



Operational Resilience: A Legacy Challenge

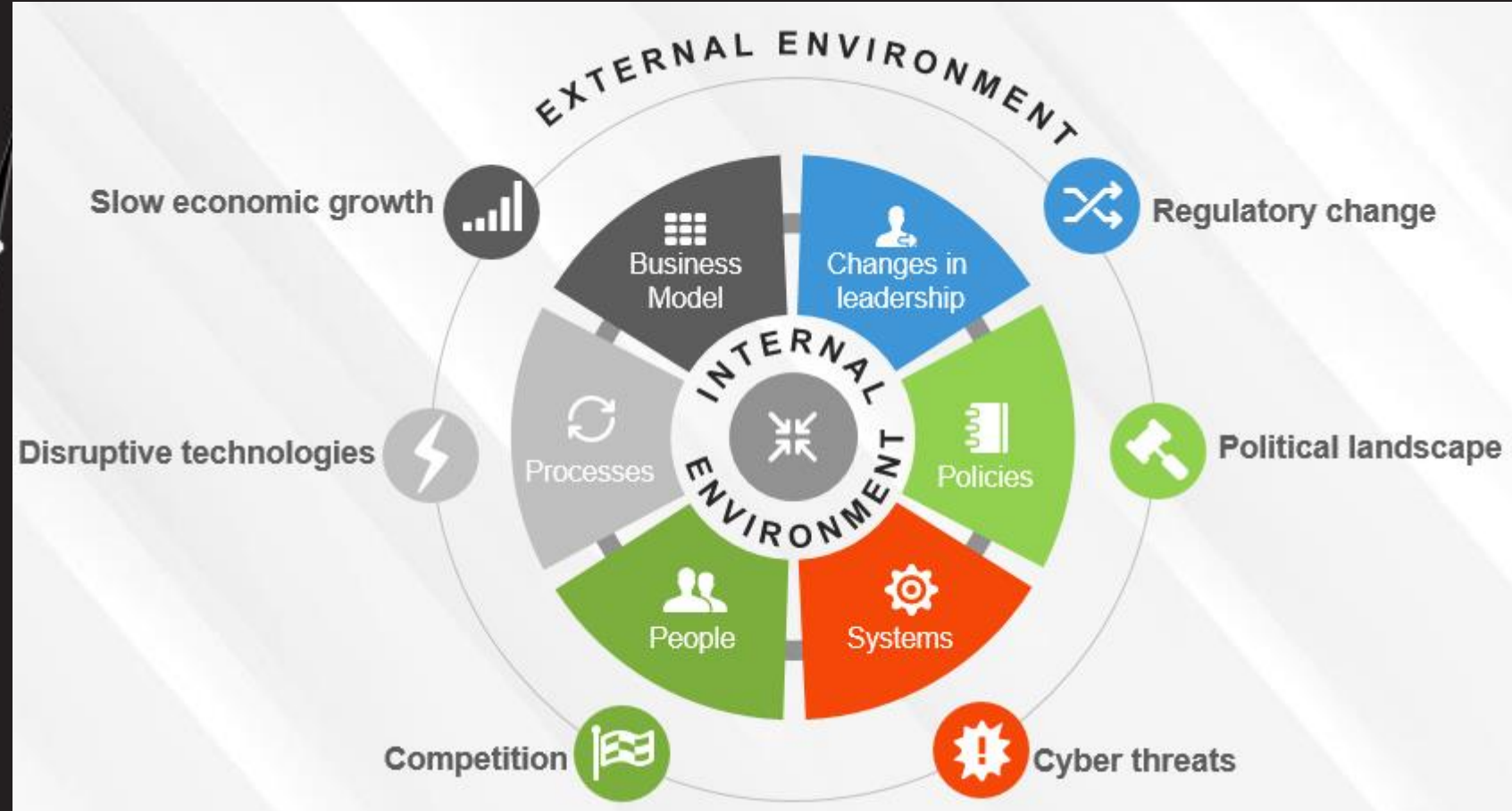
Qiniso Mthembu

JSE Senior Enterprise Risk Manager

09 December 2020

Value Creation & Value Preservation

Risk: The effect of uncertainty on objectives. The effect is the positive or negative deviation from what is expected. [ISO 31000:2018]



A Holistic Approach to Strategy, Risk & Resilience



The aim is to enable the organisation to proactively anticipate risks and opportunities and plan for coordinated response strategies, ensuring the achievement of objectives and long-term sustainability.

Operational Resilience: An Outcome

“Every battle is won before it is fought” – Sun Tzu, The Art of War

Operational Resilience: the ability of firms to continue to provide business services in the face of adverse events by anticipating, preventing, responding to, and adapting to such events.

Key Assumption: Failures are unavoidable & could be severe

Embedding of capabilities, processes, behaviors and systems

Goes beyond traditional disaster recovery and business continuity planning

Incremental changes to operating environment

Sudden Disruption

Sector alignment important

Why Now?

Drivers of exposure to disruption

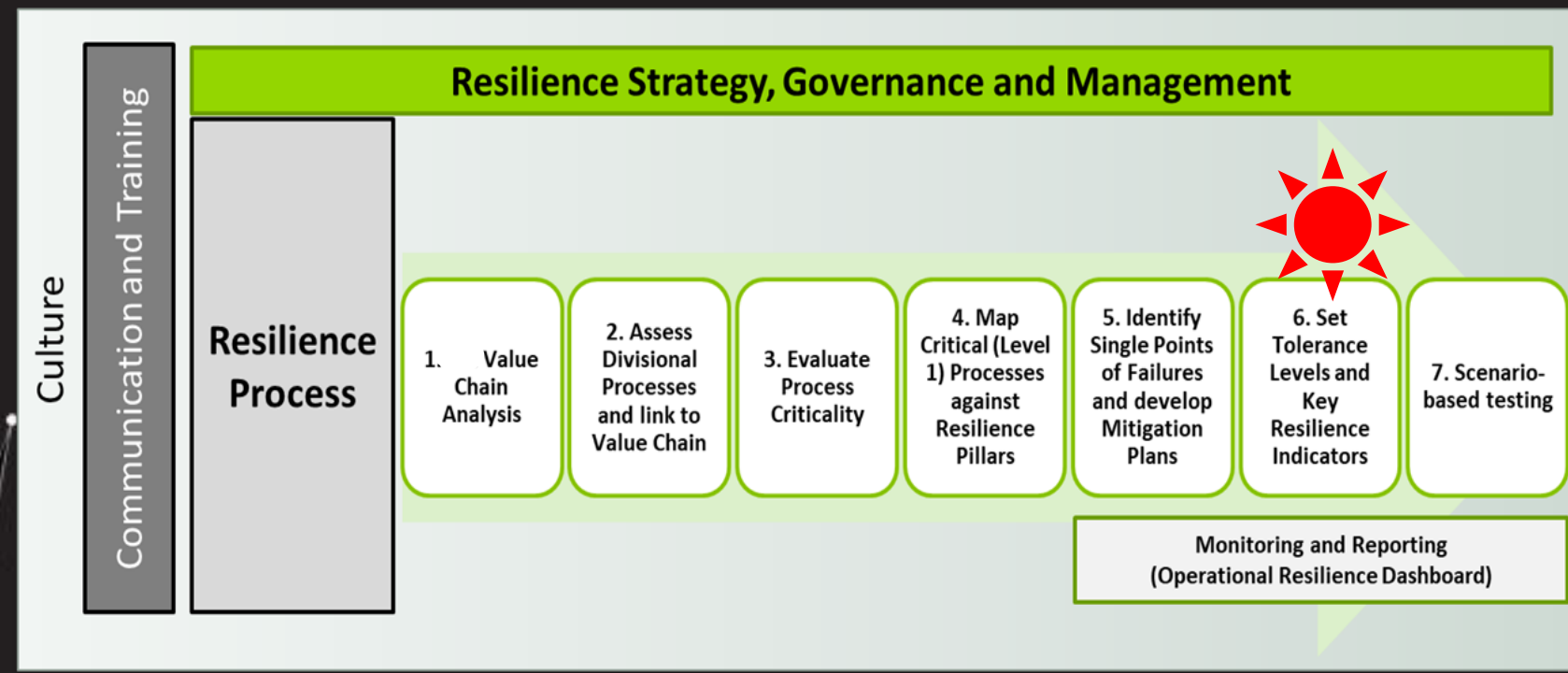
	DRIVER	IMPACT ON EXPOSURE TO DISRUPTION
SCALE AND PACE OF INNOVATION	Competition and customer demand are driving the need for more disruptive innovations and faster innovation cycles	Increasing complexity of processes and infrastructure required for product and service delivery, and risk of imbalance between time to market and security/resilience
CONTINUED DIGITIZATION	Availability of new technology, customer expectations, and desires for efficiency are driving increasing levels of automation and faster adoption of digital delivery capabilities	Traditional (manual) fallback methods no longer viable, and more challenging to identify the “weakest link” among connected digital systems
RELIANCE ON LEGACY INFRASTRUCTURE	Incumbent institutions rely on older technology infrastructure that is less flexible, requires specialized knowledge to maintain, and is difficult to integrate with new technologies and processes	Challenging to embed risk and resilience requirements in technology, which increases the exposure to disruptive events
EXTENSION OF THE SUPPLY CHAIN	Institutions are increasingly adopting outsourcing as a business strategy, expanding their reliance on third parties (and their third parties’ third parties)	More difficult to gain a comprehensive view of the firm’s third-party dependencies and exposure, as well as to assess the risk and resilience posture of all relevant third parties
INTERCONNECTEDNESS AND SHARING	Financial institutions are sharing more information and services more broadly (partly through deliberate government policy)	More likely to be affected by vulnerabilities and disruptions in another part of the ecosystem
CONTINUED RISE IN SOPHISTICATION OF MALICIOUS ACTORS	Cyber attackers are innovating rapidly to identify new means of attack and ways of exploiting firms’ vulnerabilities	More challenging to prevent, detect, respond, and recover from cyber attacks

Bend, But Don't Break

Get your house in order



“Resilient organizations focus on anticipation, prevention and adaptation, rather than recovery actions once the “horse has bolted.”



Operational Resilience Pillars



Impact Tolerances

“ The maximum tolerable level of disruption to an important business service, including the maximum tolerable duration of such a disruption.”



Assumes risks have crystallized

Measures should identify:

- Harm to consumers or market participants
- Harm to market integrity
- Threat to policyholder protection
- Threat to safety and soundness of the firm
- Threat to financial sustainability

Relate to a single disruption

?

How quickly can you recover – service continuity to end customer

Response focus: end-customer

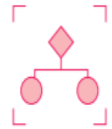
JS

Getting Started: Important Questions Boards & Senior Management Should Ask



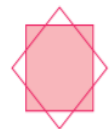
GOVERNANCE

- What is our risk appetite for resilience risk?
- What KRIs and KPIs provide us with a comprehensive view of our maturity and uplift program?
- Who is accountable in the 1st and 2nd lines of defense for managing, monitoring, and reporting on resilience?



ORGANIZATIONAL FOCUS

- Does the organization understand the dependencies of critical business services on organizational assets?
- What are our most critical assets that impact service delivery?
- How does our approach to resilience change the way we manage operations, technology, and third parties?



INTEGRATION

- What is our measure of criticality?
- What are our critical business services and why?
- How are we leveraging existing definitions of criticality and critical business services (e.g., from resolution planning)?
- What is our impact on customers and the financial system?



MEASUREMENT

- What are the most important resilience risks for the organization?
- How do we monitor and manage the level of resilience of the organization?
- How is risk appetite reflected in our impact tolerances?
- In which scenarios are we outside of our defined impact tolerances?



PREPAREDNESS

- How do we make sure we are effectively prepared for different disruption events?
- How frequently are we testing our response and recovery capabilities for different disruptive scenarios?

Getting Started: Key Steps For Establishing an Effective Operational Resilience Program

1. Establish the foundation	<ul style="list-style-type: none">• Assign accountability and develop an operating model for resilience• Conduct a resilience maturity assessment to establish a baseline of the organization's capabilities• Articulate the organization's critical business services
2. Provide visibility to the Board	<ul style="list-style-type: none">• Define the target resilience maturity ambition for the organization• Identify an initial set of metrics (including resilience program metrics) to provide ongoing reporting to the board
3. Focus on a single critical service	<ul style="list-style-type: none">• Run a pilot on one critical service to enhance resilience:<ul style="list-style-type: none">✓ Identify key dependencies and assess risks✓ Define impact tolerances and evaluate resilience through scenarios✓ Craft an improvement roadmap• Identify key learnings and program enhancements to facilitate the rollout of the program more broadly
4. Expand the program	<ul style="list-style-type: none">• Establish the program to drive resilience improvements based on lessons learned from the pilot and identified areas of enhancement• Expand the program to enhance capabilities and roll out a resilience approach across the remaining critical services

The Benefits



1.

Helps to align approach to operational resilience with strategic goals and navigate both the operational and the financial risks that emerge from increasingly complex and interconnected business models.

2.

Rapid recovery to deliver good customer outcomes leads to retention of customer trust and loyalty in increasingly competitive markets.

3.

Greater end-to-end focus on business services and clearer accountabilities based on such a focus should enable reduction of operational risks – both probability and impact of disruptions. The resultant benefits imply reduction in associated costs.

4.

Clearer understanding from mapping of business services and associated dependencies positions firm for greater efficiencies including confidence to take on more risk.

5.

Investment decisions based on what is most important to the continuity of key business services should ultimately reduce costs and contribute to competitive advantage.

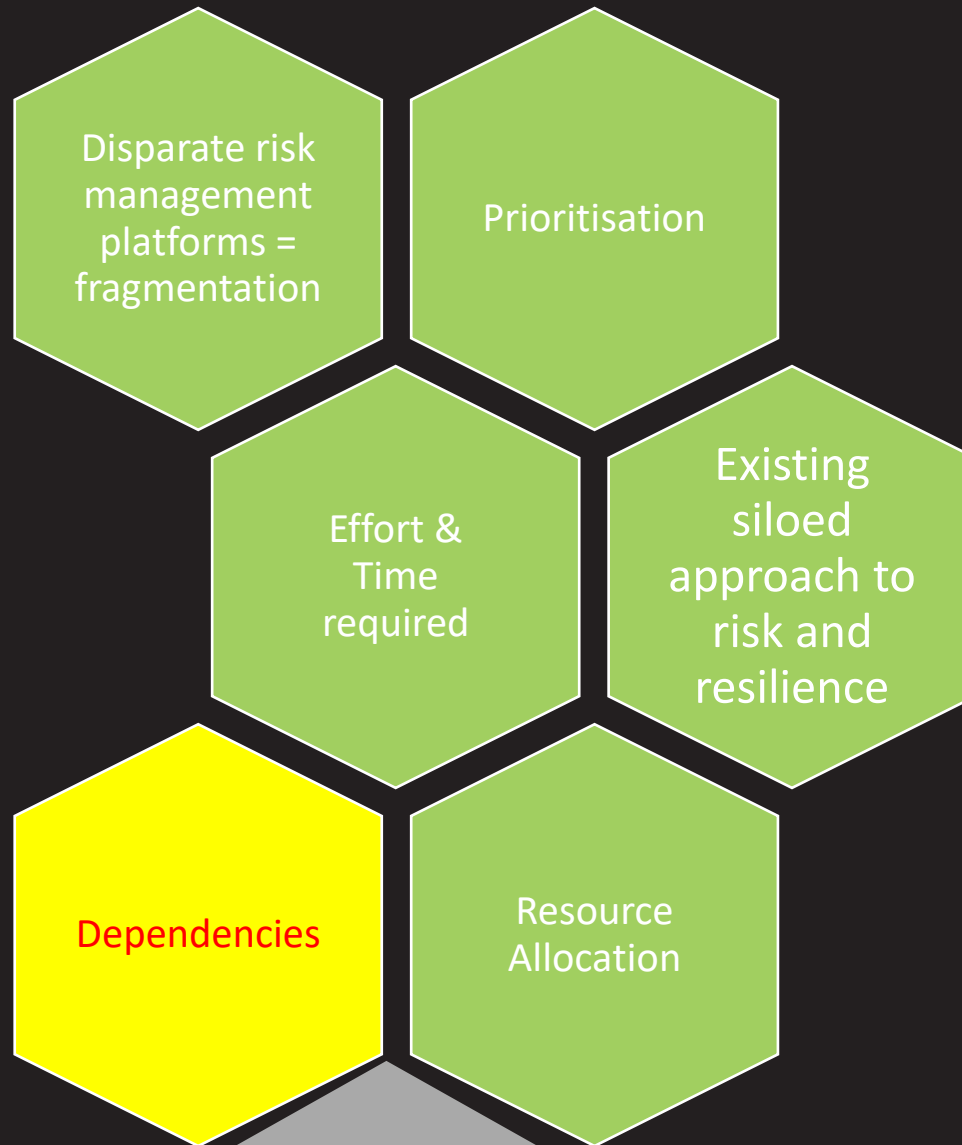
What do you see as the biggest challenge/s for implementing an operational resilience framework?



Challenges

*"I would like our firms to be on a WAR footing:
withstand, absorb, recover."*

Lyndon Nelson
Deputy CEO & Executive Director
Bank of England



**Resilience Maturity
Curve under-estimated**

Legacy Challenge to ESAAG

Strengthening governance in the East & Southern Africa Region through sound and effective public financial management in member countries.



Thank You



JS