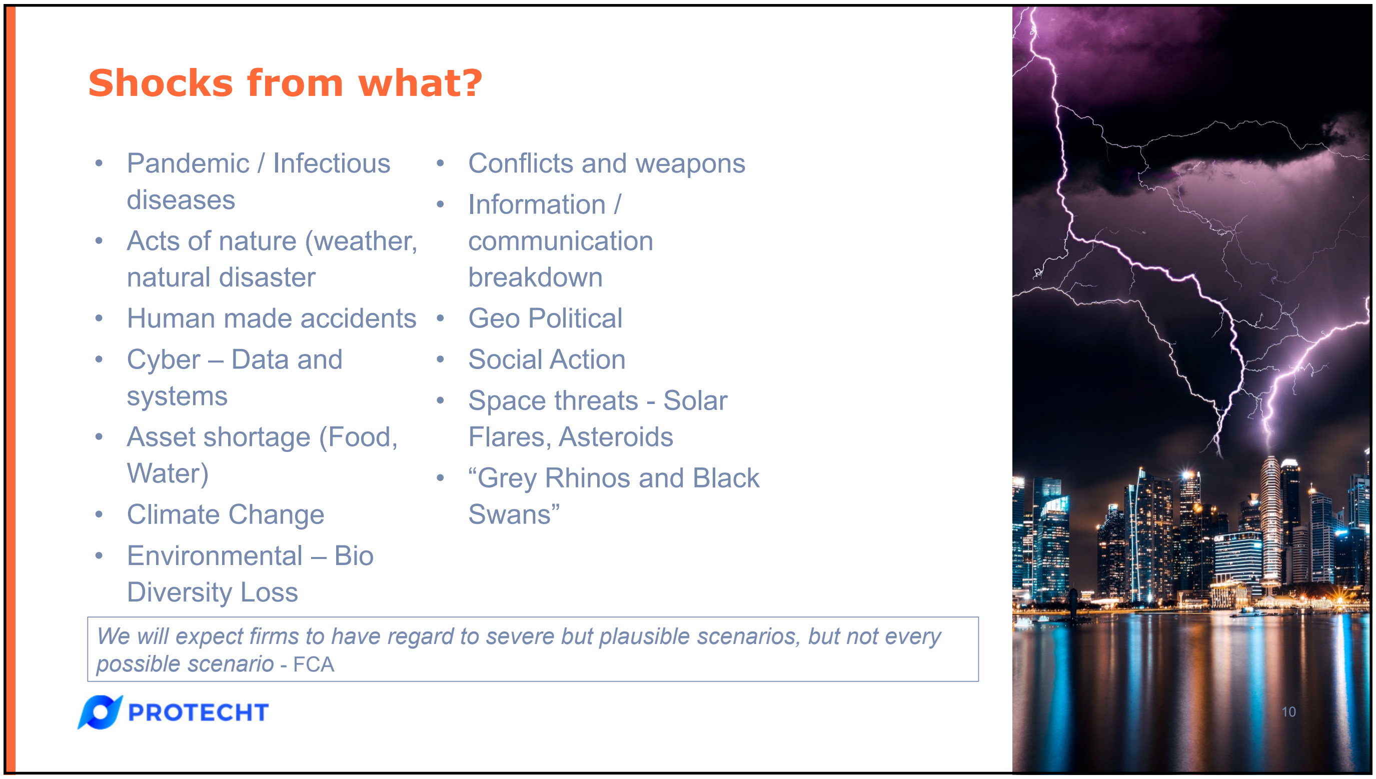


Operational Resilience – In reality

1. Prevent / reduce the likelihood of shocks on the business. “Don’t get hit”
2. Be robust to shocks so as to minimize the impact on the business. “Don’t falter when you do get hit”
3. Where shocks lead to impact, to be able to recover quickly and effectively. “Get up quickly after you have been hit”
4. Where the shock creates permanent change (the new normal), to be able to quickly and effectively adapt. “Change process or strategy to be smarter and tougher”
5. To be able to learn from shock experiences to become more resilient. “Learn to dodge!”

PROTECHT

9



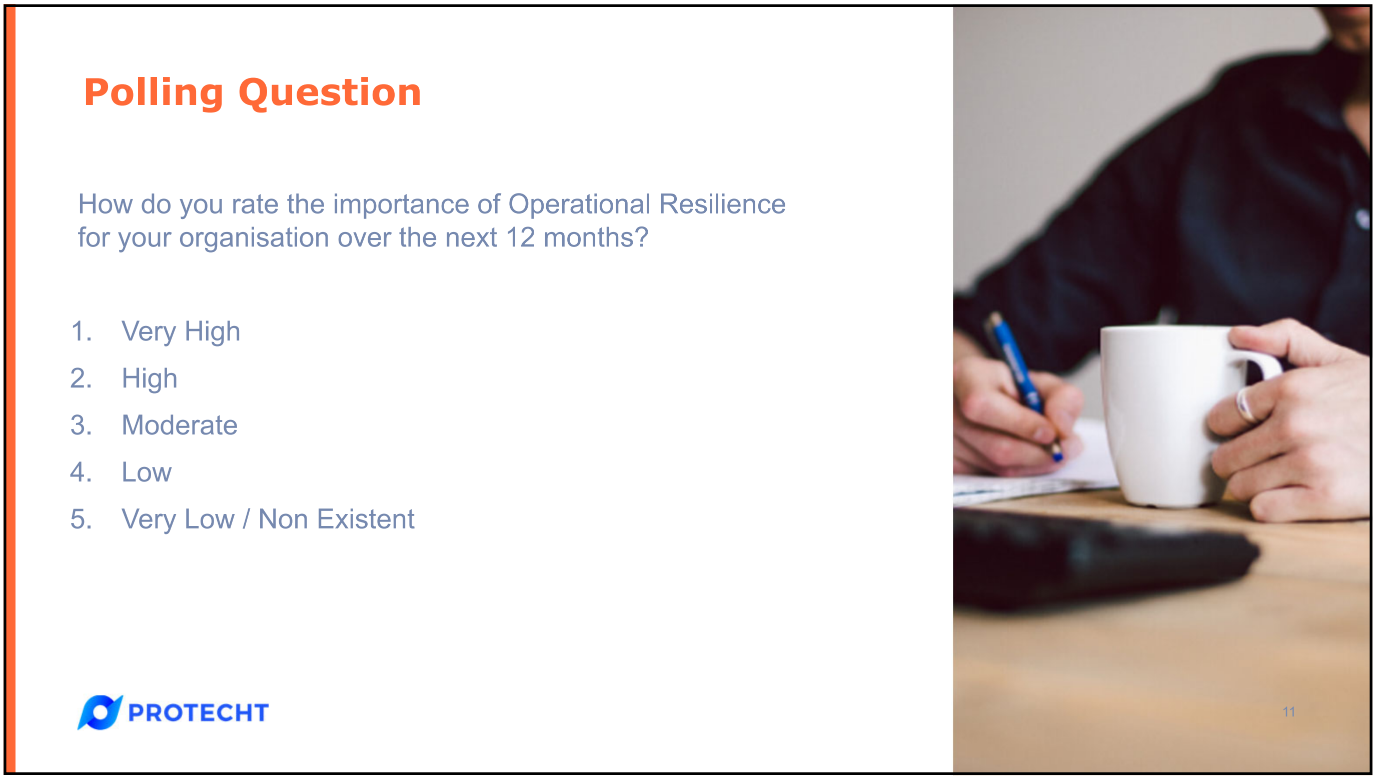
Shocks from what?

- Pandemic / Infectious diseases
- Acts of nature (weather, natural disaster
- Human made accidents
- Cyber – Data and systems
- Asset shortage (Food, Water)
- Climate Change
- Environmental – Bio Diversity Loss
- Conflicts and weapons
- Information / communication breakdown
- Geo Political
- Social Action
- Space threats - Solar Flares, Asteroids
- “Grey Rhinos and Black Swans”

We will expect firms to have regard to severe but plausible scenarios, but not every possible scenario - FCA

PROTECHT

10



Polling Question

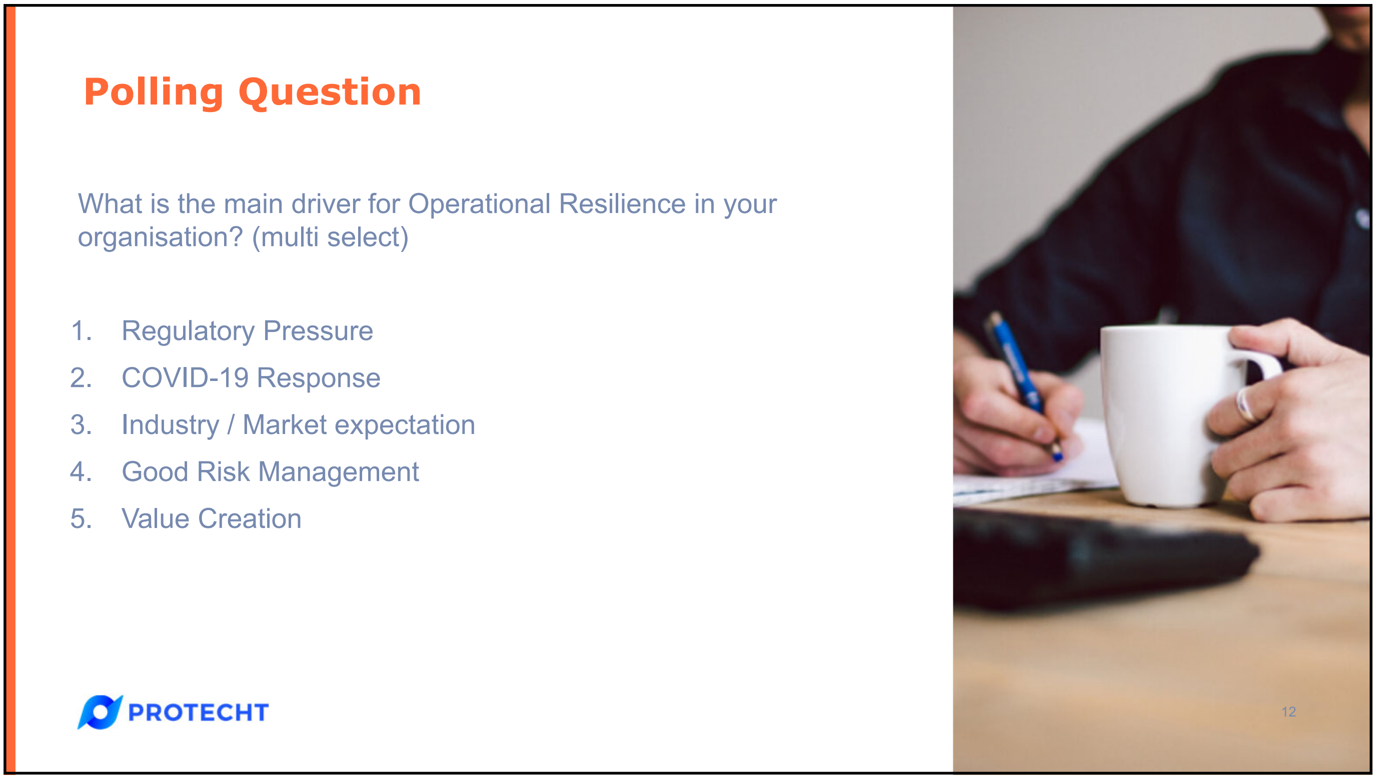
How do you rate the importance of Operational Resilience for your organisation over the next 12 months?

1. Very High
2. High
3. Moderate
4. Low
5. Very Low / Non Existent

PROTECHT

11

11



Polling Question

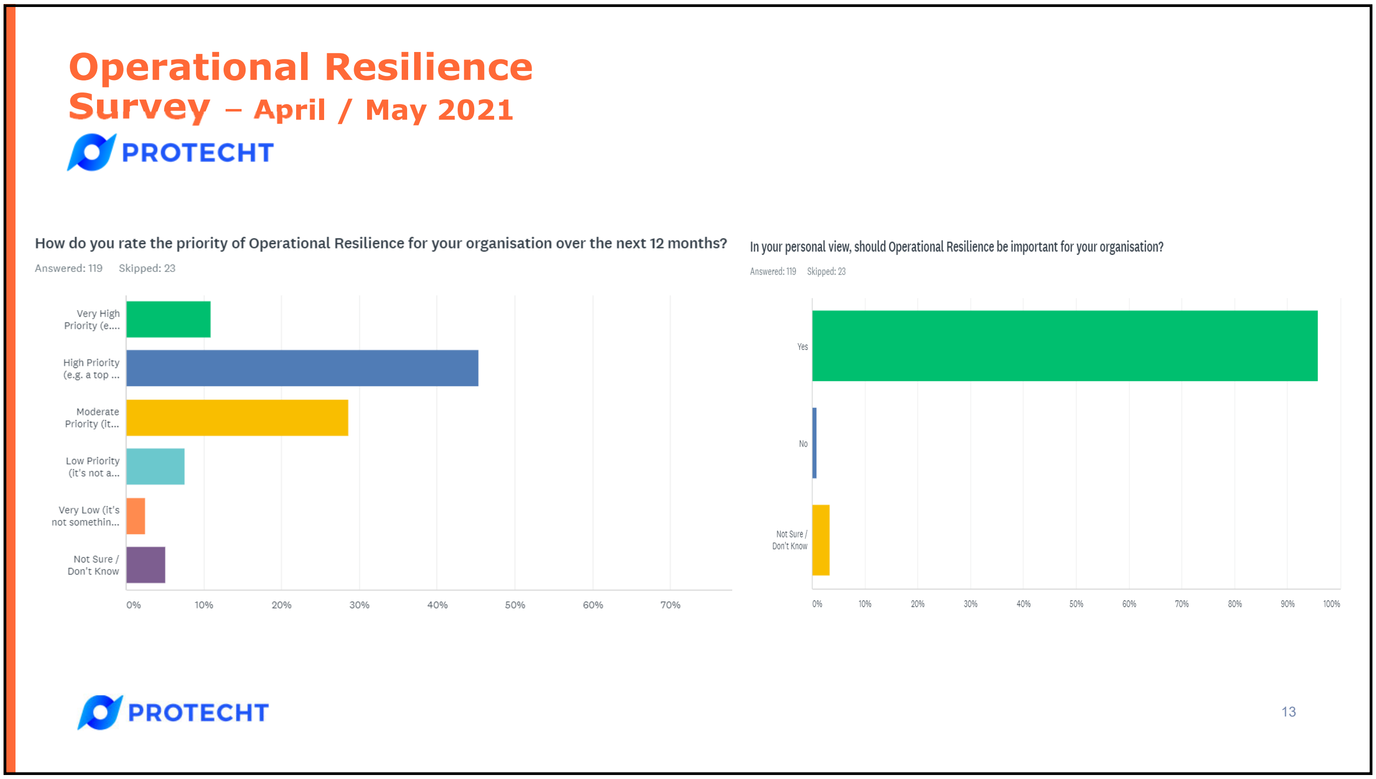
What is the main driver for Operational Resilience in your organisation? (multi select)

1. Regulatory Pressure
2. COVID-19 Response
3. Industry / Market expectation
4. Good Risk Management
5. Value Creation

PROTECHT

12

12



Operational Resilience Survey – April / May 2021

PROTECHT

How do you rate the priority of Operational Resilience for your organisation over the next 12 months?

Answered: 119 Skipped: 23

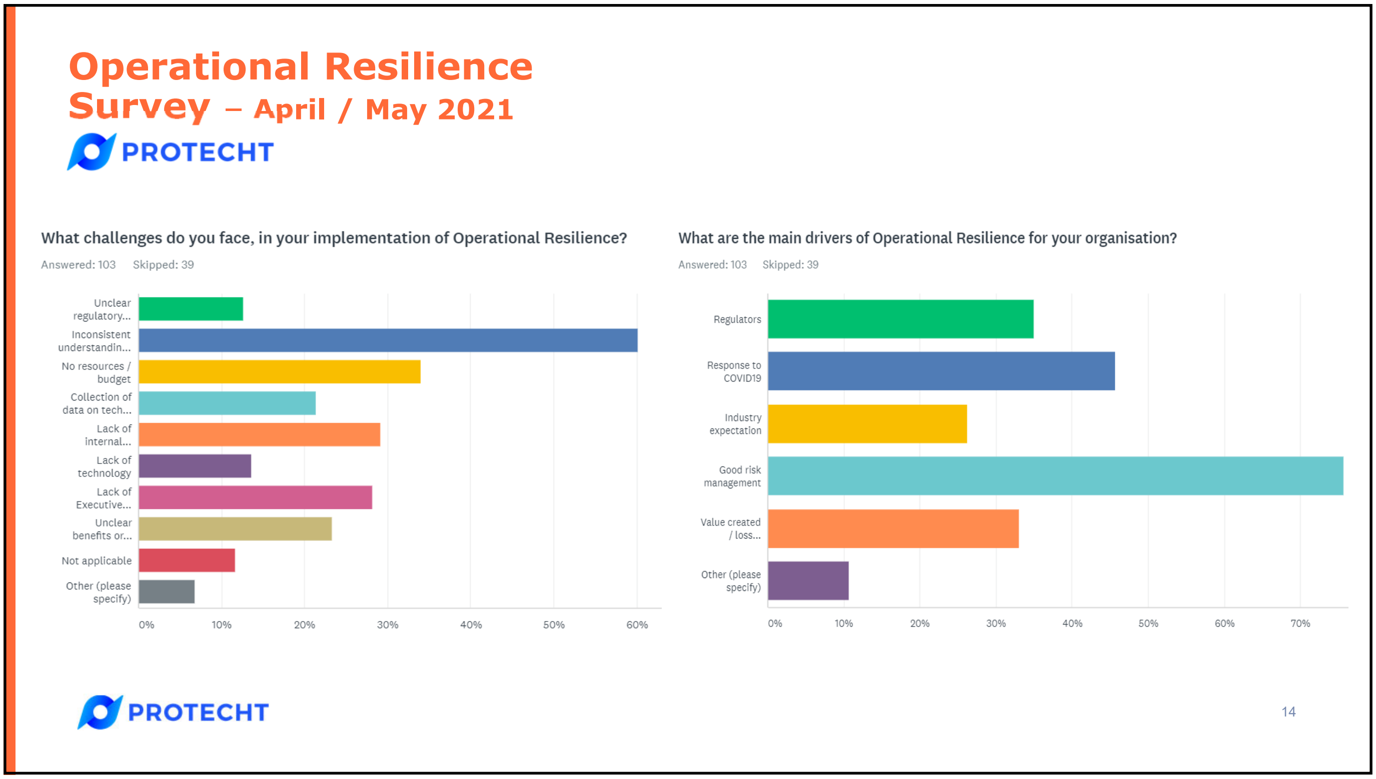
In your personal view, should Operational Resilience be important for your organisation?

Answered: 119 Skipped: 23

PROTECHT

13

13



Operational Resilience Survey – April / May 2021

PROTECHT

What challenges do you face, in your implementation of Operational Resilience?

Answered: 103 Skipped: 39

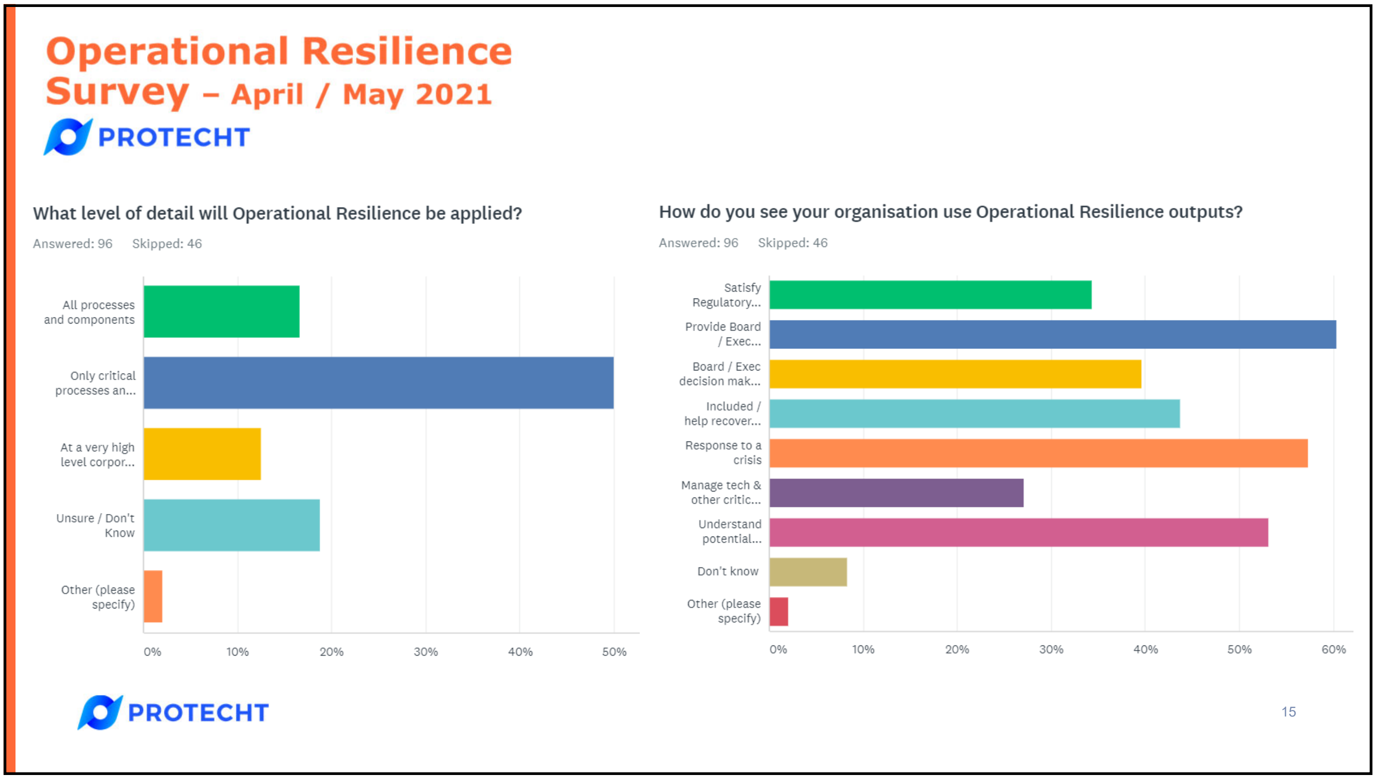
What are the main drivers of Operational Resilience for your organisation?

Answered: 103 Skipped: 39

PROTECHT

14

14

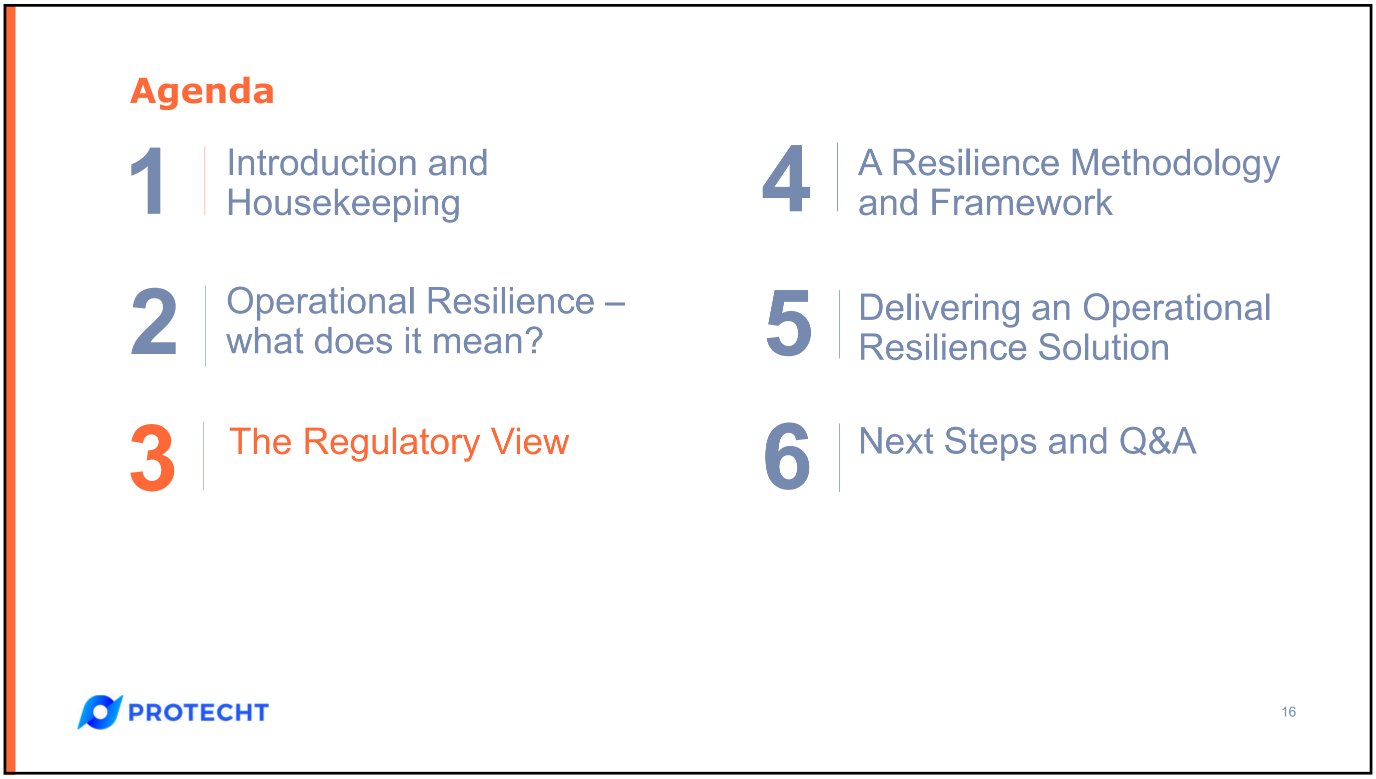


Operational Resilience Survey – April / May 2021

PROTECHT

PROTECHT 15

15



Agenda

1 Introduction and Housekeeping

2 Operational Resilience – what does it mean?

3 The Regulatory View

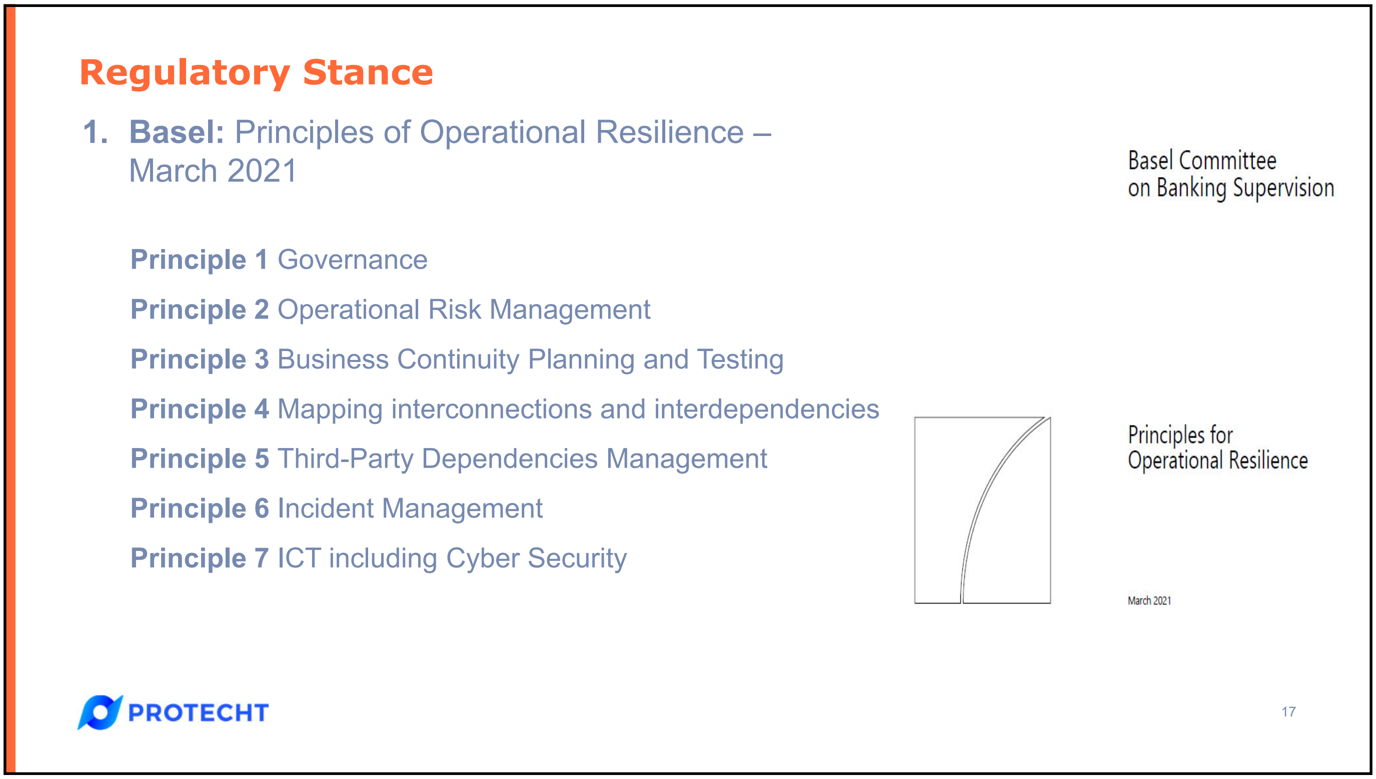
4 A Resilience Methodology and Framework

5 Delivering an Operational Resilience Solution

6 Next Steps and Q&A

PROTECHT 16

16



Regulatory Stance

1. **Basel:** Principles of Operational Resilience – March 2021

Principle 1 Governance

Principle 2 Operational Risk Management

Principle 3 Business Continuity Planning and Testing

Principle 4 Mapping interconnections and interdependencies

Principle 5 Third-Party Dependencies Management

Principle 6 Incident Management

Principle 7 ICT including Cyber Security

Basel Committee
on Banking Supervision

Principles for
Operational Resilience

March 2021

PROTECHT

17

17

Regulatory Stance

1. **Basel:** Principles of Operational Resilience – March 2021
2. **PRA (BoE):** Operational Resilience – Statement of Policy – March 2021

   1. Governance;
   2. Operational risk management;
   3. Business continuity planning (BCP); and
   4. The management of outsourced relationships.

BANK OF ENGLAND
PRUDENTIAL REGULATION
AUTHORITY

Publication

Statement of Policy

Operational resilience

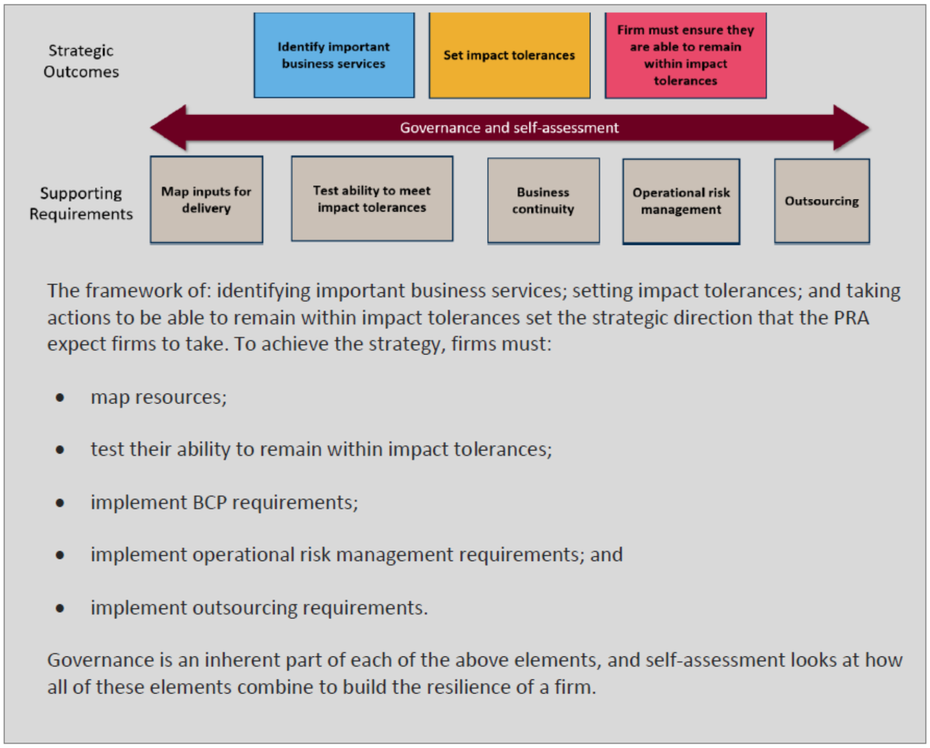
March 2021

PROTECHT

18

18

PRA



Strategic Outcomes
Identify important business services
Set impact tolerances
Firm must ensure they are able to remain within impact tolerances
Governance and self-assessment
Supporting Requirements
Map inputs for delivery
Test ability to meet impact tolerances
Business continuity
Operational risk management
Outsourcing

The framework of: identifying important business services; setting impact tolerances; and taking actions to be able to remain within impact tolerances set the strategic direction that the PRA expect firms to take. To achieve the strategy, firms must:

- map resources;
- test their ability to remain within impact tolerances;
- implement BCP requirements;
- implement operational risk management requirements; and
- implement outsourcing requirements.

Governance is an inherent part of each of the above elements, and self-assessment looks at how all of these elements combine to build the resilience of a firm.

PROTECHT

19

19

PRA - Operational Resilience

1. Prevent disruption occurring to the extent practicable
2. Adapt systems and processes to continue to provide services and functions in the event of an incident
3. Return to normal running promptly when a disruption is over; and
4. Learn and evolve from both incidents and near misses.

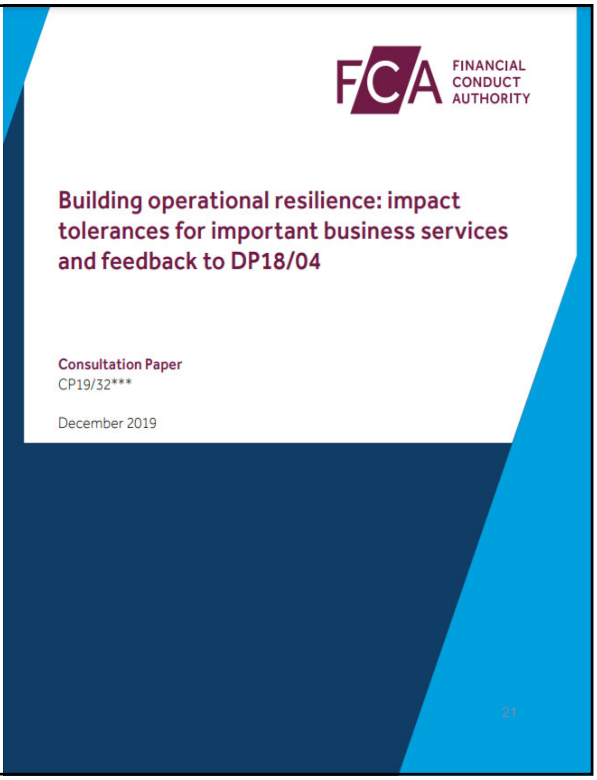
PRA "Operational Resilience" March 2021

PROTECHT

20

Regulatory Stance

1. **Basel:** Principles of Operational Resilience – March 2021
2. **PRA (BoE):** Operational Resilience – Statement of Policy – March 2021
3. **FCA:** CP19/32 Building Operational Resilience



FCA FINANCIAL CONDUCT AUTHORITY

Building operational resilience: impact tolerances for important business services and feedback to DP18/04

Consultation Paper
CP19/32***

December 2019

PROTECHT

21

21

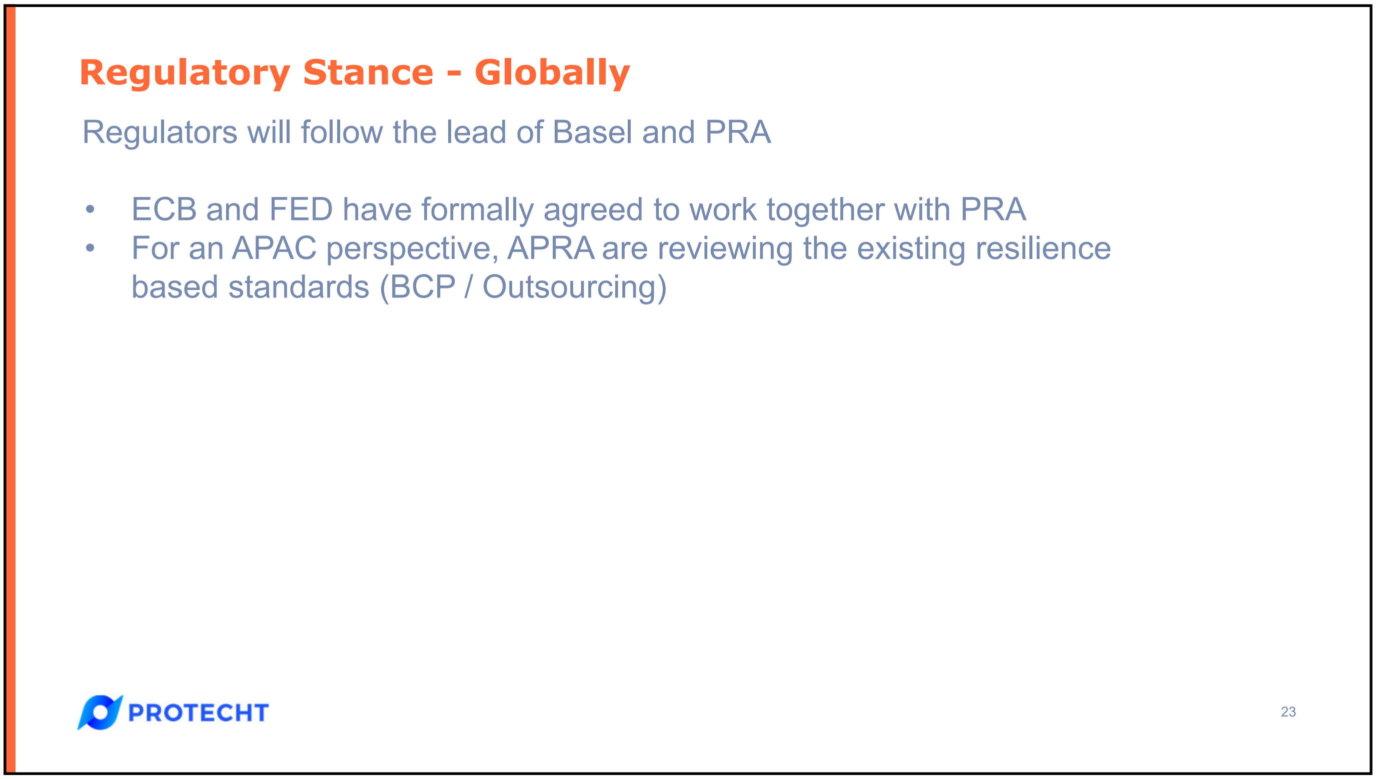
FCA

- identify their **important business services** that if disrupted could cause harm to consumers or market integrity
- identify and document the **people, processes, technology, facilities and information** that support a firm's important business services (mapping)
- set **impact tolerances** for each important business service (i.e. thresholds for maximum tolerable disruption)
- test their **ability to remain within their impact tolerances** through a range of severe but plausible disruption scenarios
- conduct **lessons learned exercises** to identify, prioritise and invest in their ability to respond and recover from disruptions as effectively as possible
- develop internal and external **communications plans** for when important business services are disrupted
- create a **self-assessment** document

PROTECHT

22

22



Regulatory Stance - Globally

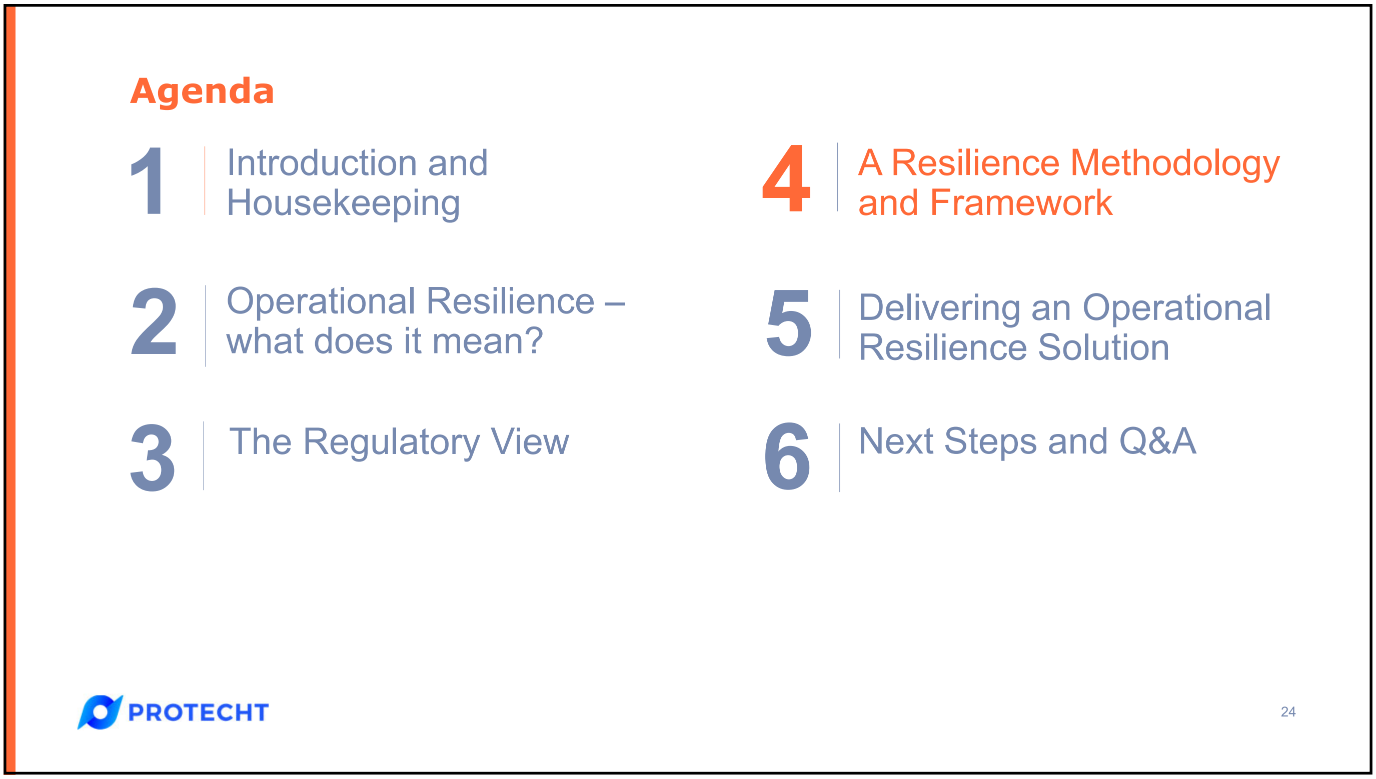
Regulators will follow the lead of Basel and PRA

- ECB and FED have formally agreed to work together with PRA
- For an APAC perspective, APRA are reviewing the existing resilience based standards (BCP / Outsourcing)

PROTECHT

23

23



Agenda

1 Introduction and Housekeeping

2 Operational Resilience – what does it mean?

3 The Regulatory View

4 A Resilience Methodology and Framework

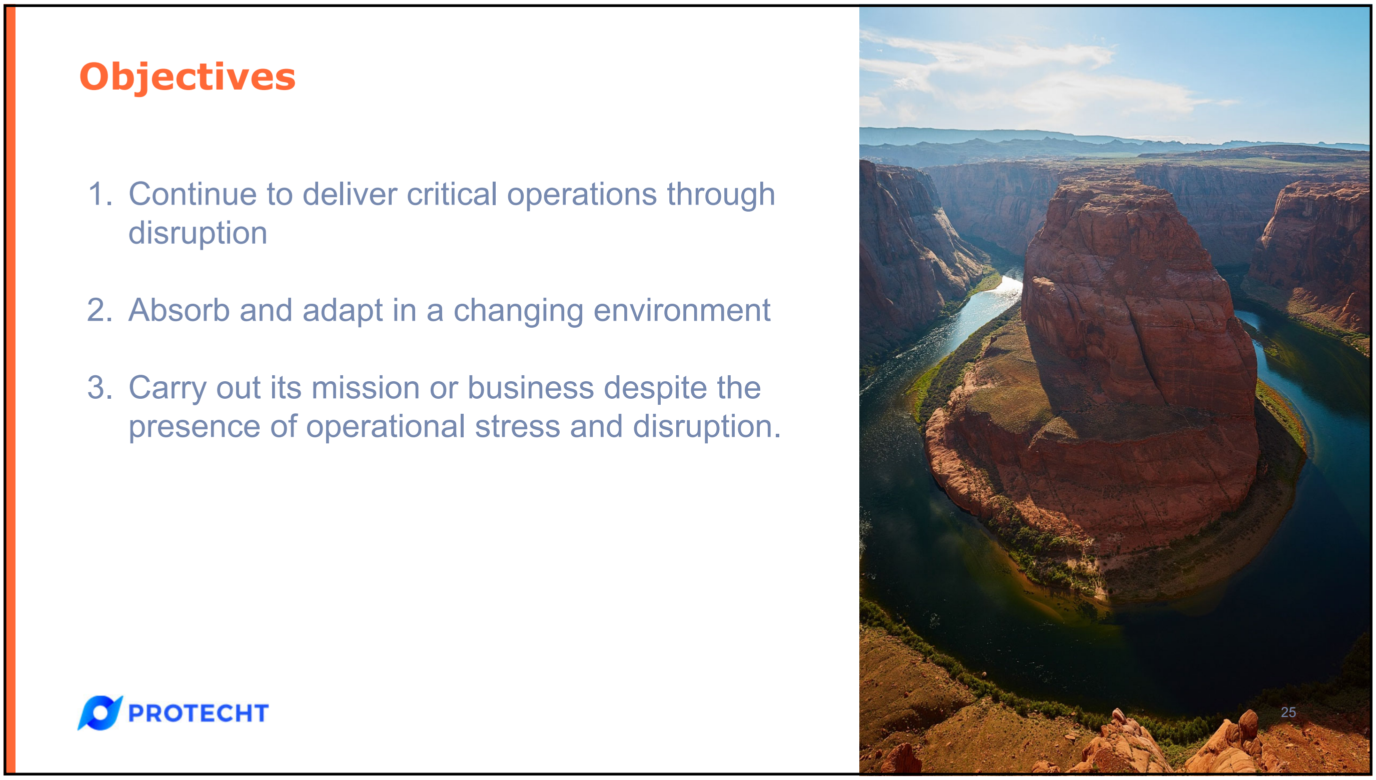
5 Delivering an Operational Resilience Solution

6 Next Steps and Q&A

PROTECHT

24

24



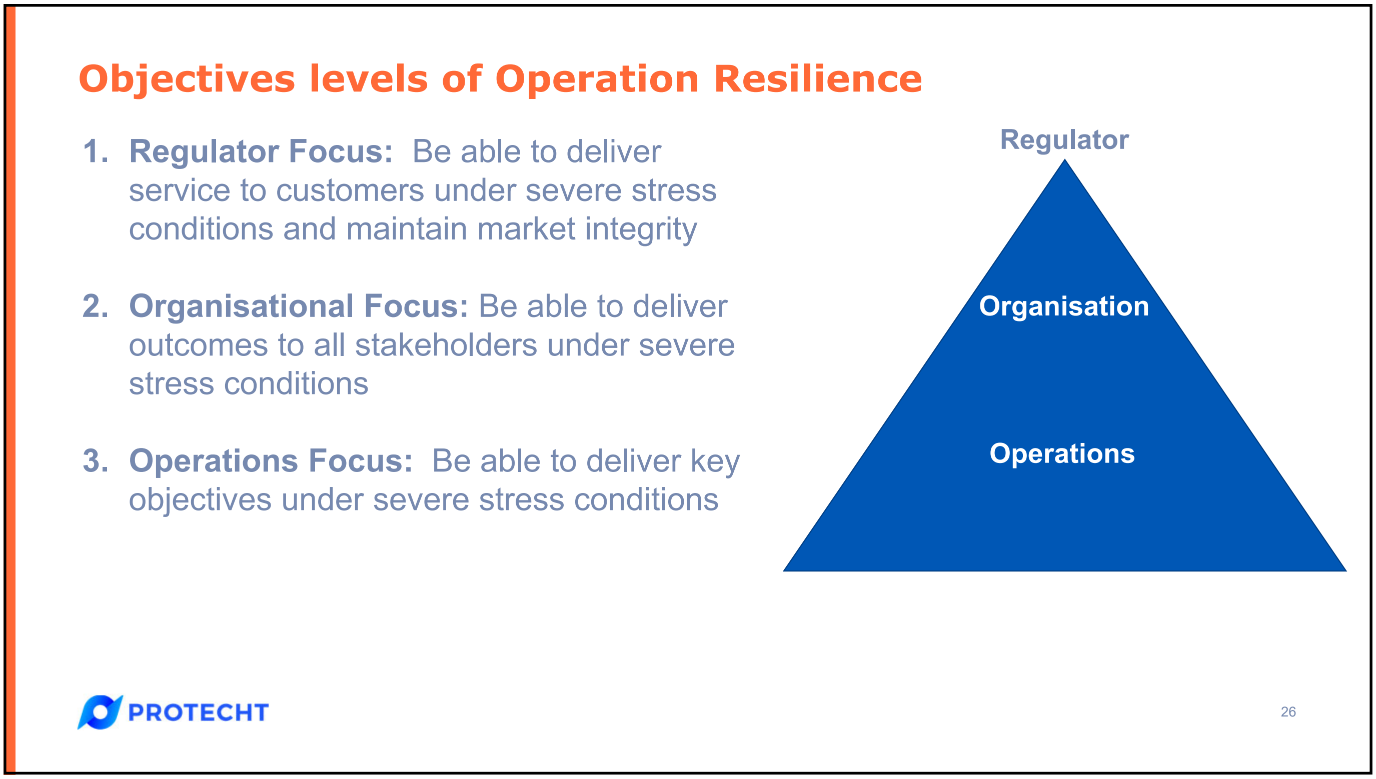
Objectives

1. Continue to deliver critical operations through disruption
2. Absorb and adapt in a changing environment
3. Carry out its mission or business despite the presence of operational stress and disruption.

PROTECHT

25

25



Objectives levels of Operation Resilience

1. **Regulator Focus:** Be able to deliver service to customers under severe stress conditions and maintain market integrity
2. **Organisational Focus:** Be able to deliver outcomes to all stakeholders under severe stress conditions
3. **Operations Focus:** Be able to deliver key objectives under severe stress conditions

Regulator

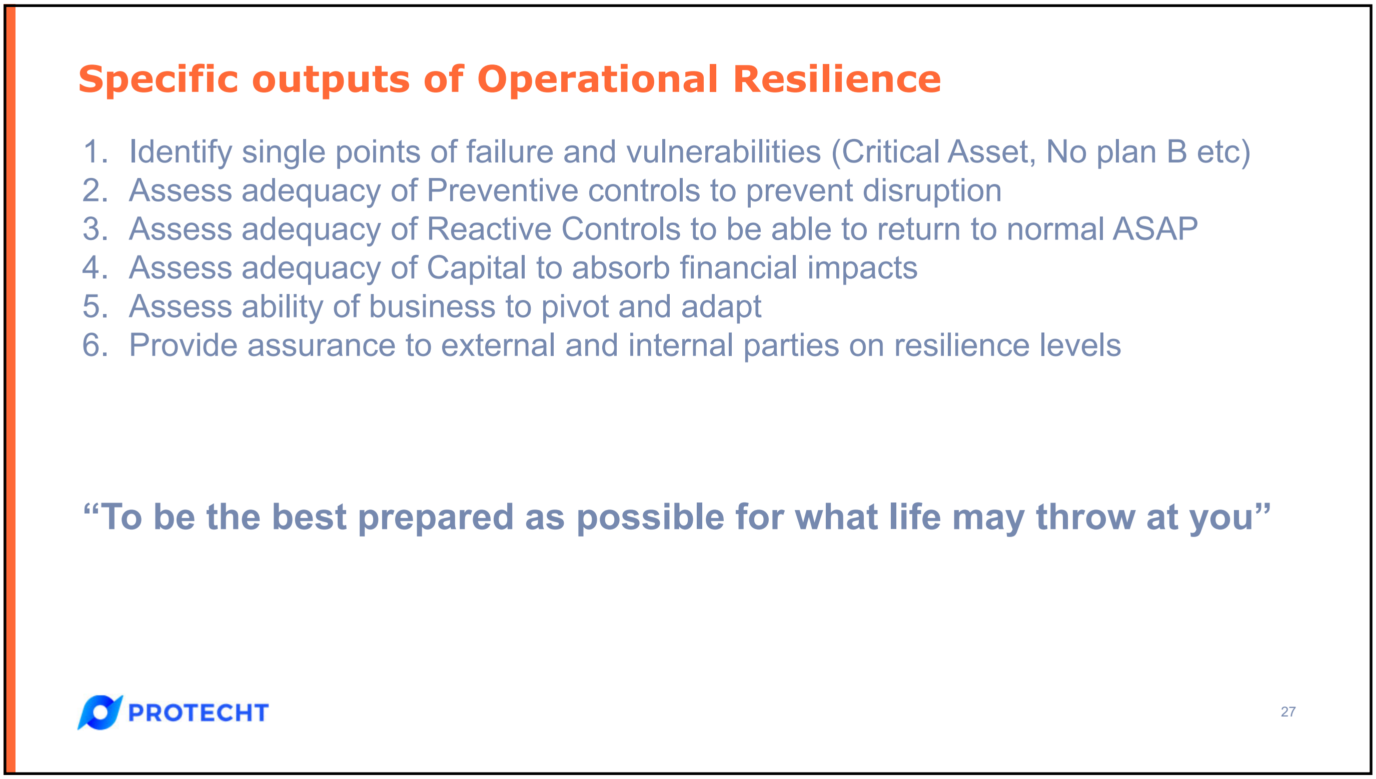
Organisation

Operations

PROTECHT

26

26



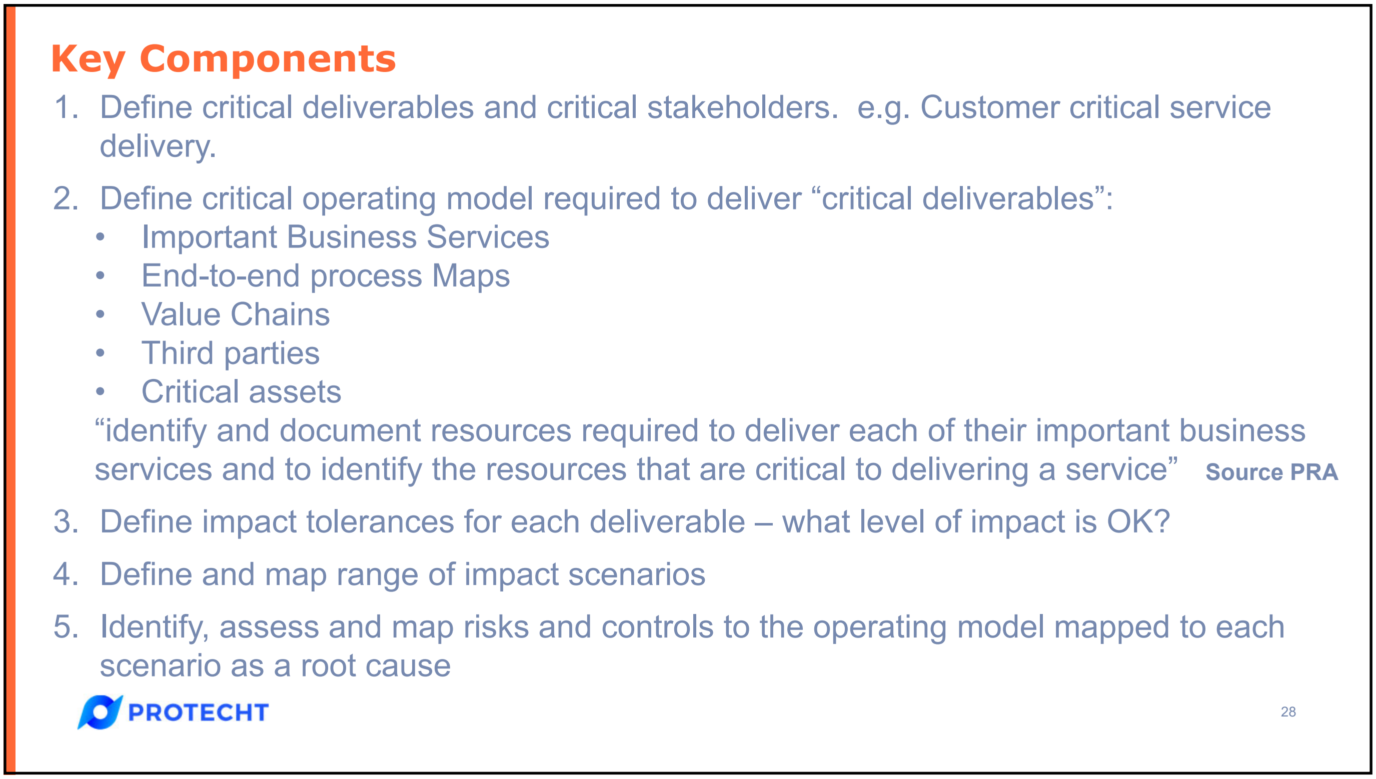
Specific outputs of Operational Resilience

1. Identify single points of failure and vulnerabilities (Critical Asset, No plan B etc)
2. Assess adequacy of Preventive controls to prevent disruption
3. Assess adequacy of Reactive Controls to be able to return to normal ASAP
4. Assess adequacy of Capital to absorb financial impacts
5. Assess ability of business to pivot and adapt
6. Provide assurance to external and internal parties on resilience levels

“To be the best prepared as possible for what life may throw at you”

PROTECHT 27

27



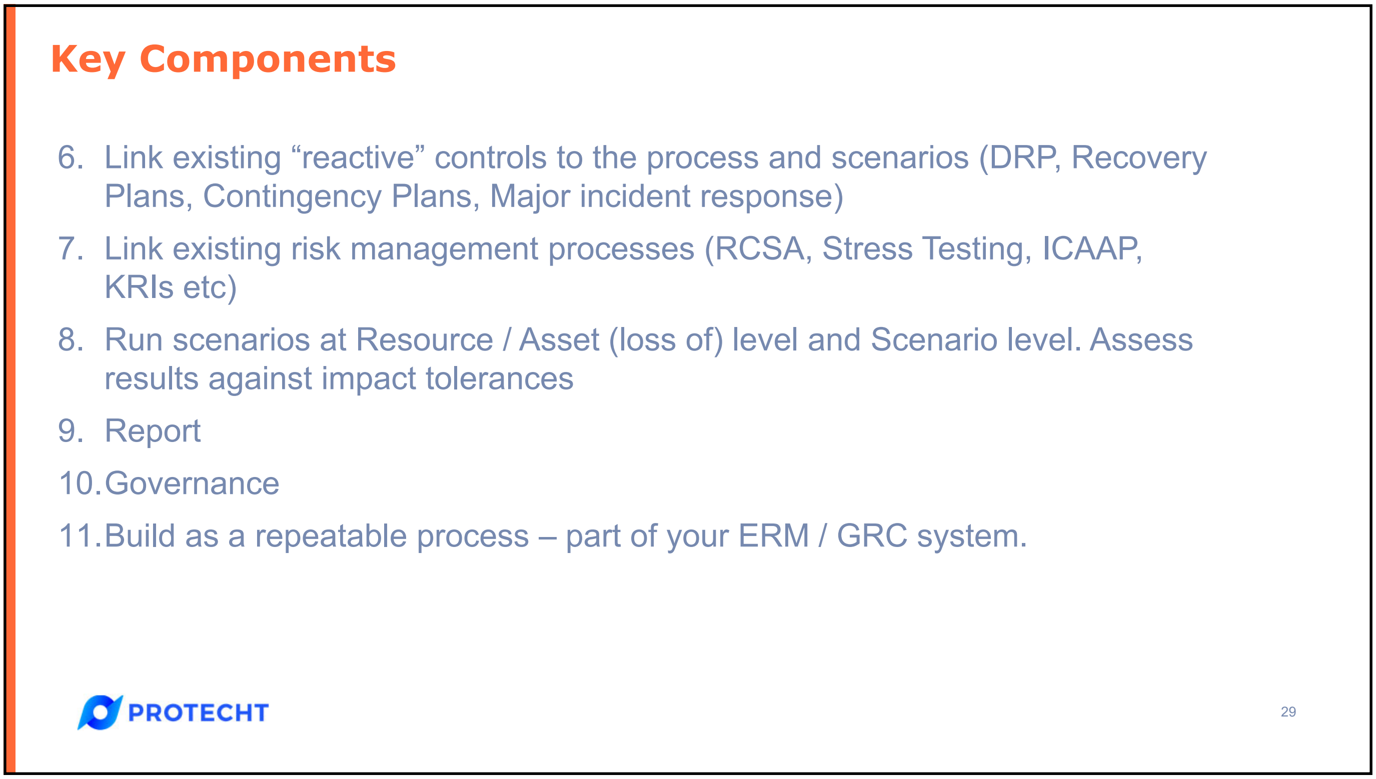
Key Components

1. Define critical deliverables and critical stakeholders. e.g. Customer critical service delivery.
2. Define critical operating model required to deliver “critical deliverables”:
   - Important Business Services
   - End-to-end process Maps
   - Value Chains
   - Third parties
   - Critical assets

   “identify and document resources required to deliver each of their important business services and to identify the resources that are critical to delivering a service” **Source PRA**
3. Define impact tolerances for each deliverable – what level of impact is OK?
4. Define and map range of impact scenarios
5. Identify, assess and map risks and controls to the operating model mapped to each scenario as a root cause

PROTECHT 28

28

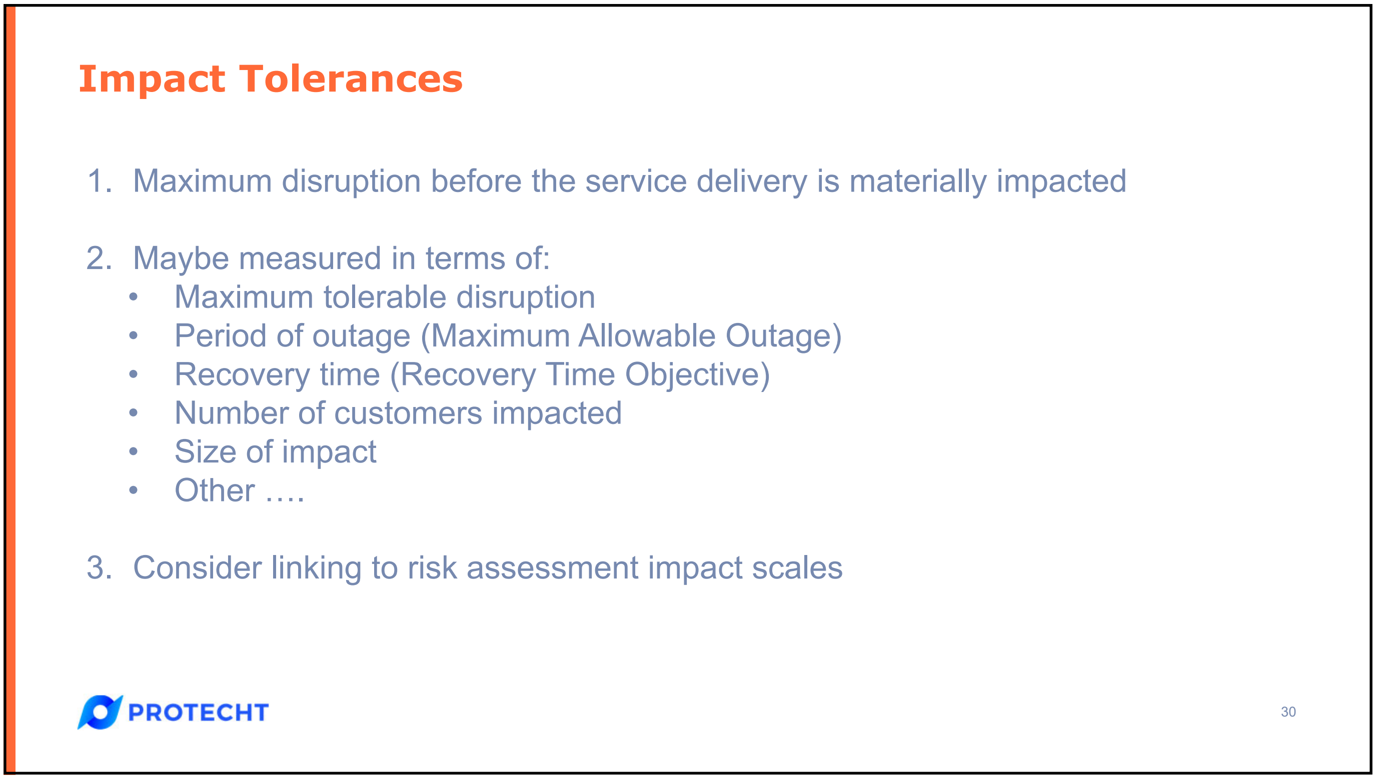


Key Components

6. Link existing “reactive” controls to the process and scenarios (DRP, Recovery Plans, Contingency Plans, Major incident response)
7. Link existing risk management processes (RCSA, Stress Testing, ICAAP, KRIs etc)
8. Run scenarios at Resource / Asset (loss of) level and Scenario level. Assess results against impact tolerances
9. Report
10. Governance
11. Build as a repeatable process – part of your ERM / GRC system.

PROTECHT 29

29



Impact Tolerances

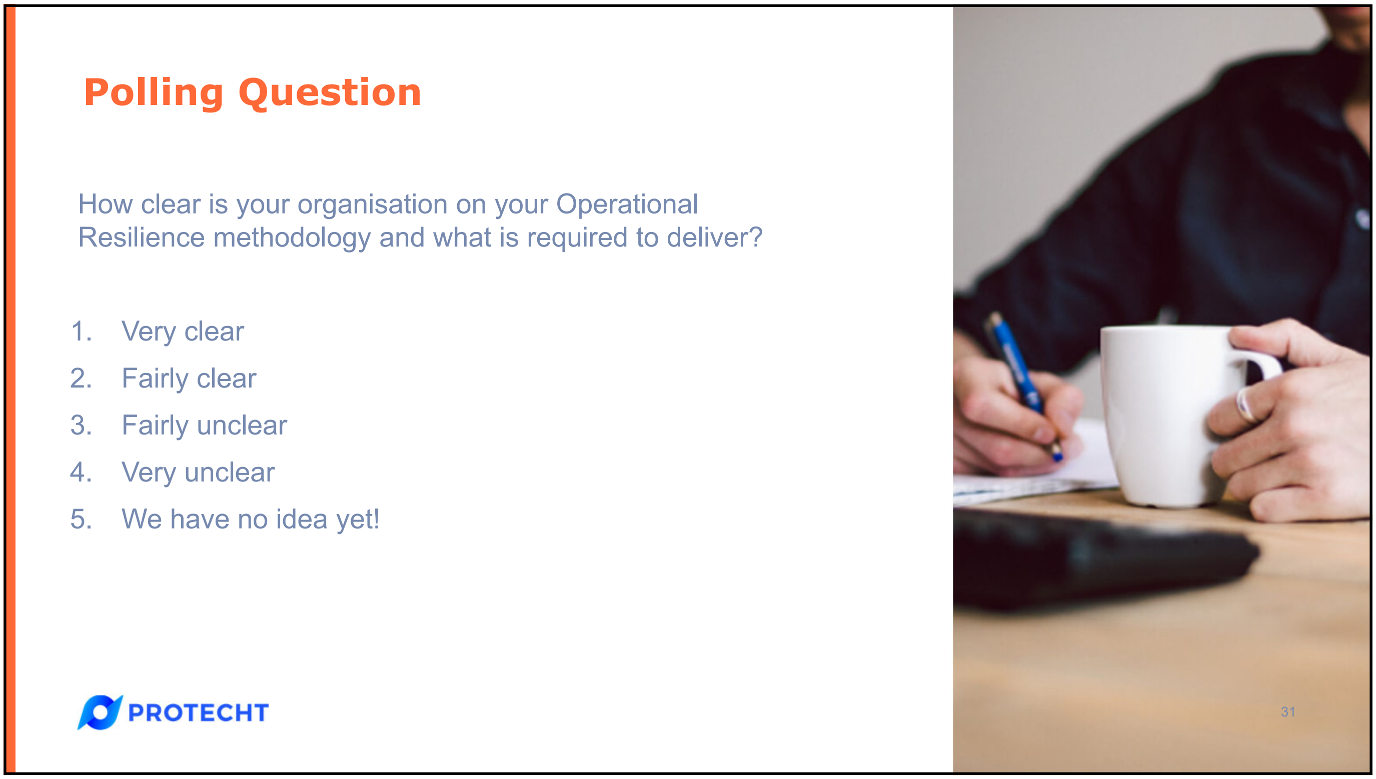
1. Maximum disruption before the service delivery is materially impacted

2. Maybe measured in terms of:
   - Maximum tolerable disruption
   - Period of outage (Maximum Allowable Outage)
   - Recovery time (Recovery Time Objective)
   - Number of customers impacted
   - Size of impact
   - Other ….

3. Consider linking to risk assessment impact scales

PROTECHT 30

30



Polling Question

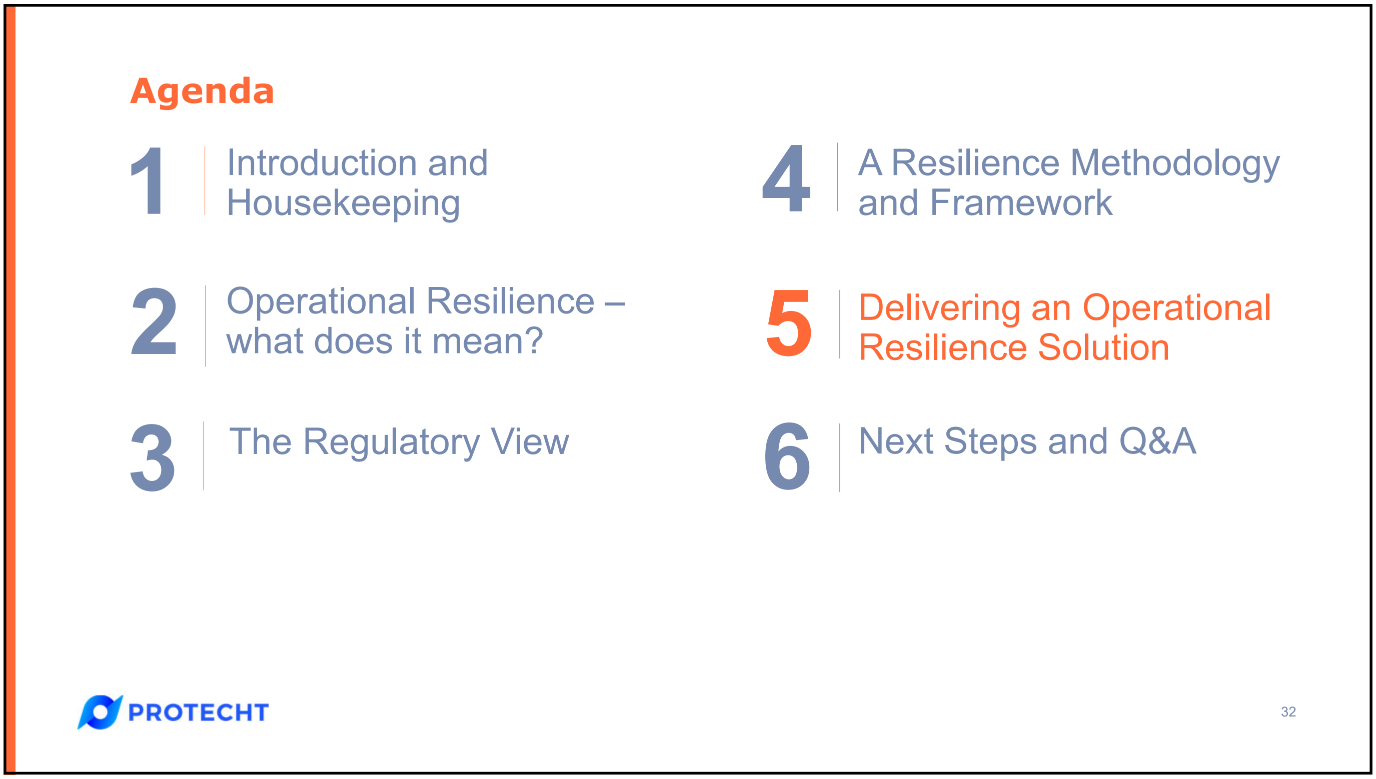
How clear is your organisation on your Operational Resilience methodology and what is required to deliver?

1. Very clear
2. Fairly clear
3. Fairly unclear
4. Very unclear
5. We have no idea yet!

PROTECHT

31

31



Agenda

1 Introduction and Housekeeping

2 Operational Resilience – what does it mean?

3 The Regulatory View

4 A Resilience Methodology and Framework

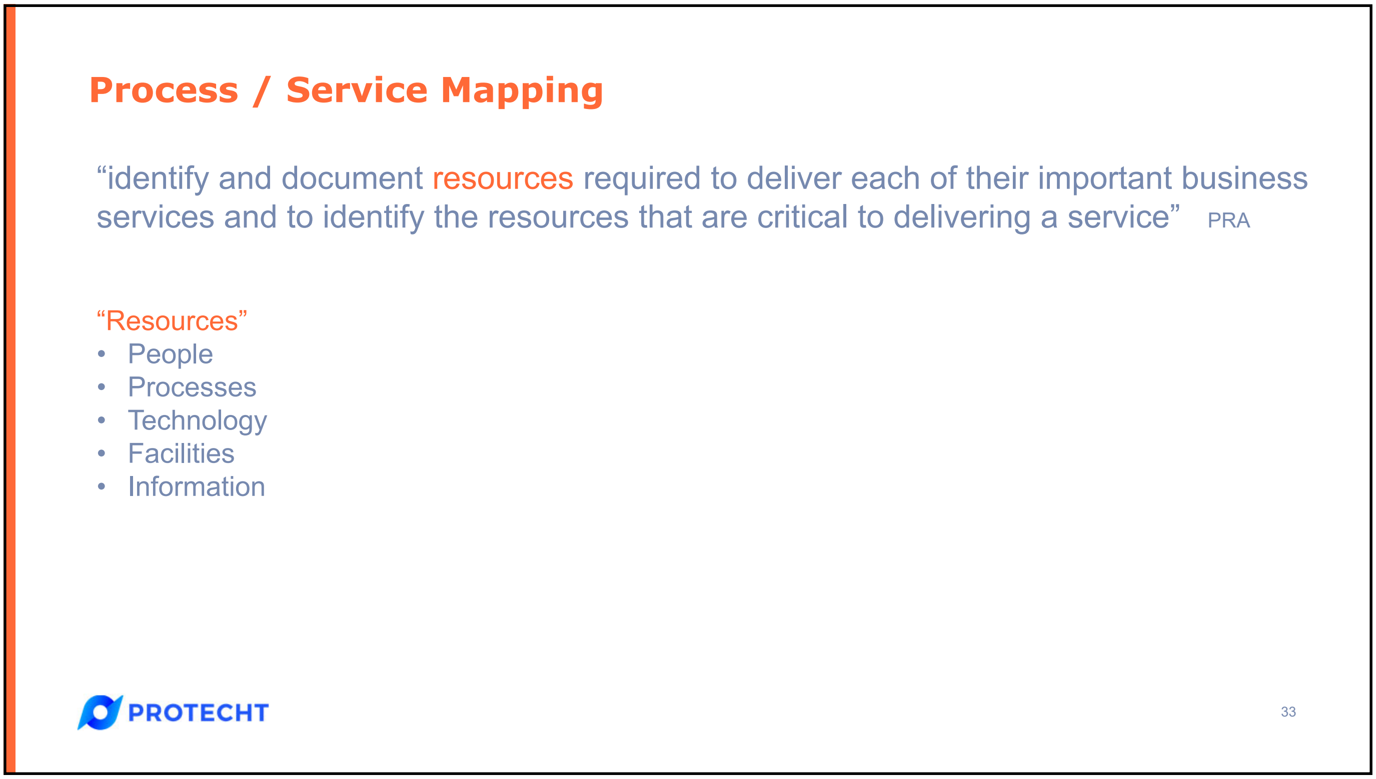
5 Delivering an Operational Resilience Solution

6 Next Steps and Q&A

PROTECHT

32

32



Process / Service Mapping

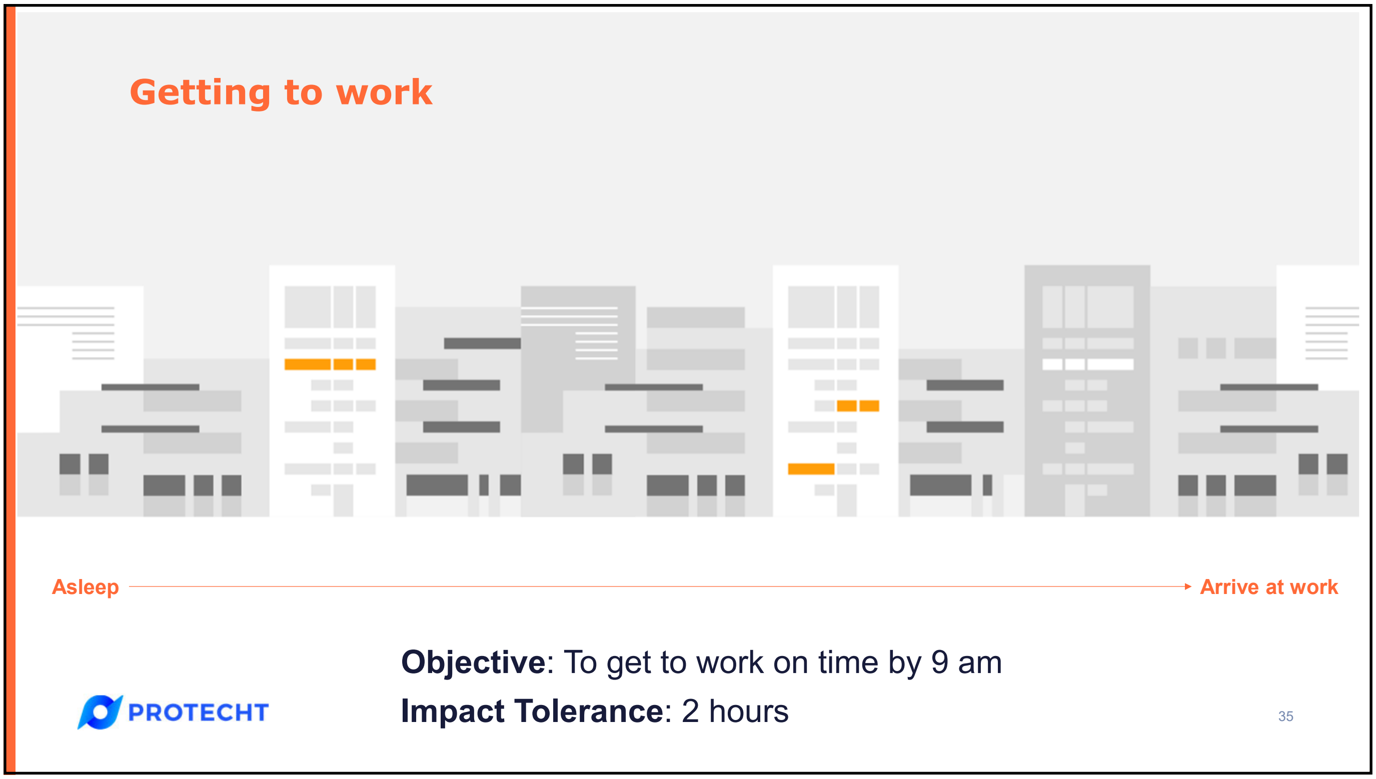
"identify and document resources required to deliver each of their important business services and to identify the resources that are critical to delivering a service" PRA

"Resources"

- People
- Processes
- Technology
- Facilities
- Information

PROTECHT 33

33



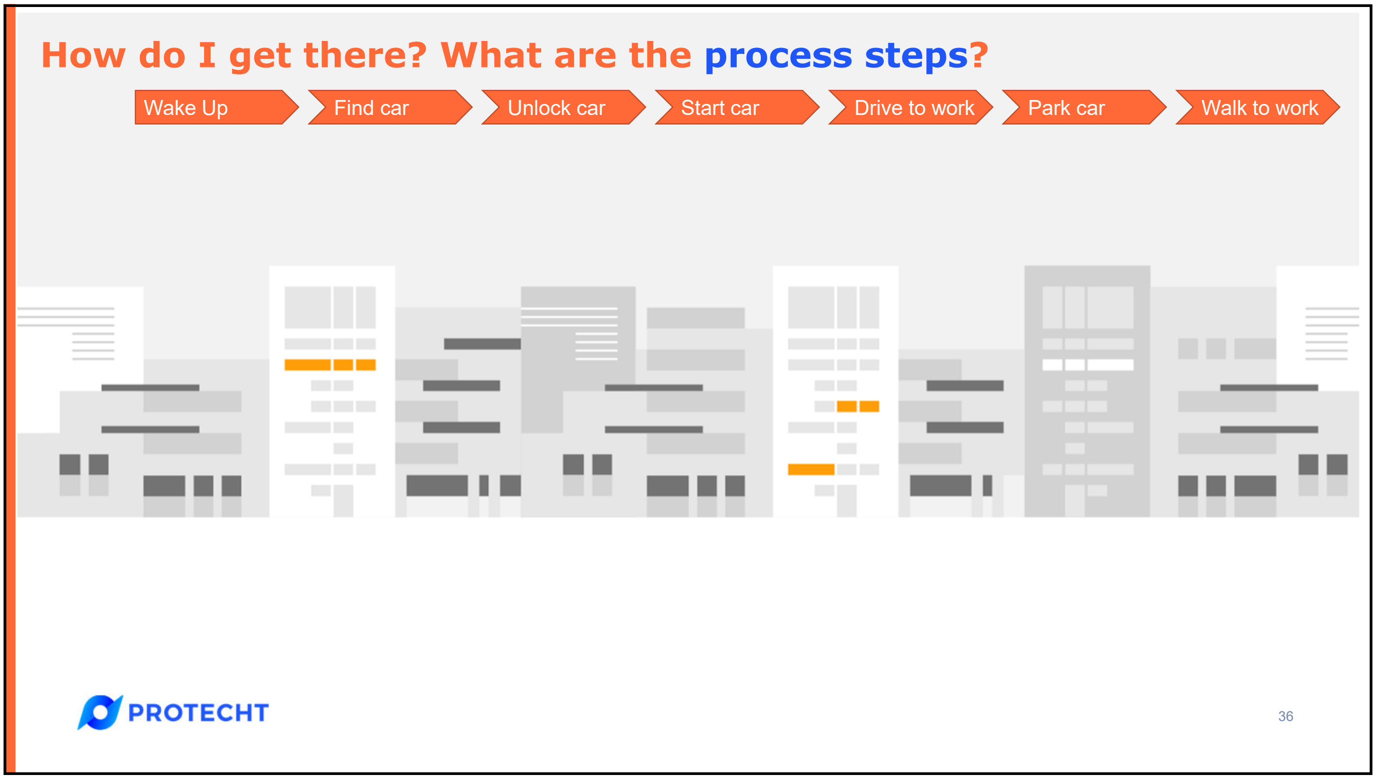
Getting to work

Objective: To get to work on time by 9 am

Impact Tolerance: 2 hours

PROTECHT 35

34



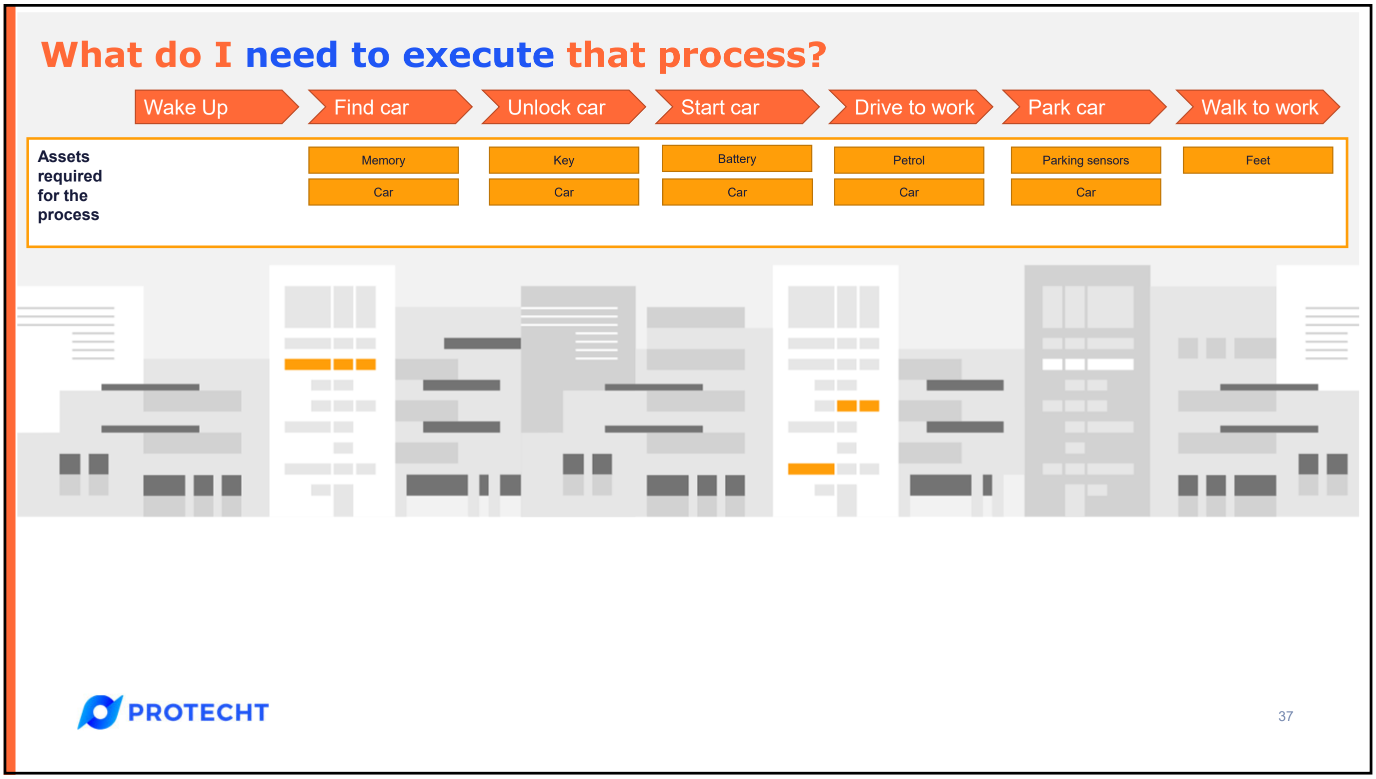
How do I get there? What are the process steps?

Wake Up → Find car → Unlock car → Start car → Drive to work → Park car → Walk to work

PROTECHT

36

35



What do I need to execute that process?

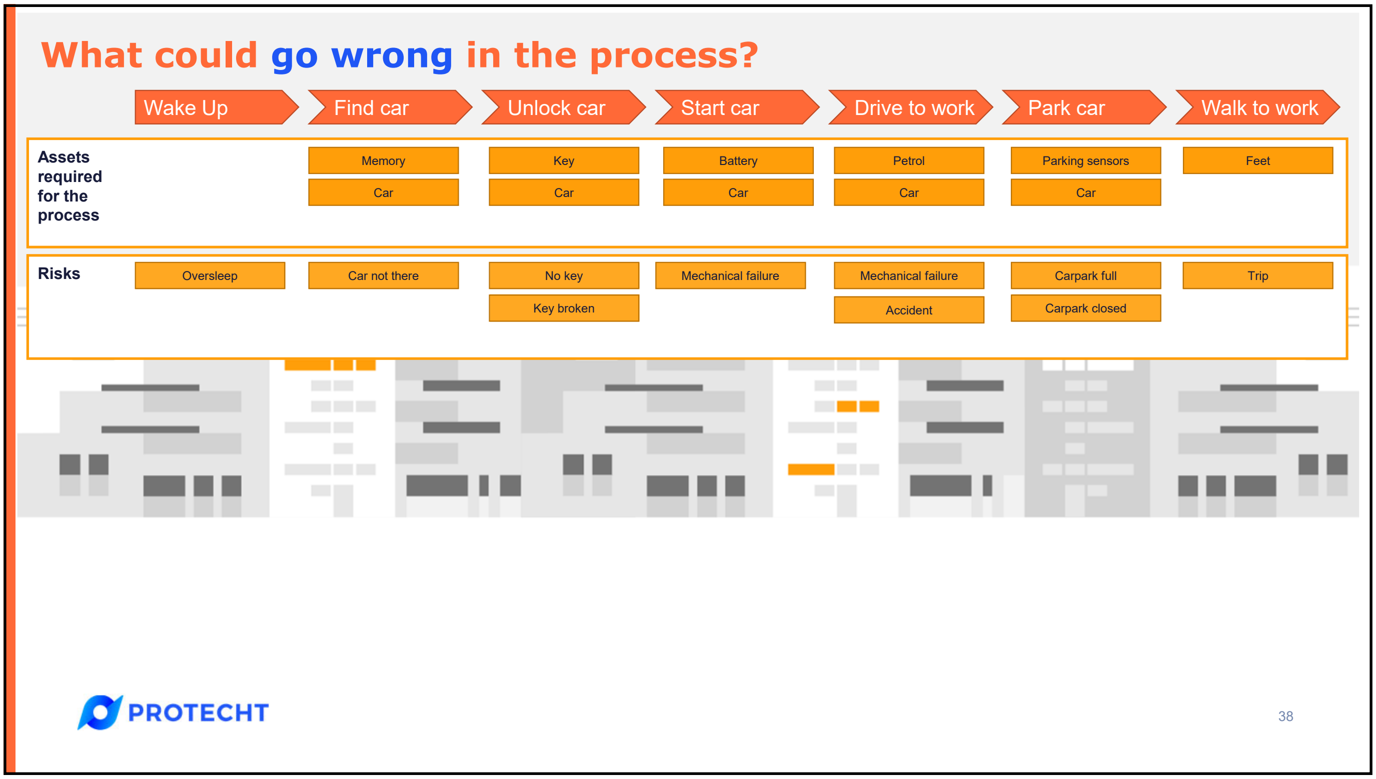
Wake Up → Find car → Unlock car → Start car → Drive to work → Park car → Walk to work

	Wake Up	Find car	Unlock car	Start car	Drive to work	Park car	Walk to work
Assets required for the process		Memory Car	Key Car	Battery Car	Petrol Car	Parking sensors Car	Feet

PROTECHT

37

36



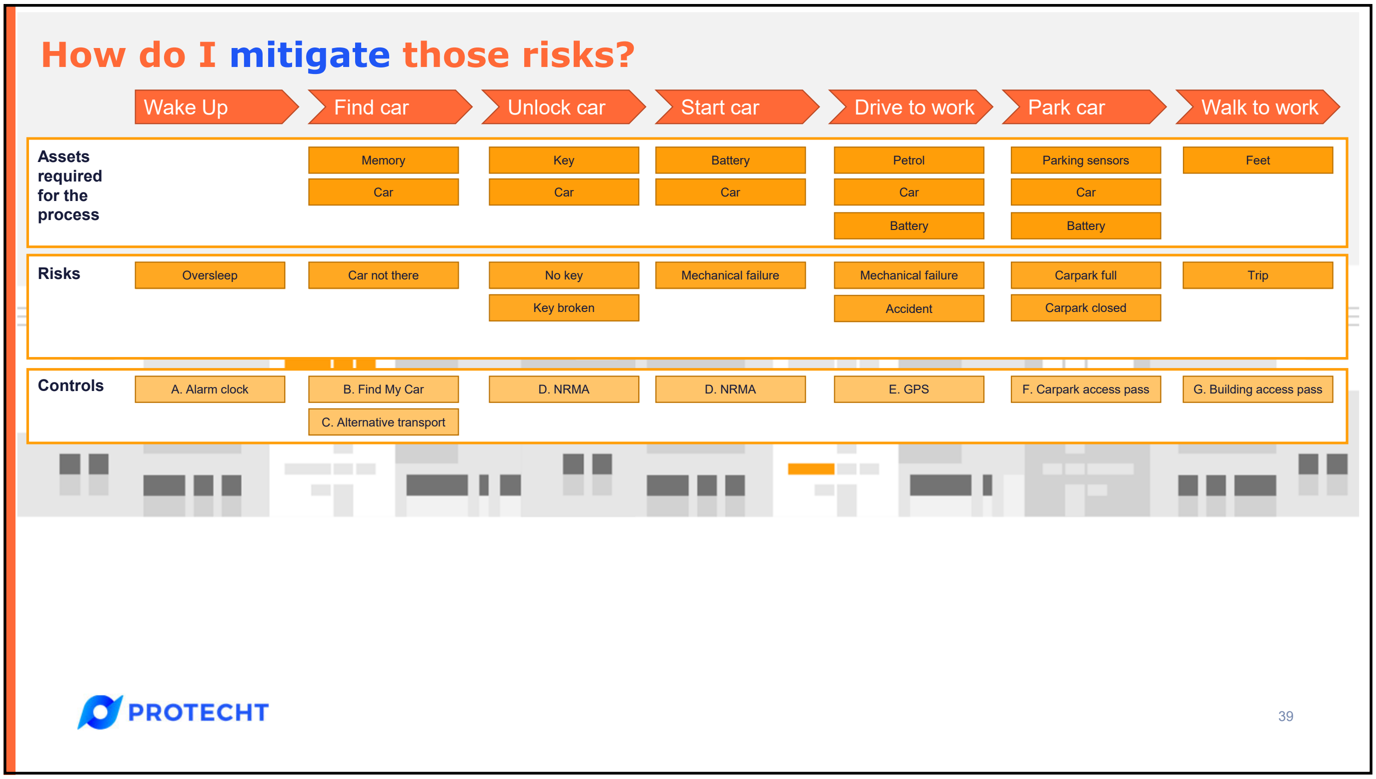
What could go wrong in the process?

	Wake Up	Find car	Unlock car	Start car	Drive to work	Park car	Walk to work
Assets required for the process		Memory Car	Key Car	Battery Car	Petrol Car	Parking sensors Car	Feet
Risks	Oversleep	Car not there	No key Key broken	Mechanical failure	Mechanical failure Accident	Carpark full Carpark closed	Trip

PROTECHT

38

37



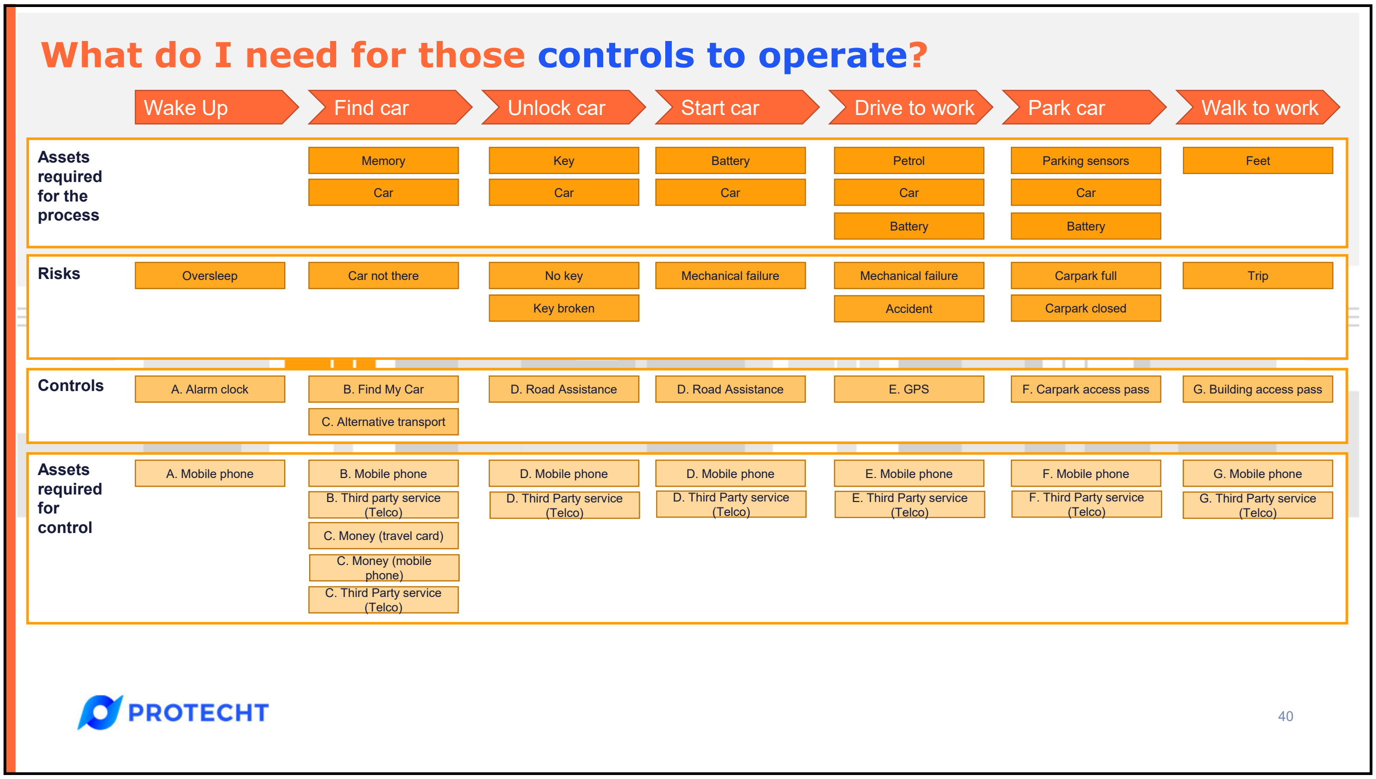
How do I mitigate those risks?

	Wake Up	Find car	Unlock car	Start car	Drive to work	Park car	Walk to work
Assets required for the process		Memory Car	Key Car	Battery Car	Petrol Car Battery	Parking sensors Car Battery	Feet
Risks	Oversleep	Car not there	No key Key broken	Mechanical failure	Mechanical failure Accident	Carpark full Carpark closed	Trip
Controls	A. Alarm clock	B. Find My Car C. Alternative transport	D. NRMA	D. NRMA	E. GPS	F. Carpark access pass	G. Building access pass

PROTECHT

39

38



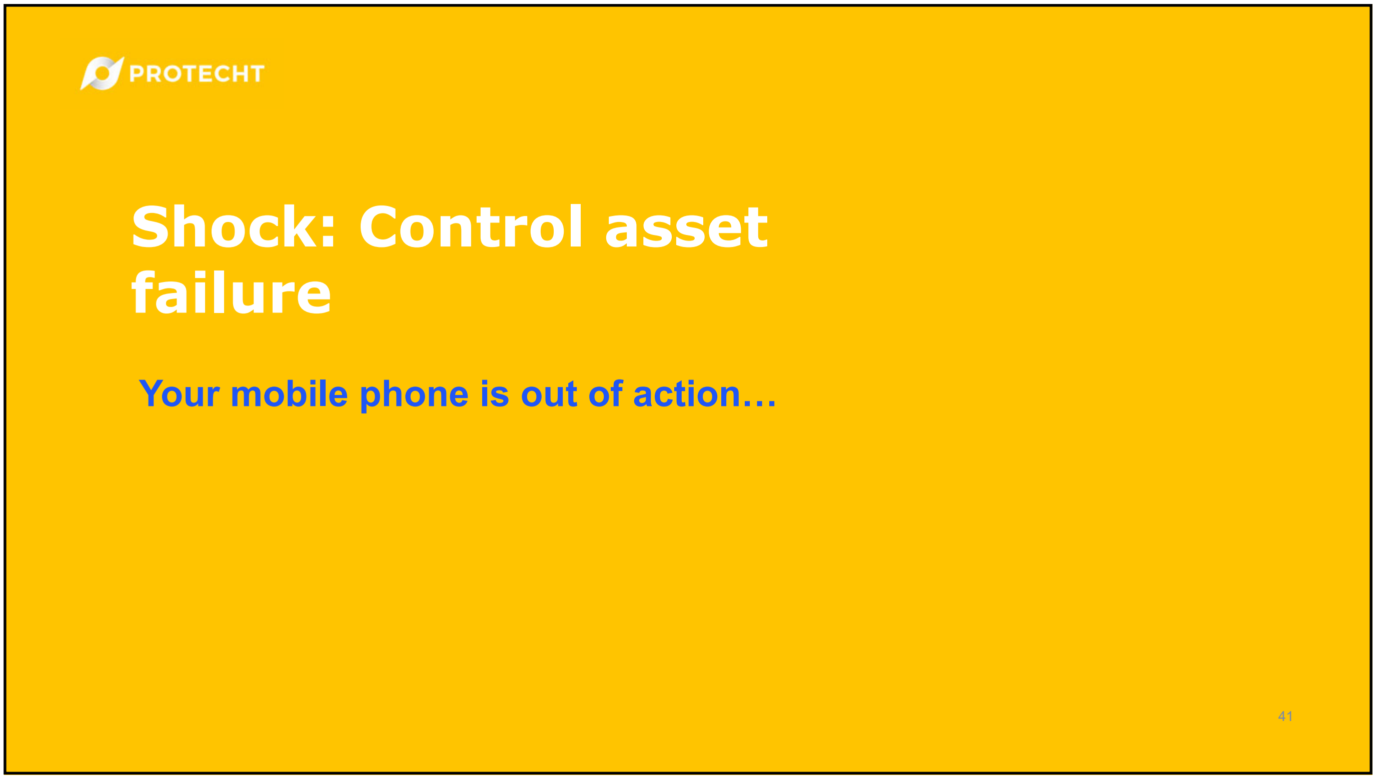
What do I need for those controls to operate?

	Wake Up	Find car	Unlock car	Start car	Drive to work	Park car	Walk to work
Assets required for the process		Memory Car	Key Car	Battery Car	Petrol Car Battery	Parking sensors Car Battery	Feet
Risks	Oversleep	Car not there	No key Key broken	Mechanical failure	Mechanical failure Accident	Carpark full Carpark closed	Trip
Controls	A. Alarm clock	B. Find My Car C. Alternative transport	D. Road Assistance	D. Road Assistance	E. GPS	F. Carpark access pass	G. Building access pass
Assets required for control	A. Mobile phone	B. Mobile phone B. Third party service (Telco) C. Money (travel card) C. Money (mobile phone) C. Third Party service (Telco)	D. Mobile phone D. Third Party service (Telco)	D. Mobile phone D. Third Party service (Telco)	E. Mobile phone E. Third Party service (Telco)	F. Mobile phone F. Third Party service (Telco)	G. Mobile phone G. Third Party service (Telco)

PROTECHT

40

39



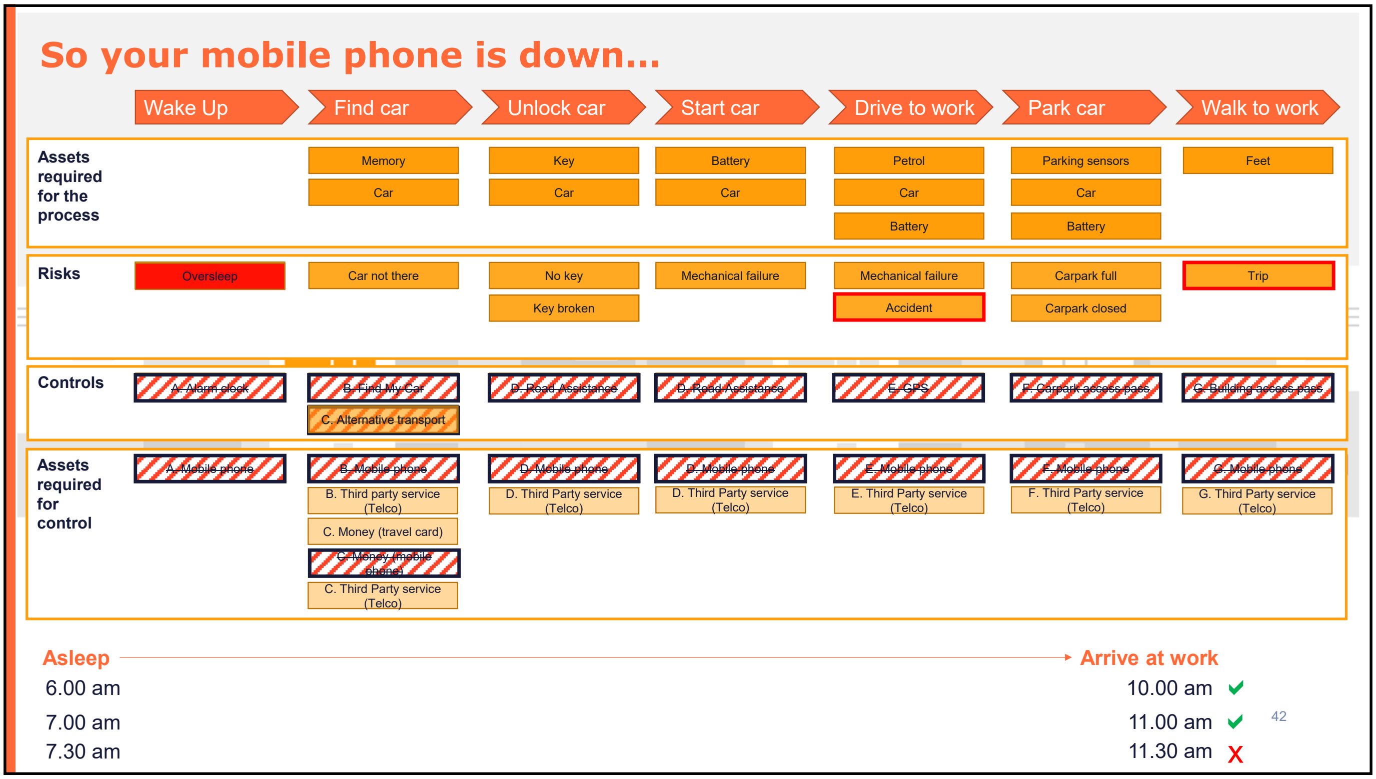
PROTECHT

Shock: Control asset failure

Your mobile phone is out of action…

41

40



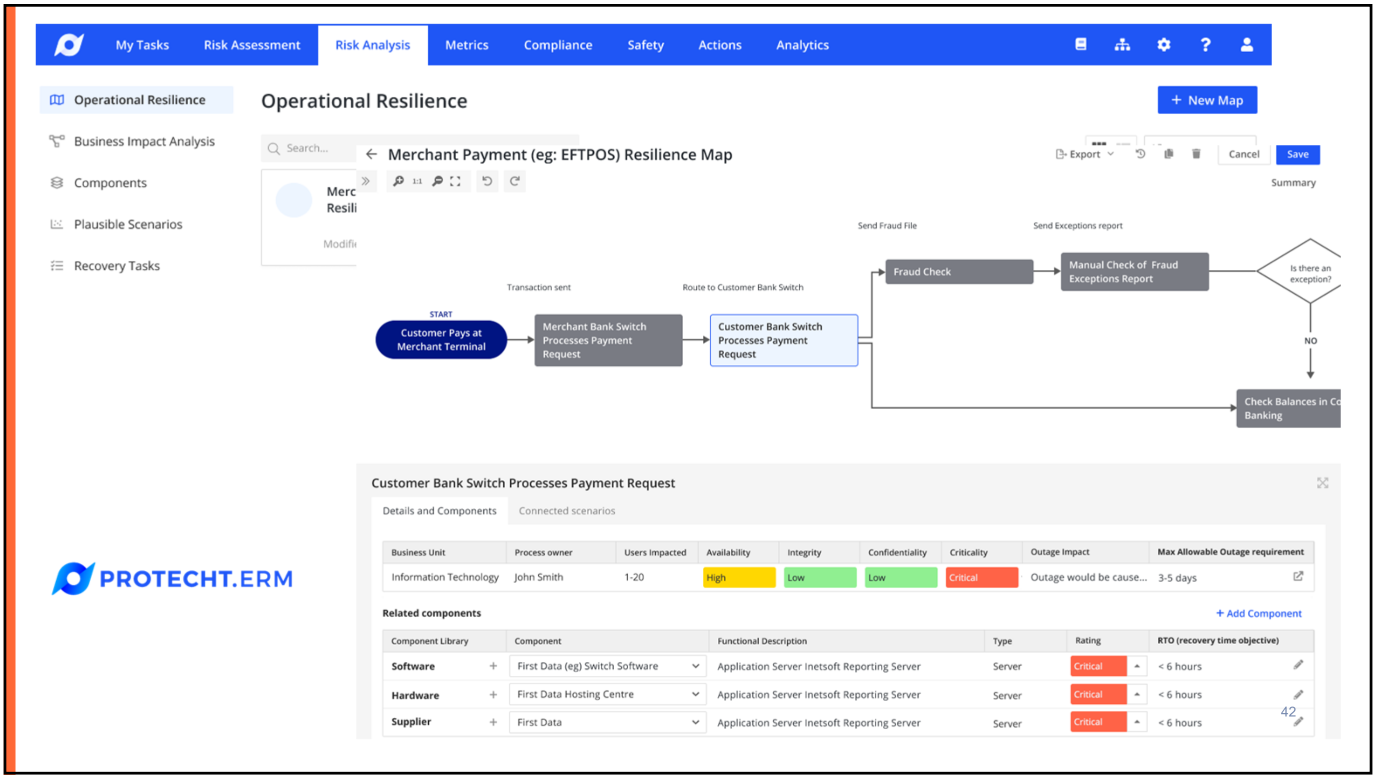
So your mobile phone is down…

	Wake Up	Find car	Unlock car	Start car	Drive to work	Park car	Walk to work
Assets required for the process		Memory Car	Key Car	Battery Car	Petrol Car Battery	Parking sensors Car Battery	Feet
Risks	Oversleep	Car not there	No key Key broken	Mechanical failure	Mechanical failure Accident	Carpark full Carpark closed	Trip
Controls	~~A. Alarm clock~~	~~B. Find My Car~~ C. Alternative transport	~~D. Road Assistance~~	~~D. Road Assistance~~	~~E. GPS~~	~~F. Carpark access pass~~	~~G. Building access pass~~
Assets required for control	~~A. Mobile phone~~	~~B. Mobile phone~~ B. Third party service (Telco) C. Money (travel card) ~~C. Money (mobile phone)~~ C. Third Party service (Telco)	~~D. Mobile phone~~ D. Third Party service (Telco)	~~D. Mobile phone~~ D. Third Party service (Telco)	~~E. Mobile phone~~ E. Third Party service (Telco)	~~F. Mobile phone~~ F. Third Party service (Telco)	~~G. Mobile phone~~ G. Third Party service (Telco)

Asleep	Arrive at work
6.00 am	10.00 am ✓
7.00 am	11.00 am ✓
7.30 am	11.30 am X

42

41



Operational Resilience

Merchant Payment (eg: EFTPOS) Resilience Map

START
Customer Pays at Merchant Terminal
Transaction sent
Merchant Bank Switch Processes Payment Request
Route to Customer Bank Switch
Customer Bank Switch Processes Payment Request
Send Fraud File
Fraud Check
Send Exceptions report
Manual Check of Fraud Exceptions Report
Is there an exception?
NO
Check Balances in C
Banking

Customer Bank Switch Processes Payment Request

Details and Components | Connected scenarios

Business Unit	Process owner	Users Impacted	Availability	Integrity	Confidentiality	Criticality	Outage Impact	Max Allowable Outage requirement
Information Technology	John Smith	1-20	High	Low	Low	Critical	Outage would be cause...	3-5 days

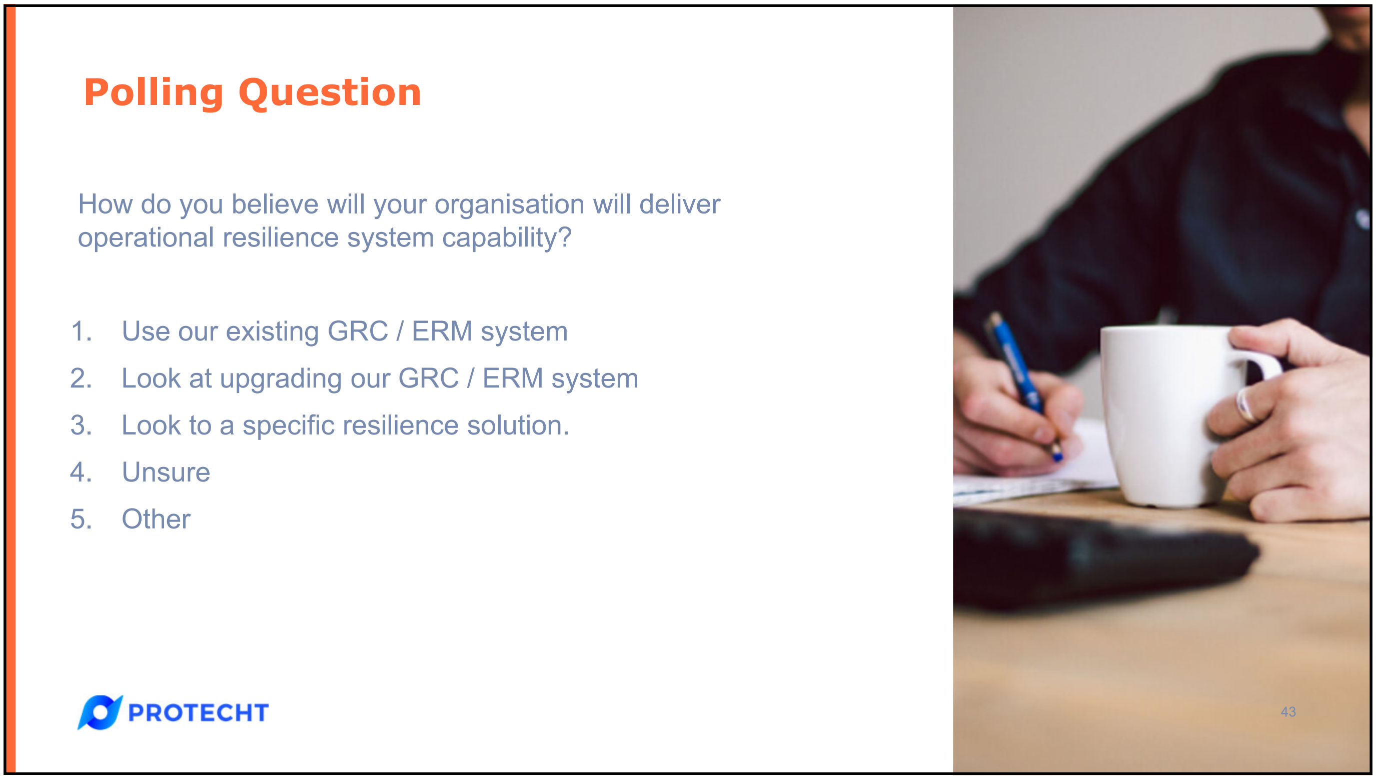
Related components

+ Add Component

Component Library	Component	Functional Description	Type	Rating	RTO (recovery time objective)
Software	First Data (eg) Switch Software	Application Server Inetsoft Reporting Server	Server	Critical	< 6 hours
Hardware	First Data Hosting Centre	Application Server Inetsoft Reporting Server	Server	Critical	< 6 hours
Supplier	First Data	Application Server Inetsoft Reporting Server	Server	Critical	< 6 hours

42

42



Polling Question

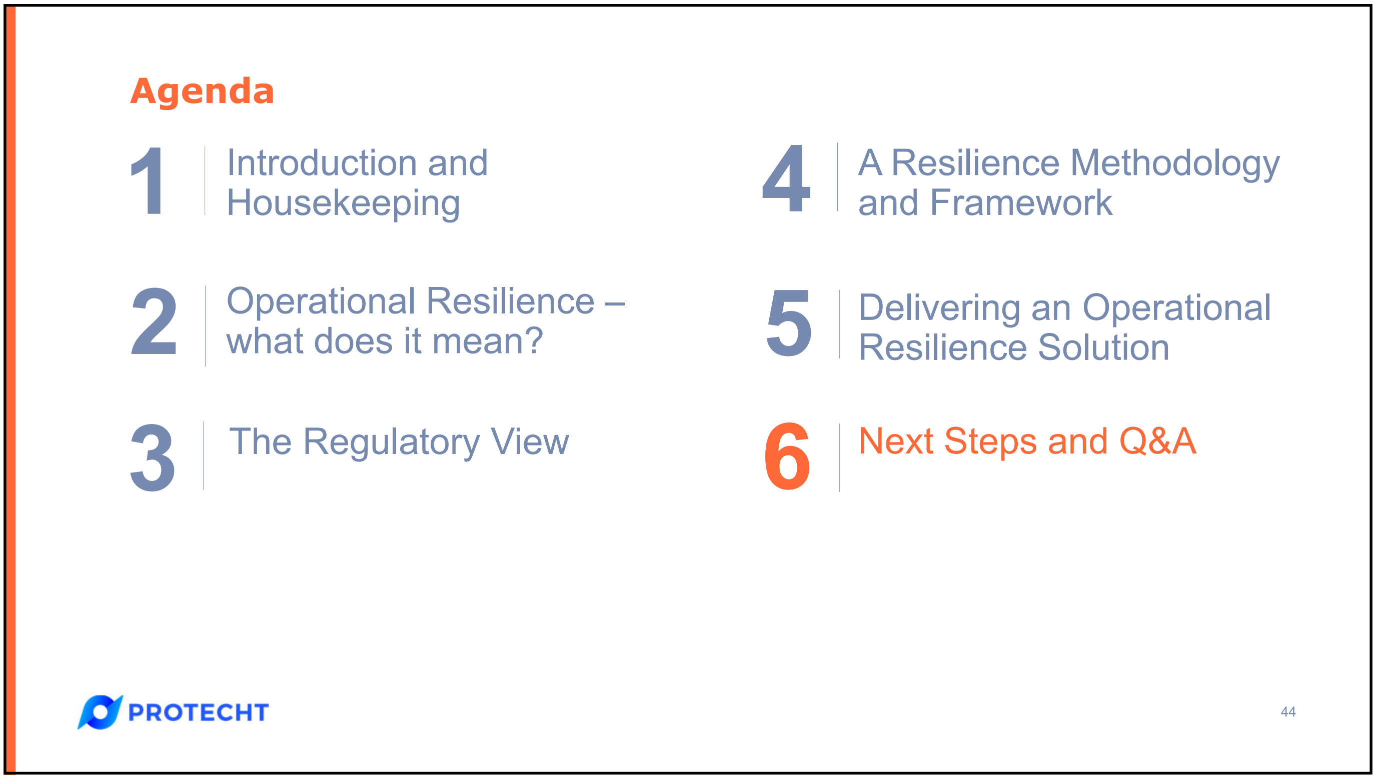
How do you believe will your organisation will deliver operational resilience system capability?

1. Use our existing GRC / ERM system
2. Look at upgrading our GRC / ERM system
3. Look to a specific resilience solution.
4. Unsure
5. Other

PROTECHT

43

43



Agenda

1 Introduction and Housekeeping

2 Operational Resilience – what does it mean?

3 The Regulatory View

4 A Resilience Methodology and Framework

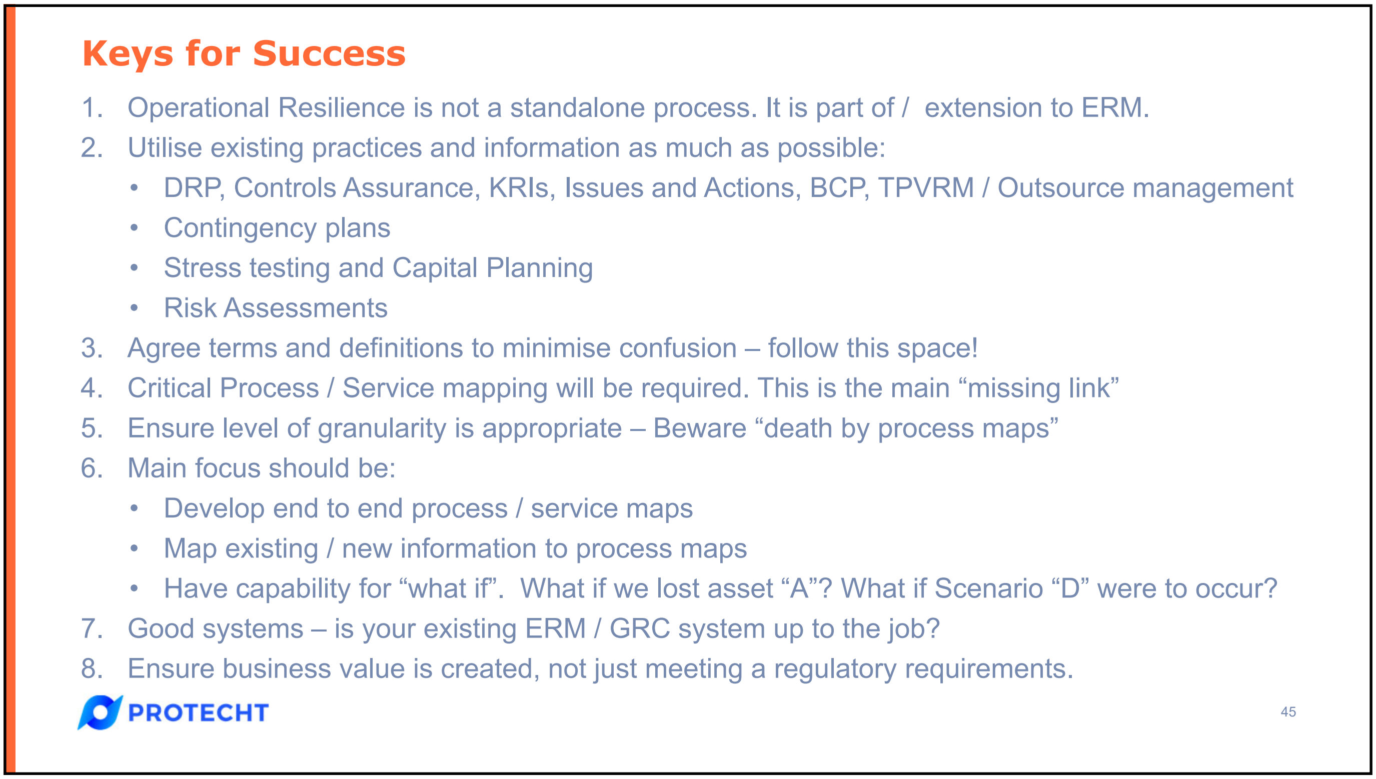
5 Delivering an Operational Resilience Solution

6 Next Steps and Q&A

PROTECHT

44

44

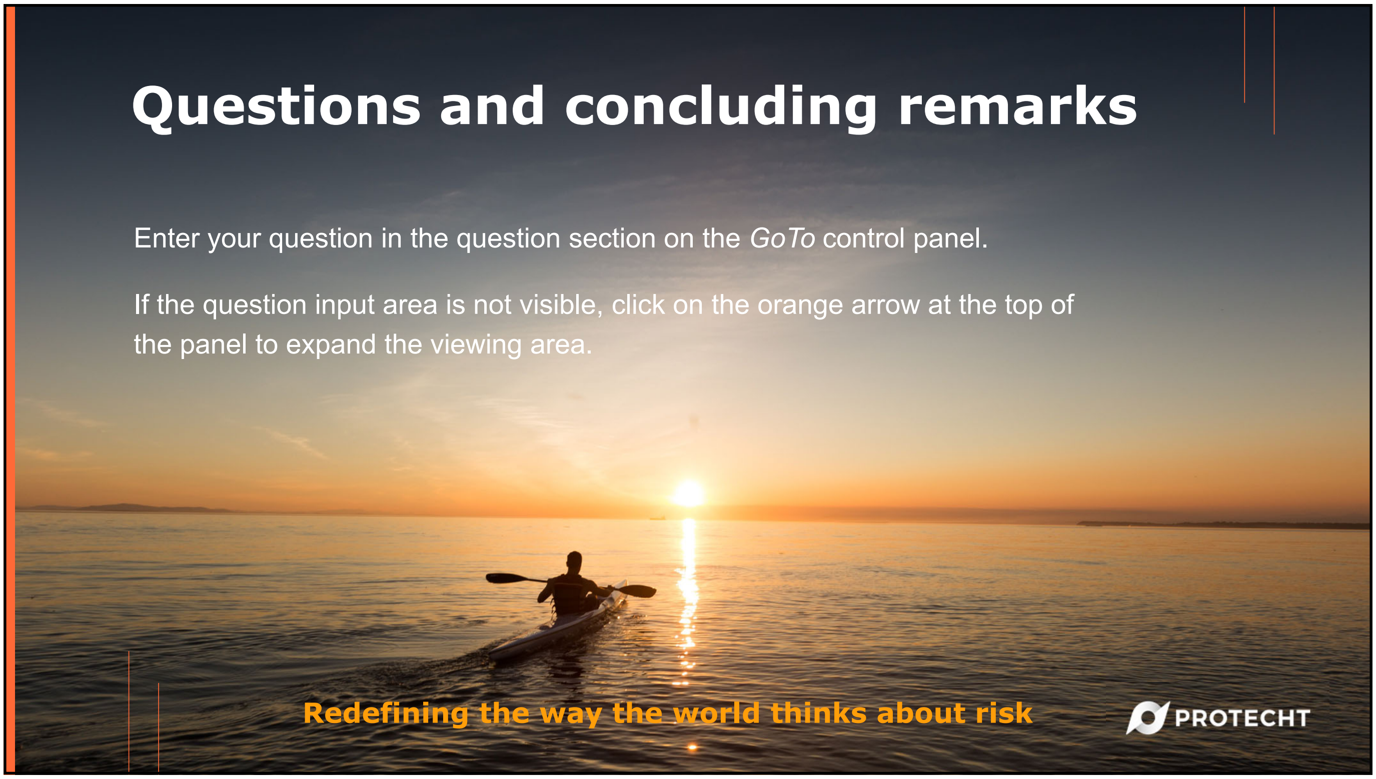


Keys for Success

1. Operational Resilience is not a standalone process. It is part of / extension to ERM.
2. Utilise existing practices and information as much as possible:
   - DRP, Controls Assurance, KRIs, Issues and Actions, BCP, TPVRM / Outsource management
   - Contingency plans
   - Stress testing and Capital Planning
   - Risk Assessments
3. Agree terms and definitions to minimise confusion – follow this space!
4. Critical Process / Service mapping will be required. This is the main “missing link”
5. Ensure level of granularity is appropriate – Beware “death by process maps”
6. Main focus should be:
   - Develop end to end process / service maps
   - Map existing / new information to process maps
   - Have capability for “what if”. What if we lost asset “A”? What if Scenario “D” were to occur?
7. Good systems – is your existing ERM / GRC system up to the job?
8. Ensure business value is created, not just meeting a regulatory requirements.

PROTECHT 45

45



Questions and concluding remarks

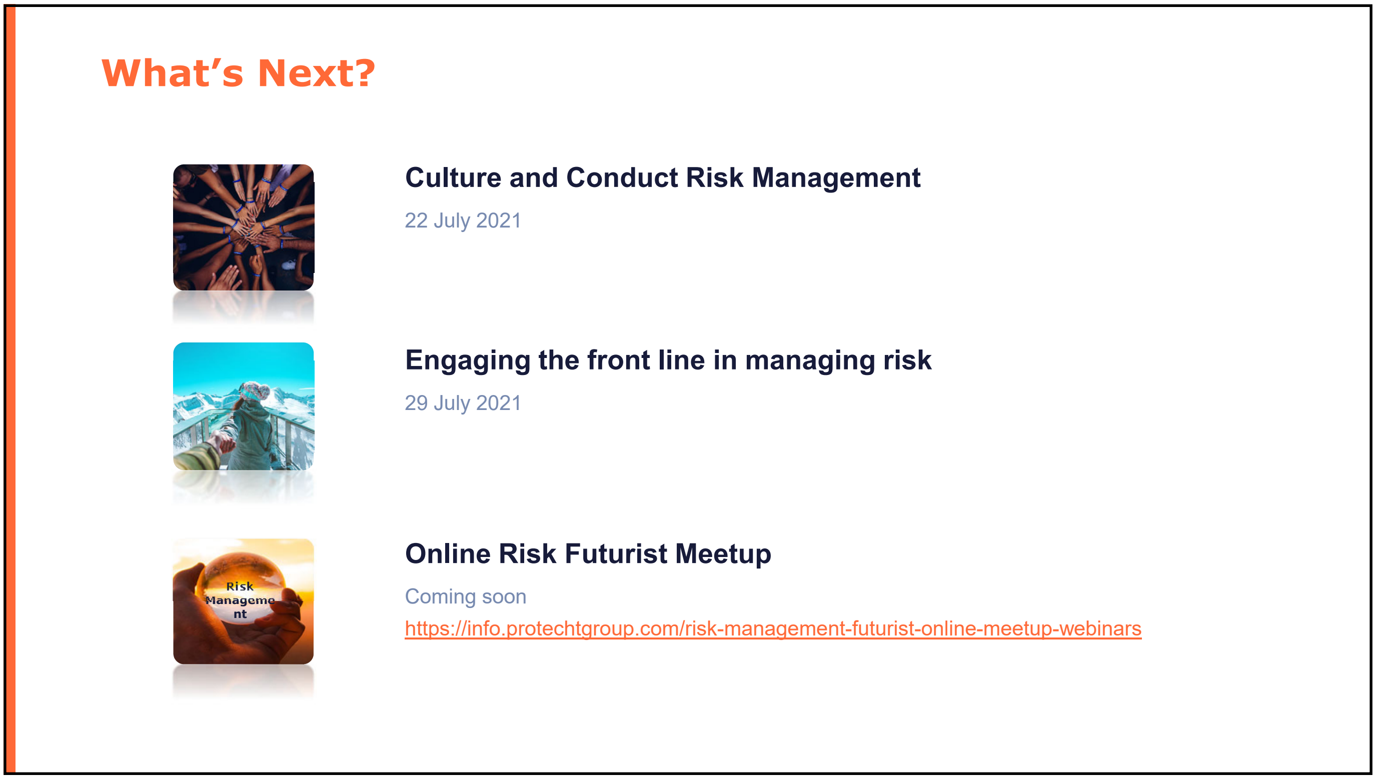
Enter your question in the question section on the *GoTo* control panel.

If the question input area is not visible, click on the orange arrow at the top of the panel to expand the viewing area.

Redefining the way the world thinks about risk

PROTECHT

46



What's Next?

Culture and Conduct Risk Management

22 July 2021

Engaging the front line in managing risk

29 July 2021

Online Risk Futurist Meetup

Coming soon

https://info.protechtgroup.com/risk-management-futurist-online-meetup-webinars

Risk
Manageme
nt

47

PROTECHT

Thank you!

david.tattam@protecht.com.au

Get in touch:

- UK, Europe & Middle East: +44 20 3978 1360
- Australia - Asia Pacific & Americas: +61 433 149 949

info@protechtgroup.com
www.protechtgroup.com/erm

48