Operational Resilience Measure and Report

26 Sept 2017

Lewis McKenzie | Andrew Charlton

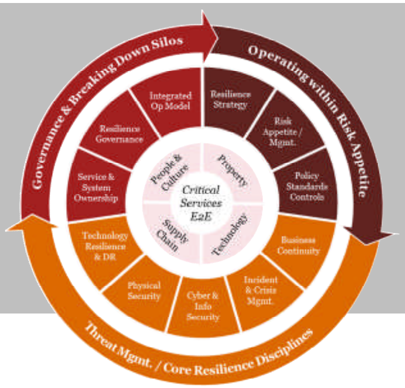
Evolution of Resilience Regulation

Regulatory Challenge

- Board accountability for critical infrastructure. Requirement for IT expertise on the board.
- End-to-end (E2E) resilience collaboration *vs* silo approach.
- Resilience requirements not as advanced as they should be [e.g. E2E mapping and testing of critical economic functions (CEFs)].
- Insufficient prioritisation in operationalising resilience requirements that have been identified.
- Greater appreciation for / demonstration of conduct considerations within IT Risk appetite.
- Maturity and delineation of 3LoD - risk and control management not keeping pace with newly emerging risks.
- Breadth of IT risk assessment activities *vs* individual service.
- Need for a better understanding of 3rd party dependencies and ensuring their compliance with the given organisation's conduct framework.
- Granularity of RTOs, including interdependencies.

Outcomes

- Increase in infrastructure reviews to address IT resilience. However, firms are not fully taking into account the need for resilience across the business.
- Confused granularity of metrics, compounded by a lack of clarity / consistency in key metric reporting.
- PwC development of the Operational Resilience Maturity Assessment tool (ORMA), utilising knowledge of Dear Chairman exercises.
- PwC development of Operational Resilience programme methodology and supporting tools.



The supervisory journey

Gamechanger

H1 2012

- Multiple incidents at several banks.

Q2 2012

- Payments outage at RBS affects 6.5m customers for up to a month.

Q3 2012

- FSA undertakes Dear Chairman Exercise making IT resilience a Board issue.

Validation/Learning

Q4 2012

- Board Chairpersons explain to FSA how they manage and control IT risk, and deliver DCE1 response.

Q2 2013

- FSA becomes PRA and FCA. Focus on IT resilience is sustained.

Regime response

Q3 2014

- European Supervisory Authority joint committee report identifies insufficient understanding of IT risks by regulators.

Q4 2014

- CHAPS RTGS outage highlights concentration risks in payment infrastructure.
- FCA / PRA fine RBS £56m.
- Banks respond to DCEII.
- SEC 'Flash Crash' proposals.

Supervision

H2 2015

- Private DCEII feedback to 7 participants. No market report was forthcoming from FCA / PRA.

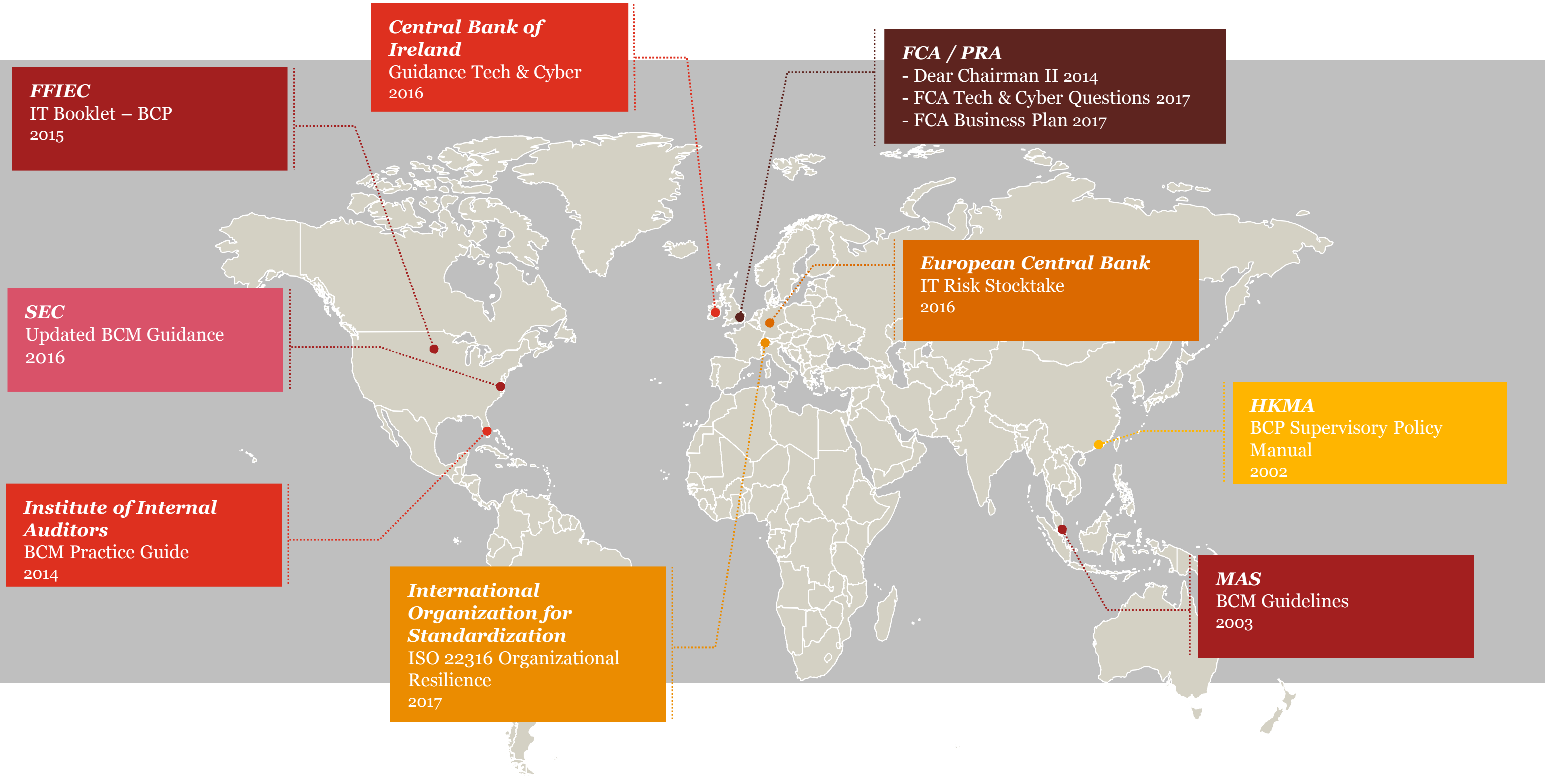
Today

- Supervisory focus on resilience at FCA / PRA and international regulators. Technology Resilience Questionnaire issued by FCA.

Regulatory Changes Worldwide

Global regulatory expectations and standards

- European regulators and international standards are now setting a **clear expectation** that organisations should make the **strategic shift** from BCM, recovery focused programmes to an integrated multi-disciplined end-to-end resilience approach, **with client and market impacts** as the **significant influencers**.



FFIEC
IT Booklet – BCP
2015

Central Bank of Ireland
Guidance Tech & Cyber
2016

FCA / PRA
- Dear Chairman II 2014
- FCA Tech & Cyber Questions 2017
- FCA Business Plan 2017

SEC
Updated BCM Guidance
2016

European Central Bank
IT Risk Stocktake
2016

HKMA
BCP Supervisory Policy Manual
2002

Institute of Internal Auditors
BCM Practice Guide
2014

International Organization for Standardization
ISO 22316 Organizational Resilience
2017

MAS
BCM Guidelines
2003

The Path to Resilience

	Siloed Continuity, Recovery & Planning			***Operational Resilience***	
	Undeveloped	**Formalised**	**Established**	**Integrated**	**Optimised**
Characteristics	Piecemeal and *ad hoc* plans, usually driven by a need to comply with legislation or regulation.	BCM policy is set, and business continuity plans developed for key sites and facilities.	Business Continuity is integrated with incident and crisis management, and emergency response. BCM is embedded in the organisation, with regular exercising.	Resilience analysis has been done across the organisational silos, taking into account supply and value chain dependencies and risks.	Resilience is integrated within the overall risk management approach, and is embedded within the corporate governance processes.
Metrics	Little evidence of metric guided BC. Metrics are minimal and fragmented.	Metrics have been formalised, but reporting / capture lacks consistency.	Mature set of metrics, but requires refinement to identify gaps and establish those metrics that are truly key.	The organisation has identified a set of KRIs with which to measure resilience.	KRIs inform key resilience decisions at all levels. KRIs are streamlined and manageable.
Ability to Respond	Minimum legal / regulatory requirements are met, but the ability to respond is patchy and uncertain.	Key sites and facilities can respond to major incidents and they should be able to reduce the disruption to their operations.	Response capabilities are optimised at a site level and their ability to recover operations is reasonably certain and efficient.	Key business priorities are understood, and the organisation can implement a strategic response to disruptions, across its sites and supply chain.	Investment in resilience and risk is optimised, and the organisation has sustained capability to respond to major threats.

Minimal —— ***Resilience Level*** —— ***High***

End-to-End Operational Resilience – The Journey

Resilience Trajectory

Stages

Phases

Benefits

Identify Critical Services (CS) & set Governance

CS selection should take into account services identified as systemic by the regulator, as well as the following four areas:

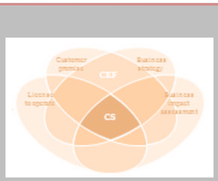
(1) License to Operate

(2) Customer Promise

(3) Business Strategy

(4) Business Impact Assessment

1



Identify & Select

Critical Services

- Knowing what matters most to the bank
- Well-understood priorities
- Ownership established
- Quicker decision making in crises

You are here…

Define Risk Appetite & top-down KPIs & KRIs

Define risk appetite for the CS (including the channels that make up the CS) by utilising prioritised service tiers; assign thresholds for KRIs based on this tiering.

2

Risk Appetite and KRIs

- Driven by risk appetite and performance
- Linked into Risk Management
- Resilience across siloed activities
- Meeting regulatory expectations

Mapping

The CS and principle channels are mapped out, identifying the critical path through activities. The four pillars of service capability (People, Premises, 3rd Parties, and Technnology) are mapped against each activity on the critical path.

3

End-to-End Mapping

- Understanding of value chain
- Critical path identified
- Key dependencies and their owners identified
- Single points of failure and concentration of risk identified

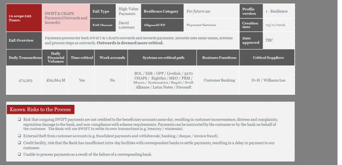
Assessment

Risk assessment leverages reproducible, consistent methodology, delineated through execution of the initial programme. This approach provides an overall risk profile and gap analysis; risks, summaries, and overall ratings are mapped for each service.

Assessing KRIs – KRIs are applied across the critical path to help identify risk hot-spots (both vulnerabilities and dependencies).

4

Measure & Assess



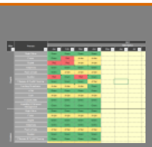
Metrics that count

- Direct link between KRIs and risk appetite
- Ability to drill down and diagnose issues relating to service delivery
- Cross-cutting analyses provide pillars with business impact data
- Ability to assess forward looking indicators to anticipate problems
- Combination and extension of existing metrics for efficiency

Reporting & Remediation

Reporting will enable the bank to make informed decisions regarding remediation actions spanning the organisation.

5



Reporting & Controls

Insight and Action

- Overall Resilience dashboard
- Controls applied at best point
- Integration with risk management
- Joined up top-to-bottom view
- Follows regulatory direction
- Timeliness of action
- Efficiency of investment

Stage 1:
Identify Critical Services (CS) & set Governance

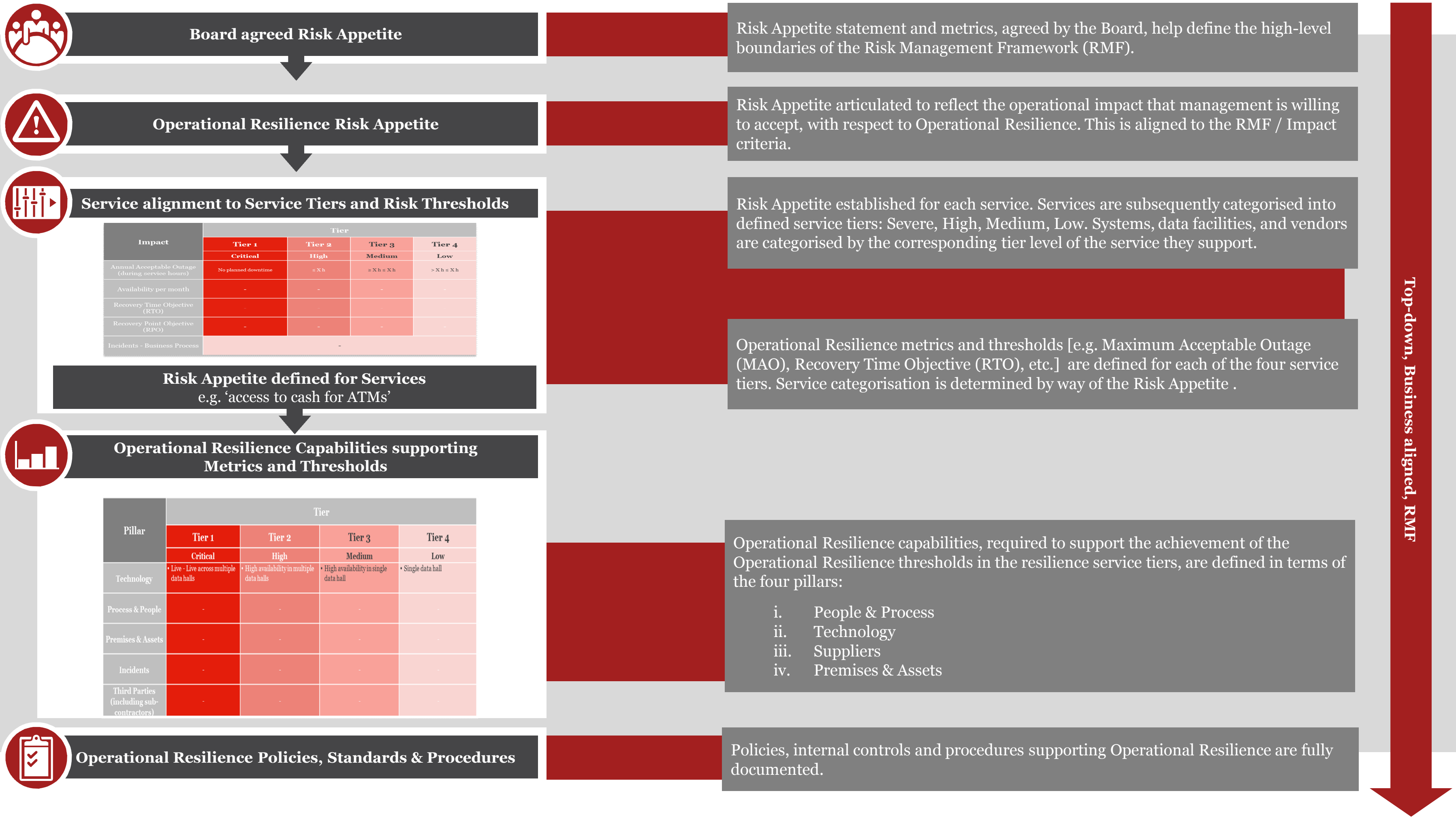
Stage 2:
Define Risk Appetite & top-down KPIs & KRIs

Stage 3:
Mapping

Stage 4:
Assessment

Stage 5:
Reporting & Controls

Stage 2 – Define Risk Appetite & Top-Down KPIs & KRIs



Board agreed Risk Appetite

Risk Appetite statement and metrics, agreed by the Board, help define the high-level boundaries of the Risk Management Framework (RMF).

Operational Resilience Risk Appetite

Risk Appetite articulated to reflect the operational impact that management is willing to accept, with respect to Operational Resilience. This is aligned to the RMF / Impact criteria.

Service alignment to Service Tiers and Risk Thresholds

Impact	Tier			
	Tier 1	Tier 2	Tier 3	Tier 4
	Critical	High	Medium	Low
Annual Acceptable Outage (during service hours)	No planned downtime	≤ X h	≥ X h ≤ X h	> X h ≤ X h
Availability per month	-	-	-	-
Recovery Time Objective (RTO)	-	-	-	-
Recovery Point Objective (RPO)	-	-	-	-
Incidents - Business Process	-			

Risk Appetite defined for Services
e.g. ‘access to cash for ATMs’

Risk Appetite established for each service. Services are subsequently categorised into defined service tiers: Severe, High, Medium, Low. Systems, data facilities, and vendors are categorised by the corresponding tier level of the service they support.

Operational Resilience metrics and thresholds [e.g. Maximum Acceptable Outage (MAO), Recovery Time Objective (RTO), etc.] are defined for each of the four service tiers. Service categorisation is determined by way of the Risk Appetite .

Operational Resilience Capabilities supporting Metrics and Thresholds

Pillar	Tier			
	Tier 1	Tier 2	Tier 3	Tier 4
	Critical	High	Medium	Low
Technology	• Live - Live across multiple data halls	• High availability in multiple data halls	• High availability in single data hall	• Single data hall
Process & People	-	-	-	-
Premises & Assets	-	-	-	-
Incidents	-	-	-	-
Third Parties (including sub-contractors)	-	-	-	-

KPIs and KRIs are set in parallel with tiers and thresholds so that generated MI is succinct, specific, and relevant.

Operational Resilience capabilities, required to support the achievement of the Operational Resilience thresholds in the resilience service tiers, are defined in terms of the four pillars:

i. People & Process
ii. Technology
iii. Suppliers
iv. Premises & Assets

Operational Resilience Policies, Standards & Procedures

Policies, internal controls and procedures supporting Operational Resilience are fully documented.

Stage 4 – Assessment

Risk profile

- The **Critical Process owner** is responsible for the completion of the **Gap Analysis** using data validated through the workshop, risks that sit within the risk portal, and KRIs.
- Once approved this should be shared with the organisation's Resilience team for their oversight and collation into a central repository.

In scope E2E Name:	SWIFT & CHAPS Payments	**E2E Type**	High-Value Payments	**Resilience Category**	Tier 1	**Profile version**	1 - Resilience
		E2E Owner	A.N.Other	**Aligned CEF**	Payment Services	**Creation date**	01/01/0000
E2E Overview	Payments process for both SWIFT & CHAPS outwards and inwards payments. Inwards uses same teams, systems and process steps as outwards. **Outwards is deemed more critical.**					**Date approved**	01/01/0000

Daily Transactions	Daily Financial Volumes	Time critical	Work arounds	Systems on critical path	Business Functions	Critical Suppliers
xxx	xxx	xx	xx	xxxx	xxxx	xxxxx

Known Risks to the Process

- ❑ Risk 1
- ❑ Risk 2
- ❑ Risk 3

Example Output: Board Risk Profile

Stage 5 – Reporting & Remediation

The KRIs utilise data from across the 4 pillars of resilience, this data can be fed in to the reporting dashboard to provide 3 views. From the process level the data can be aggregated to provide monthly and quarterly reporting and YTD trend analysis.

People

Premises

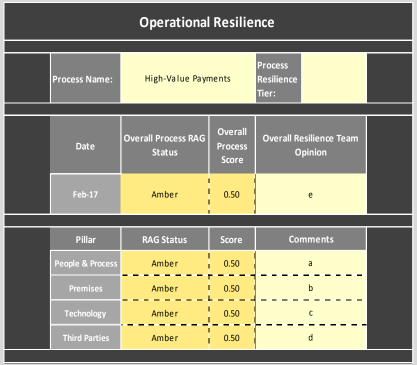
Suppliers

Technology

DATA

KRIs across 4 pillars inform MI summary

While the 4 pillars provide a mutually exclusive and comprehensive segmentation of the business, we understand that many organisations may align their focus differently. PwC methodology and tools are customisable to your needs.



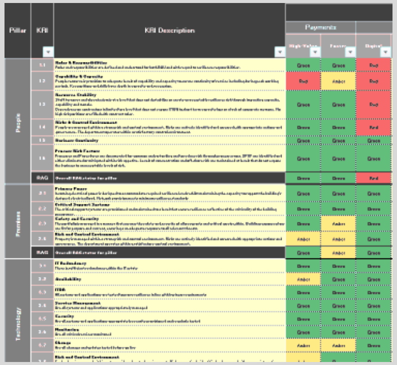
Operational Resilience

Process Name:	High-Value Payments	Process Resilience Tier:	

Date	Overall Process RAG Status	Overall Process Score	Overall Resilience Team Opinion
Feb-17	Amber	0.50	e

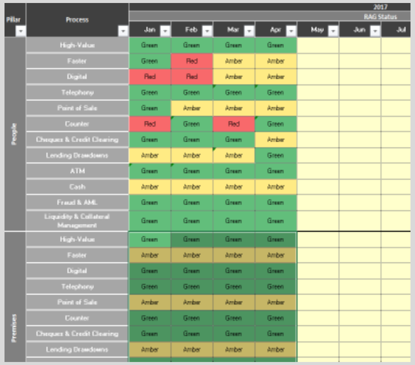
Pillar	RAG Status	Score	Comments
People & Process	Amber	0.50	a
Premises	Amber	0.50	b
Technology	Amber	0.50	c
Third Parties	Amber	0.50	d

Process Level



Pillar	KRI	KRI Description	Payments High-Value	 Faster	 Digital
People	1.1	Roles & Responsibilities [illegible]	Green	Green	Red
	1.2	Capability & Capacity [illegible]	Red	Amber	Red
	1.3	Resource Stability [illegible]	Green	Green	Red
	1.4	Risk & Control Environment [illegible]	Green	Green	Red
	1.5	Business Continuity	Green	Green	Green
	1.6	Process Risk Factors [illegible]	Green	Green	Green
	RAG	Overall RAG status for pillar	Green	Green	Red
Premises	2.1	Primary Power [illegible]	Green	Green	Green
	2.2	Critical Support Systems [illegible]	Green	Green	Green
	2.3	Safety and Security [illegible]	Green	Amber	Green
	2.4	Risk and Control Environment [illegible]	Amber	Amber	Green
	RAG	Overall RAG status for pillar	Green	Amber	Green
Technology	3.1	IT Redundancy [illegible]	Green	Green	Green
	3.2	Availability	Amber	Green	Green
	3.3	ITDR [illegible]	Green	Green	Green
	3.4	Service Management [illegible]	Green	Green	Green
	3.5	Security [illegible]	Green	Green	Green
	3.6	Resilience [illegible]	Green	Green	Green
	3.7	Change [illegible]	Amber	Amber	Green
	3.8	Risk and Control Environment [illegible]	[illegible]	[illegible]	[illegible]

Monthly Aggregation



Pillar	Process	2017 RAG Status Jan	 Feb	 Mar	 Apr	 May	 Jun	 Jul
People	High-Value	Green	Green	Green	Green			
	Faster	Green	Red	Amber	Amber			
	Digital	Red	Red	Amber	Amber			
	Telephony	Green	Green	Green	Green			
	Point of Sale	Green	Amber	Amber	Amber			
	Counter	Red	Green	Red	Green			
	Cheques & Credit Clearing	Green	Green	Green	Amber			
	Lending Drawdowns	Amber	Amber	Amber	Green			
	ATM	Green	Green	Green	Green			
	Cash	Amber	Amber	Amber	Amber			
	Fraud & AML	Green	Green	Green	Green			
	Liquidity & Collateral Management	Green	Green	Green	Green			
Premises	High-Value	Green	Green	Green	Green			
	Faster	Amber	Amber	Amber	Amber			
	Digital	Green	Green	Green	Green			
	Telephony	Green	Green	Green	Green			
	Point of Sale	Amber	Amber	Amber	Amber			
	Counter	Green	Green	Green	Green			
	Cheques & Credit Clearing	Green	Green	Green	Green			
	Lending Drawdowns	Amber	Amber	Amber	Amber			

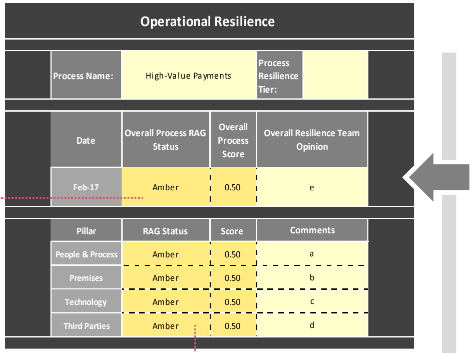
YTD Trends

Dashboards of relevant granularity provide audience appropriate MI

Gradual aggregation of data provides a **reliable view** of organisational resilience, and presents a dependable methodology that **ensures accuracy of data** reported

Stage 5 – Reporting & Remediation

Process Level



Operational Resilience

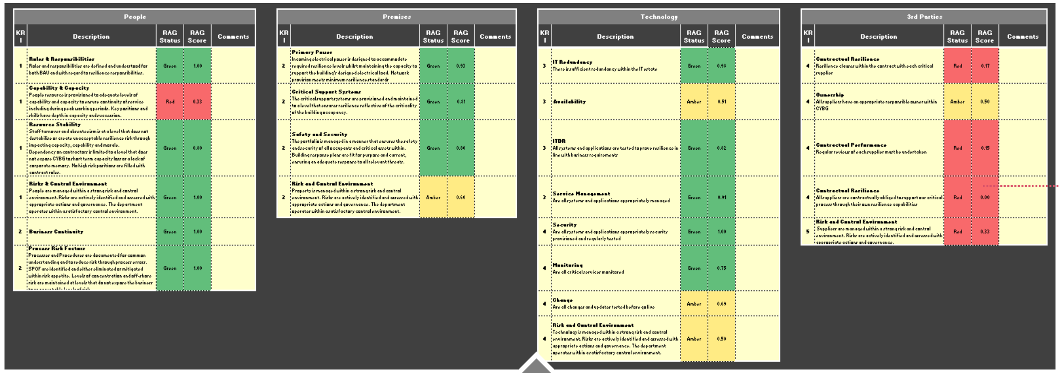
Process Name:	High-Value Payments	Process Resilience Tier:	

Date	Overall Process RAG Status	Overall Process Score	Overall Resilience Team Opinion
Feb-17	Amber	0.50	e

Pillar	RAG Status	Score	Comments
People & Process	Amber	0.50	a
Premises	Amber	0.50	b
Technology	Amber	0.50	c
Third Parties	Amber	0.50	d

Overall RAG **status of Process**

Overall RAG **status of each Pillar**



People

KRI	Description	RAG Status	RAG Score	Comments
1	**Roles & Responsibilities** Roles and responsibilities are defined and understood for both BAU and with regard to resilience responsibilities.	Green	1.00	
1	**Capability & Capacity** People resource is provisioned to adequate levels of capability and capacity to ensure continuity of service including during peak working periods. Key positions and skills have depth in capacity and succession.	Red	0.33	
1	**Resource Stability** Staff turnover and absenteeism is at a level that does not destabilise or create unacceptable resilience risk through impacting capacity, capability and morale. Dependency on contractors is limited to a level that does not expose CYBG to short term capacity loss or a lack of corporate memory. No high risk positions are filled with contract roles.	Green	0.80	
1	**Risks & Control Environment** People are managed within a strong risk and control environment. Risks are actively identified and assessed with appropriate actions and governance. The department operates within a satisfactory control environment.	Green	1.00	
2	**Business Continuity**	Green	1.00	
2	**Process Risk Factors** Processes and Procedures are documented for common understanding and to reduce risk through process errors. SPOF are identified and either eliminated or mitigated within risk appetite. Levels of concentration and off-shore risk are maintained at levels that do not expose the business	Green	1.00	

Premises

KRI	Description	RAG Status	RAG Score	Comments
2	**Primary Power** Incoming electrical power is designed to accommodate required resilience levels whilst maintaining the capacity to support the building's designed electrical load. Network provision meets minimum resilience standards	Green	0.93	
2	**Critical Support Systems** The critical support systems are provisioned and maintained to a level that ensures resilience reflective of the criticality of the building occupancy.	Green	0.81	
2	**Safety and Security** The portfolio is managed in a manner that ensures the safety and security of all occupants and critical assets within. Building response plans are fit for purpose and current, ensuring an adequate response to all relevant threats.	Green	0.80	
2	**Risk and Control Environment** Property is managed within a strong risk and control environment. Risks are actively identified and assessed with appropriate actions and governance. The department operates within a satisfactory control environment.	Amber	0.60	

Technology

KRI	Description	RAG Status	RAG Score	Comments
3	**IT Redundancy** There is sufficient redundancy within the IT estate	Green	0.98	
3	**Availability**	Amber	0.51	
3	**ITDR** All systems and applications are tested to prove resilience in line with business requirements	Green	0.82	
3	**Service Management** Are all systems and applications appropriately managed	Green	0.91	
4	**Security** Are all systems and applications appropriately security provisioned and regularly tested	Green	1.00	
4	**Monitoring** Are all critical services monitored	Green	0.75	
4	**Change** Are all changes and updates tested before go live	Amber	0.69	
4	**Risk and Control Environment** Technology is managed within a strong risk and control environment. Risks are actively identified and assessed with appropriate actions and governance. The department operates within a satisfactory control environment.	Amber	0.50	

3rd Parties

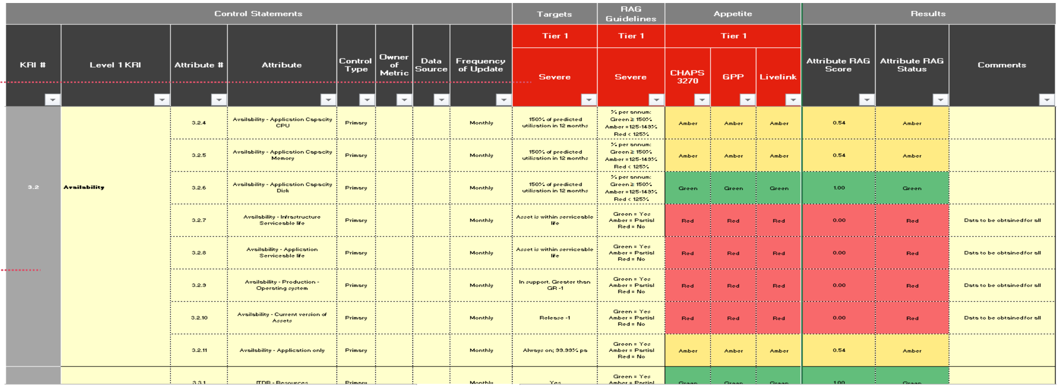
KRI	Description	RAG Status	RAG Score	Comments
4	**Contractual Resilience** Resilience clauses within the contract with each critical supplier	Red	0.17	
4	**Ownership** All suppliers have an appropriate responsible owner within CYBG	Amber	0.50	
4	**Contractual Performance** Regular reviews of each supplier must be undertaken	Red	0.15	
4	**Contractual Resilience** All suppliers are contractually obliged to support our critical process through their own resilience capabilities	Red	0.00	
5	**Risk and Control Environment** Suppliers are managed within a strong risk and control environment. Risks are actively identified and assessed with appropriate actions and governance.	Red	0.33	

KRI RAGs broken down by Pillar **simple, digestible format**

Pillar assessments that are **segmented appropriately**:

- People = Teams
- Premises = Location
- Technology = Systems
- 3rd Party = Suppliers

KRIs defined by a set of Attributes. Individual RAG scores per attribute allow you to quickly identify problem areas / gaps

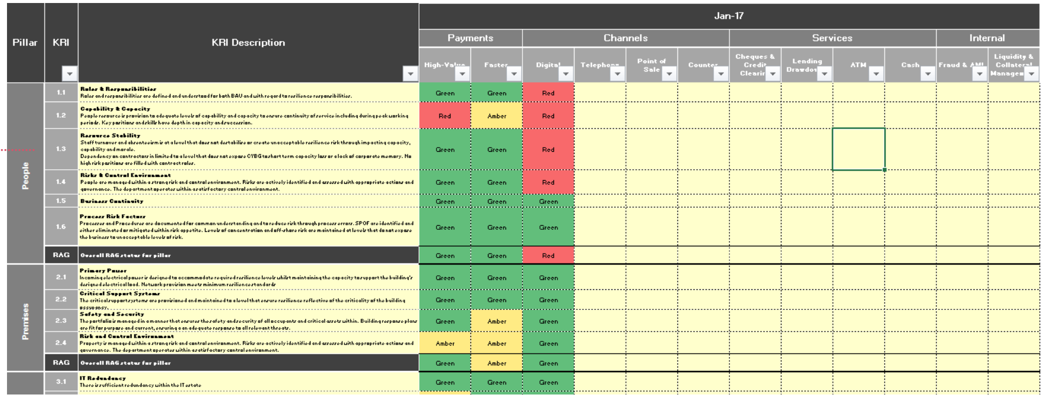


Control Statements								Targets	RAG Guidelines	Appetite			Results		
								Tier 1	Tier 1	Tier 1					
KRI #	Level 1 KRI	Attribute #	Attribute	Control Type	Owner of Metric	Data Source	Frequency of Update	Severe	Severe	CHAPS 3270	GPP	Livelink	Attribute RAG Score	Attribute RAG Status	Comments
3.2	**Availability**	3.2.4	Availability - Application Capacity CPU	Primary			Monthly	150% of predicted utilisation in 12 months	% per annum: Green ≥ 150% Amber = 125-149% Red < 125%	Amber	Amber	Amber	0.54	Amber	
		3.2.5	Availability - Application Capacity Memory	Primary			Monthly	150% of predicted utilisation in 12 months	% per annum: Green ≥ 150% Amber = 125-149% Red < 125%	Amber	Amber	Amber	0.54	Amber	
		3.2.6	Availability - Application Capacity Disk	Primary			Monthly	150% of predicted utilisation in 12 months	% per annum: Green ≥ 150% Amber = 125-149% Red < 125%	Green	Green	Green	1.00	Green	
		3.2.7	Availability - Infrastructure Serviceable life	Primary			Monthly	Asset is within serviceable life	Green = Yes Amber = Partial Red = No	Red	Red	Red	0.00	Red	Data to be obtained for all
		3.2.8	Availability - Application Serviceable life	Primary			Monthly	Asset is within serviceable life	Green = Yes Amber = Partial Red = No	Red	Red	Red	0.00	Red	Data to be obtained for all
		3.2.9	Availability - Production - Operating system	Primary			Monthly	In support. Greater than GR -1	Green = Yes Amber = Partial Red = No	Red	Red	Red	0.00	Red	Data to be obtained for all
		3.2.10	Availability - Current version of Assets	Primary			Monthly	Release -1	Green = Yes Amber = Partial Red = No	Red	Red	Red	0.00	Red	Data to be obtained for all
		3.2.11	Availability - Application only	Primary			Monthly	Always on; 99.99% pa	Green = Yes Amber = Partial Red = No	Amber	Amber	Amber	0.54	Amber	
		3.3.1	ITDR - Resources	Primary			Monthly	Yes	Green = Yes Amber = Partial	Green	Green	Green	1.00	Green	

Stage 5 – Reporting & Remediation

Monthly Aggregation

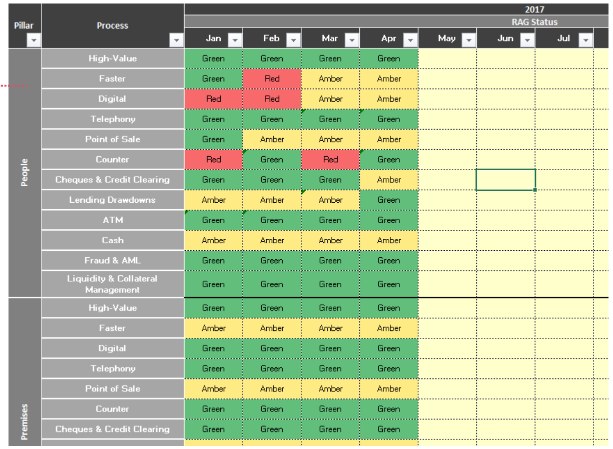
Monthly view across critical processes, aligning each process to specific functions



Pillar	KRI	KRI Description	Jan-17											
			Payments		Channels				Services				Internal	
			High-Value	Faster	Digital	Telephone	Point of Sale	Counter	Cheques & Credit Clearing	Lending Drawdowns	ATM	Cash	Fraud & AML	Liquidity & Collateral Management
People	1.1	**Roles & Responsibilities** Roles and responsibilities are defined and understood for both BAU and with regard to resilience responsibilities.	Green	Green	Red									
	1.2	**Capability & Capacity** People resource is provision to adequate levels of capability and capacity to ensure continuity of service including during peak working periods. Key positions and skills have depth in capacity and succession.	Red	Amber	Red									
	1.3	**Resource Stability** Staff turnover and absenteeism is at a level that does not destabilise or create unacceptable resilience risk through impacting capacity, capability and morale. Dependency on contractors in limited to a level that does not expose CYBG to short term capacity loss or a lack of corporate memory. No high risk positions are filled with contract roles.	Green	Green	Red									
	1.4	**Risks & Control Environment** People are managed within a strong risk and control environment. Risks are actively identified and assessed with appropriate actions and governance. The department operates within a satisfactory control environment.	Green	Green	Red									
	1.5	**Business Continuity**	Green	Green	Green									
	1.6	**Process Risk Factors** Processes and Procedures are documented for common understanding and to reduce risk through process errors. SPOF are identified and either eliminated or mitigated within risk appetite. Levels of concentration and off-shore risk are maintained at levels that do not expose the business to unacceptable levels of risk.	Green	Green	Green									
	RAG	**Overall RAG status for pillar**	Green	Green	Red									
Premises	2.1	**Primary Power** Incoming electrical power is designed to accommodate required resilience levels whilst maintaining the capacity to support the building's designed electrical load. Network provision meets minimum resilience standards	Green	Green	Green									
	2.2	**Critical Support Systems** The critical support systems are provisioned and maintained to a level that ensure resilience reflective of the criticality of the building occupancy.	Green	Green	Green									
	2.3	**Safety and Security** The portfolio is managed in a manner that ensures the safety and security of all occupants and critical assets within. Building response plans are fit for purpose and current, ensuring a an adequate response to all relevant threats.	Green	Amber	Green									
	2.4	**Risk and Control Environment** Property is managed within a strong risk and control environment. Risks are actively identified and assessed with appropriate actions and governance. The department operates within a satisfactory control environment.	Amber	Amber	Green									
	RAG	**Overall RAG status for pillar**	Green	Amber	Green									
	3.1	**IT Redundancy** There is sufficient redundancy within the IT estate	Green	Green	Green									

YTD Trends

Quickly identify emerging trends in your resilience portfolio using aggregated data from your monthly assessments



Pillar	Process	2017						
		RAG Status						
		Jan	Feb	Mar	Apr	May	Jun	Jul
People	High-Value	Green	Green	Green	Green			
	Faster	Green	Red	Amber	Amber			
	Digital	Red	Red	Amber	Amber			
	Telephony	Green	Green	Green	Green			
	Point of Sale	Green	Amber	Amber	Amber			
	Counter	Red	Green	Red	Green			
	Cheques & Credit Clearing	Green	Green	Green	Amber			
	Lending Drawdowns	Amber	Amber	Amber	Green			
	ATM	Green	Green	Green	Green			
	Cash	Amber	Amber	Amber	Amber			
	Fraud & AML	Green	Green	Green	Green			
	Liquidity & Collateral Management	Green	Green	Green	Green			
Premises	High-Value	Green	Green	Green	Green			
	Faster	Amber	Amber	Amber	Amber			
	Digital	Green	Green	Green	Green			
	Telephony	Green	Green	Green	Green			
	Point of Sale	Amber	Amber	Amber	Amber			
	Counter	Green	Green	Green	Green			
	Cheques & Credit Clearing	Green	Green	Green	Green			

Remediation

- Prioritisation – MI dashboards provide a means to identify those areas that require immediate attention
- Repeat Issues – automated 90 day RAG statuses allow the resilience team to make a fairer assessment on the state of a given resilience area
- Investment – MI reporting in this way allows the organisation to distribute its investment into the most relevant areas

Stage 1:
Identify Critical Services (CS) & set Governance

Stage 2:
Define Risk Appetite & top-down KPIs & KRIs

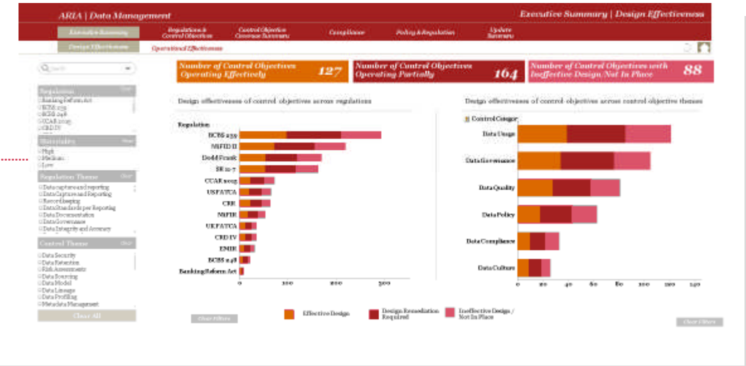
Stage 3:
Mapping

Stage 4:
Assessment

Stage 5:
Reporting & Controls

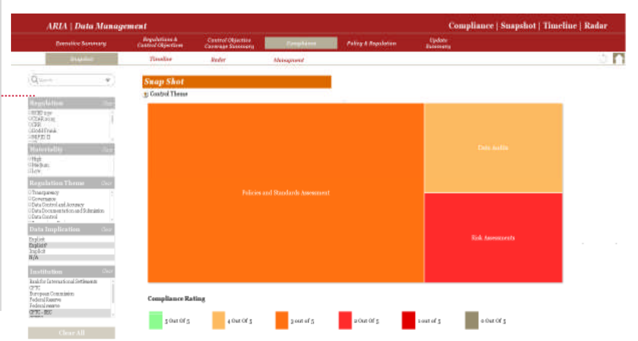
Stage 5 – Reporting & Remediation – Dashboards

Easy-Interpret Metrics



Pivot data at the touch of a button without fear of scrambling data

Audience Specific



Quickly identify emerging trends in your resilience in a format that can be tailored easily to different audiences

Benefits

- Disseminate data without the need for static reporting
- Identify trends using dynamic data arrays
- Instant visualisation in a plethora of chart types, matrices, etc.
- Minimises exposure to editable data

This publication has been prepared for general guidance on matters of interest only, and does not constitute professional advice. You should not act upon the information contained in this publication without obtaining specific professional advice. No representation or warranty (express or implied) is given as to the accuracy or completeness of the information contained in this publication, and, to the extent permitted by law, PricewaterhouseCoopers LLP, its members, employees and agents do not accept or assume any liability, responsibility or duty of care for any consequences of you or anyone else acting, or refraining to act, in reliance on the information contained in this publication or for any decision based on it.

© 2017 PricewaterhouseCoopers LLP. All rights reserved. In this document, "PwC" refers to PricewaterhouseCoopers LLP (a limited liability partnership in the United Kingdom) which is a member firm of PricewaterhouseCoopers International Limited, each member firm of which is a separate legal entity.