Operational Resilience Maturity Assessment

Overview

Dec 2020

TORI perspective on Operational Resilience

Operational Resilience (OR) is all encompassing. It must be embedded as a mindset through ways of working and reinforced through culture and behaviours. While Regulation has yet to come into force, now is the time to act: clients are demanding assurance on security and resilience; OR now forms part of the Auditor's toolkit and; significant effort is needed to demonstrate the required direction of travel.

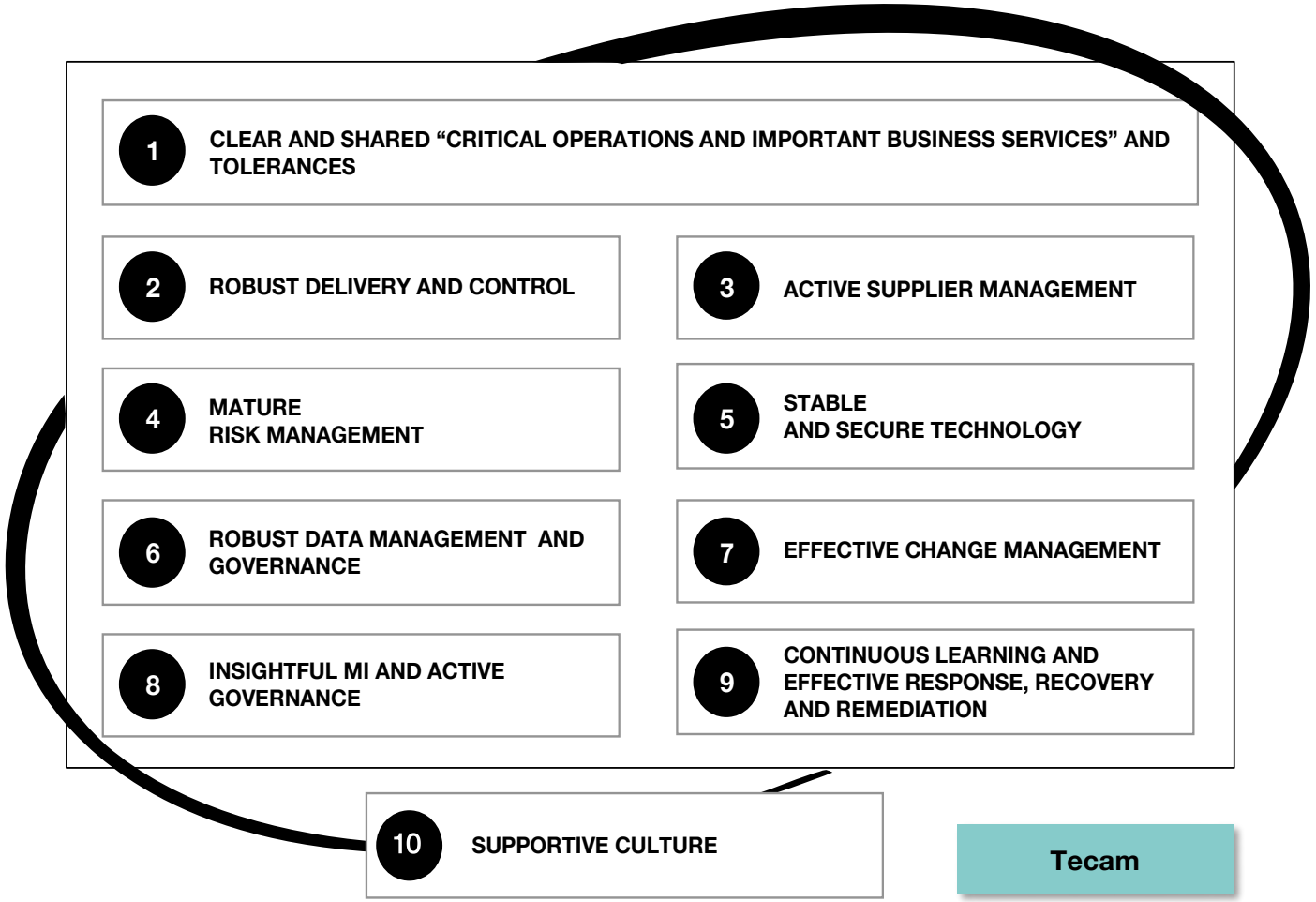
While the UK is arguably leading the way on OR (Bank of England, PRA and FCA) other regulatory jurisdictions are now coming to the table with their own frameworks and interpretations (EBA, Basel, MAS, Federal Reserve for example). For firms with an international footprint, the breadth of regulation (and divergence across jurisdictions) adds a further dimension which must be addressed - to leverage standard ways of working where possible but at the same time demonstrate conformance with jurisdictional nuances as needed. Similarly, OR regulatory commitments must effectively dove-tail with other commitments such as SMCR, SMF24, GDPR and EBA.

Regulators are adopting a pragmatic approach and understand that 'one-size-fits-all' will not produce the right outcomes. The approach is one of proportionality (size and complexity of the business plus potential systemic risk) and, by way of impact assessment and scenario planning, 'severe but plausible' i.e. there is a recognition that not all risk can or should be mitigated but it needs to be understood by reference to risk appetite and managed accordingly. In some instances, it will be acceptable and in fact necessary, to work outside of risk appetite (to avoid business, market and/or client detriment). Clear line of sight and dynamic management of risks in a crisis is the key. The use of frameworks, tooling and data to provide an end-to-end 'lookthrough' across the business is paramount. Governance, behaviours, analytics and testing are key components to deliver a sustainable Operational Resilience framework.

TORI brings a wealth of OR experience having worked first-hand with the Bank of England and the PRA. We have also supported clients with OR readiness assessments and as part of this work have developed a comprehensive Operational Resilience Maturity Assessment, delivered and facilitated on-line via a proprietary tool, TECAM. TECAM quickly captures a baseline and gap analysis by reference to regulatory requirements to inform scope and prioritisation for the subsequent OR programme. TECAM also identifies processes, tools and artefacts that can be re-purposed and re-used. Furthermore, it can be used to capture end-to-end process flows from which Standard Operating Policies and Procedures are auto-generated, ensuring a one-to-one interlock between documented processes and 'real world' BAU operations. A powerful aide to support attestation.

TORI's Operational Resilience Maturity Assessment Tool

TORI's Operational Resilience Maturity Assessment Tool comprises 10 components, each reviewed and profiled during the assessment:



Commentary

Meeting the requirement to demonstrate Operational Resilience requires more than the traditional approach to security and Business continuity - although both these areas remain important.

The requirement is complex, since it cuts across traditionally recognised business lines, across entities and also jurisdictions.

Whilst it is clear that any framework for operational resilience is predicated upon a clear, accurate and complete identification of "critical operations and important business services" (as per regulatory guidance) TORI believe that this is simply the starting point and that a more mature approach requires encompassing additional views.

TORI has developed a profiling tool comprising 10 components, which represent these views and poses key questions to assess the maturity of those components or to identify gaps.

We believe that a framework incorporating these components which are robust and effective, is the evidence needed to demonstrate mature Operational Resilience.

Delivery: method

The delivery method of our OR Maturity Assessment service recognises the broad and deep scope of Operational Resilience. There are 5 delivery activities as part of the assessment, set out below. All 5 activities are recommended for larger and more complex assessments. In other cases, clients prefer to run only assessment workshops, or others to run just surveys.

1. Mobilisation. Not strictly part of the assessment, but a key foundational activity. Within this activity we work with key stakeholders to define the scope and audience for the assessment, including assessment survey participants, different populations of participants (e.g. staff vs management) for comparisons, the population for the cultural survey (which may be far broader than for the other assessment survey) and any specific commentary to include in the launch communications. We will also agree timings and the dates for feedback workshops.

2. Assessment workshop. Where required, a small-group workshop, or several small-group workshops, are facilitated to complete the assessment. The advantages of these workshops include the conversations and the challenges that are possible, and also that consensus can quickly be established. The workshops works best for "target state" and "priority" where a smaller group view is needed.

3. Assessment survey. To cover a wider population of staff, the assessment tool is distributed to a defined group, or groups, of staff. The advantages of the survey is both scale (gathering more views), but it also provides the opportunity to compare different views form different groups e.g. staff vs management, or 1LOD vs 2LOD. These comparisons can be particularly insightful. The core assessment survey covers 9 of the 10 components – as below, culture is treated separately

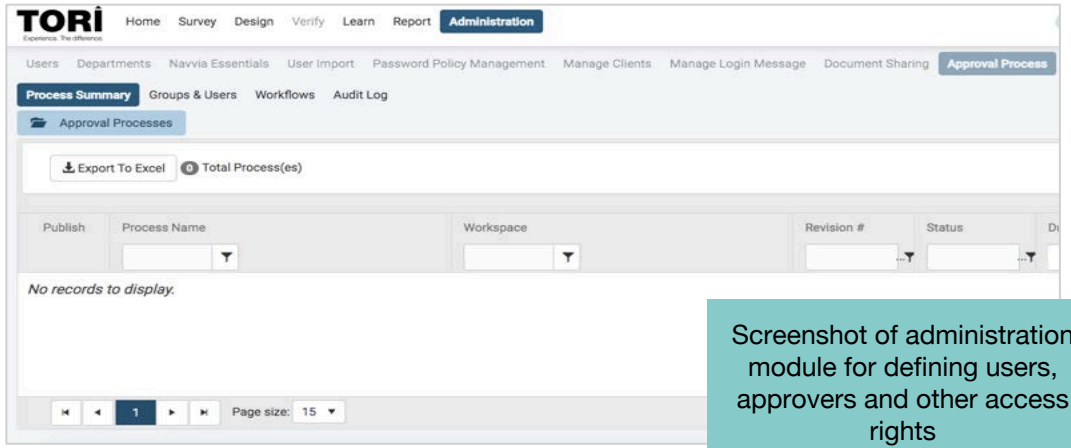
4. Culture survey. The culture survey covers the 10th component. It is delivered separately since the population of participants is generally much larger. A much larger population is important to provide an insightful view on culture.

5. Results workshop. Following the completion of the assessment, and a period of analysis, the aggregate results are presented in a results workshop. The facilitated discussion at this session acts as a springboard for action planning.

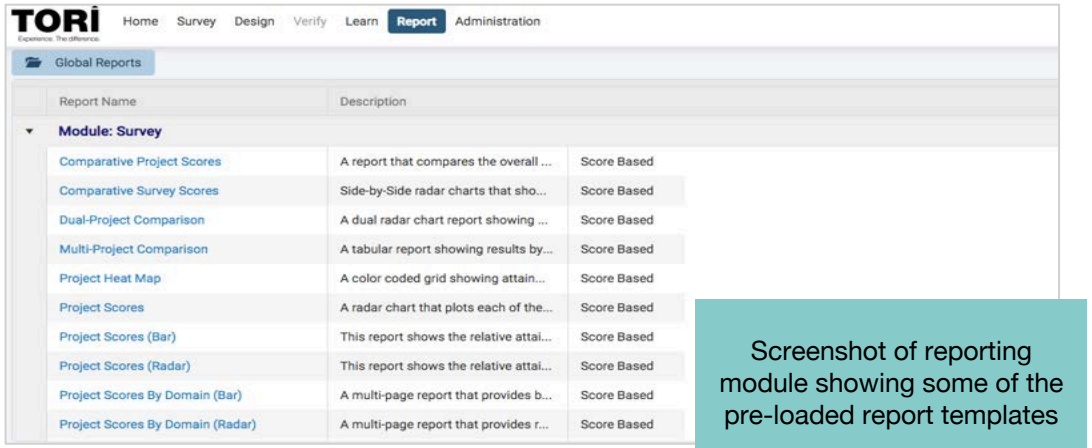
Delivery: tooling

TORI has an in-house tool, TECAM, that is used to distribute assessment tools and surveys. The Operational Resilience tool is pre-loaded in to TECAM with only very little configuration required to prepare it for use. The configuration needed includes:

1. Defining any communications to be included in the welcome or end messages.
2. Defining the populations, split by level, role, function or any combination of these.
3. Determining if access should be ”closed” or “open” – closed access allows access only to a defined population who receive a link via email, open access provides a link that can be forwarded.
4. Agreeing star and end dates, and any inflight prompts that are required to remind or chase completion.
5. Agreeing the reports that are required, drawing on standard template reports and analysis.



Screenshot of administration module for defining users, approvers and other access rights



Screenshot of reporting module showing some of the pre-loaded report templates

Example outputs (1 of 3)

The outputs include a single view for each of the 10 components, showing current and future maturity and the priority for change. Commentary and supporting evidence can also be included:

TORİ

Clear and shared "important business services" and tolerances				Current maturity	Target maturity	Priority for change
		What immature looks like	What mature looks like	1 to 5 low high	1 to 5 low high	1 to 5 low high
1	**Clear and shared view of "important business services"**	A view of important business services is either not in place, not yet agreed by all stakeholders or doesn't cover all services.	A clear view of importasnt business services has been created. Consultation was high. All stakeholders are engaged with the view. The view covers all business services	3	5	3
2	**Clear and shared view of the functions, processes and technology that deliver the "critical business services"**	There is a disconnect between services and the operating model. Some or some key functions, processes or technology have not been captured	The view of business services has been accurately and fully mapped to the operating model, so that all functions, processes and technology within each service have been identified	4	5	3
3	**Clear evidence about the decisions taken to define the "important business services"**	There is no or little evidence to demonstrate how decision on business services were made	There is strong evidence to demonstrate the decisions made to create the important business service view. There is evidence of good debate and engagement	2	5	4
4	**Clear and appropriate apportionment of accountabilities for the 'important business services" and also the supporting functions, processes and technology**	Process and activity views largely lack clarity about ownerships and responsibilities, with few complete end-to-end process views. There is no active encouragement to seek or take accountability	Defining and following accountabilities is a core competency and supported by clear documentation. Prioritisation and decision-making is transparent and all staff are well informed and engaged in reasons and evidence	1	5	3
5	**Clear and shred view of acceptable outcomes for the performance of each "critical business service"**	There are either no measures in place, or the measures that have been introduced are unclear or have a weak alignment to reports	There are clear outcomes established for the performance of the services. The outcomes are aligned to key reports, so they can be tracked	2	5	2
6	**Clear and shared view of impact tolerances**	There are either no set tolerances, or they have not bee effectively tested to demonstrate that they are valid	Impact tolerances are clear. They have been created based on analysis of historic and also desired performance. They have been subject to testing to demonstrate their validity	5	5	1
7	**Strong alignment of tolerances to existing risk appetites and other risk measures**	No analysis has been carried out to align tolerances to risk appetites	There is a strong alignment between the tolerances and the overarching risk appetite statements and/or other key risk metrics	4	4	5
8	**Clear evidence that tolerances are appropriate, given historic trends and results**	No evidence is available to demonstrate that the tolerances are valid	There is strong evidence to demonstrate that tolerances are valid based on historic trends and results	3	4	3
9	**Robust stress testing of tolerances**	No testing of tolerances has been carried out	A robust approach to testing tolerances has been carried out. The testing considered a variety of stress scenarios. The final level was set at an appropriate level	3	5	5
10	**Clear metrics to evidence performance vs. tolerances**	Management has access to limited operational measures, which are mainly lagging indicators. There are few defined KPIs and different approaches to operational management exist	Real time operational data is available at multiple layers. A sophisticated suite of KPIs is available designed around a balanced scorecard are used to drive, manage and monitor performance	5	4	4
			Average maturity score	*3.2*	*4.7*	*3.3*

Example outputs (2 of 3)

An overall view across the 10 components shows performance relative to ambition, allowing decision on focus to be made during planning.

TORİ

Operational Resilience Maturity Profiler

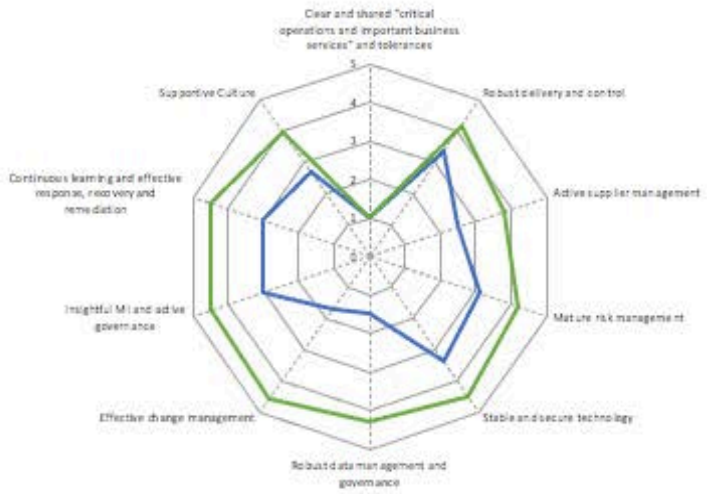
Summary report

Maturity results by component

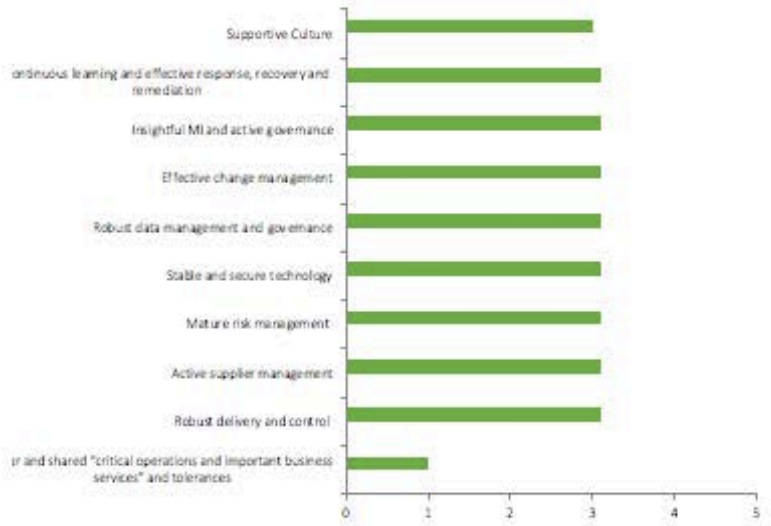
	Gap	Current	Target	Priority for change
Clear and shared "critical operations and important business services" and tolerances	0	1	1	1
Robust delivery and control	0.8	3.4	4.2	3.1
Active supplier management	1.3	2.5	3.8	3.1
Mature risk management	1.1	3.1	4.2	3.1
Stable and secure technology	1.1	3.4	4.5	3.1
Robust data management and governance	2.8	1.5	4.3	3.1
Effective change management	2.9	1.7	4.6	3.1
Insightful MI and active governance	1.5	3	4.5	3.1
Continuous learning and effective response, recovery and remediation	1.5	3	4.5	3.1
Supportive Culture	1.3	2.7	4	3

Formatting key	Less than	Between	Greater than
	1		2.5

Component maturity results



Component priority for change



Example outputs (3 of 3)

With comparisons across functions, or roles, or grades all possible to further add colour to views.

TORİ

Operational Resilience Maturity Profiler

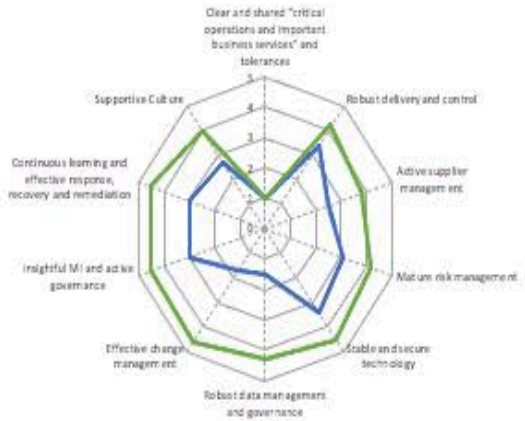
SPOC comparison

Maturity results by component

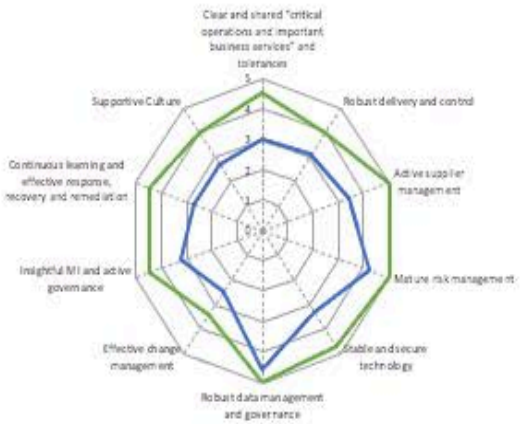
	Gap	Current	Target	Priority for change
Clear and shared "critical operations and important business services" and tolerances	0	1	1	1
Robust delivery and control	0.8	3.4	4.2	3.1
Active supplier management	1.3	2.5	3.8	3.1
Mature risk management	1.1	3.1	4.2	3.1
Stable and secure technology	1.1	3.4	4.5	3.1
Robust data management and governance	2.8	1.5	4.3	3.1
Effective change management	2.9	1.7	4.6	3.1
Insightful MI and active governance	1.5	3	4.5	3.1
Continuous learning and effective response, recovery and remediation	1.5	3	4.5	3.1
Supportive Culture	1.3	2.7	4	3

Formatting key	Less than	Between	Greater than
	1		2.5

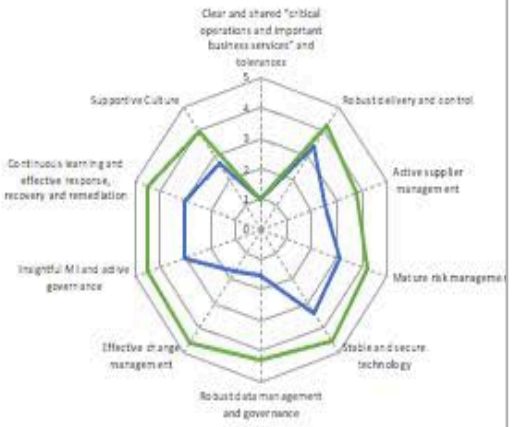
C-Suite view



Manager view



Staff view



TORI has a comprehensive suite of tools to accelerate delivery of OR

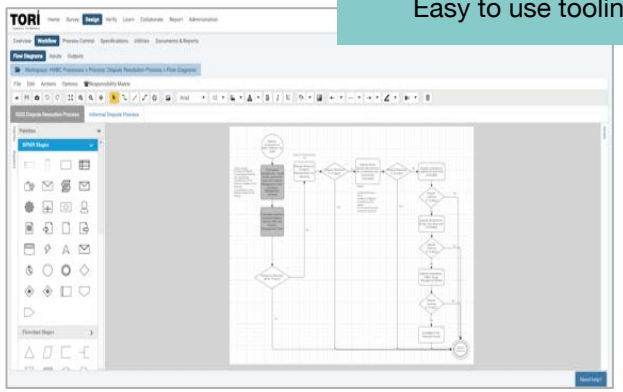
As an example, the other tools, frameworks and templates that TORI has that can support Operational Resilience analysis and delivery include:

Other maturity profilers and assessment tools	TECAM includes other profiling and maturity assessment tools including for: Cyber threat assessment and maturity; Supplier Management, including the EBA guidelines; IT maturity (ITSM and ITIL), or Programme Assurance. These are useful after an OR maturity assessment where more detailed analysis is needed or desired.
TECAM process design and control	TECAM also provides end-to-end process mapping and the ability to auto-generate Standard Operating Policies and Procedures (SoPs) from these maps to ensure an interlock between what is documented as part of your control library and what actually happens in the BAU environment. Further details on this tool follow.
ControlHUB	TORI ControlHUB provides single, clear view of risk and controls. Accessible across 3LOD and so ensures all functions are aligned to business objectives and risks. Evidences effectiveness of and conformance to controls. Modular design. Fully customisable and could support self-assessment requirements.
Automation Finder (partnership)	Automated capture of BAU desktop processing activity (re-key, manual interventions, process handling time) to identify automation opportunities and subsequent build.
Firescope (partnership)	A Configuration Management Database (CMDB) providing automated control and management of assets including capture of physical and virtual relationships of critical assets and business services plus performance monitoring.

TECAM process design and control

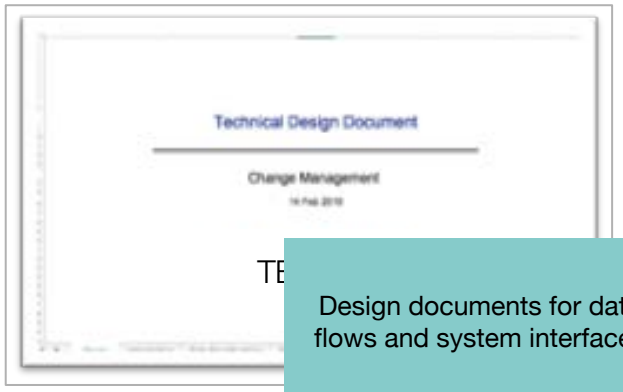
TECAM further supports Operational Resilience since the process design and control capability not only supports process definition at multiple levels, but it also automatically creates standard operating procedures, data flow documents, technical / system requirement documentation and process measurement and reporting information. The alignment provided by TECAM ensures that any changes to maps at one level are automatically cascaded to subsequent process levels and also to any associated process documentation. This ensures that any changes will be automatically captured.

Easy to use tooling

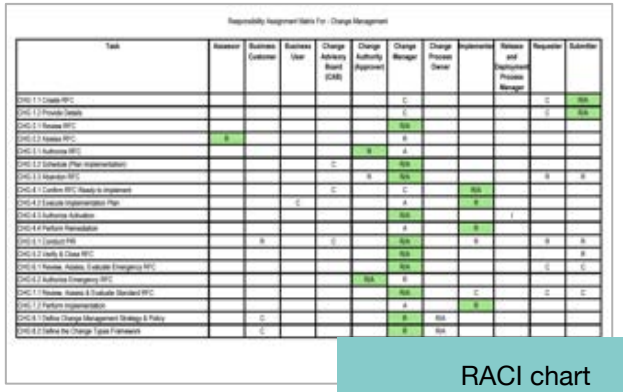


Level 0 flow chart

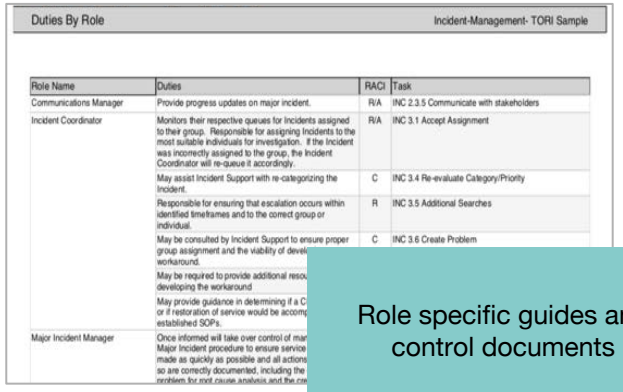
SIPOC



Design documents for data flows and system interfaces



RACI chart



Role specific guides and control documents

SOPs

Selected case studies

Selected case studies

1. “Operational Resilience & Cyber Security”

Client challenge

The Bank of England and the Financial Policy Committee (FPC) has for some time been focused on end-to-end Operational Resilience – this is not about being able to evidence the recovery of a system out-of-hours in a controlled DR / BCP test scenario.

This is about understanding the end-to-end value chain both within the regulated perimeter (banks, insurance companies, fund managers, exchanges, clearing houses etc.) and third-parties that sit outside this perimeter but provide and/or support critical services to these regulated entities.

It’s about understanding the complex inter-connected dependencies and potential impact to the real economy. In this respect, Payments, Clearing, Settlement and Custody & Safekeeping functions are a significant area of interest given the systemic risk and potential impact.

What we did

The Bank and the FPC have a detailed view on institutions that operate within the regulated perimeter. TORI was engaged to analyse third-party vendors and service suppliers that are critical to the functioning of regulated firms. As part of this analysis, TORI performed the following steps:

- Documented the landscape of third-party suppliers that support Payments, Settlement, Clearing and Custody & Safekeeping functions (PCSC)
- Identified where there is concentration risk amongst third-party suppliers
- Identified the dependencies at a process level between regulated PCSC functions and those unregulated third-parties
- Provided a broad assessment of the cyber-resiliency across the third-party firms.

Outcomes

One of the key aims of the analysis was to establish the relationship between regulated firms providing PCSC functions, and those unregulated third-party suppliers providing services to PCSC firms.

We also highlighted maturity levels viz-a-viz Operational resilience and Cyber security as well as setting out key considerations and industry Best Practice to underpin baseline analysis

BANK OF ENGLAND

Selected case studies

2. “Operational Resilience – Crisis Management”

Client challenge

We had previously completed a Business continuity capability assessment for our client, a Tier 2 London-based bank.

Among the recommendations was to run an Independent Authentic scenario exercise to test Crisis management, Emergency response management and overall BC capabilities including communication with all stakeholders including media and regulators.

What we did

Scenario scripting and prop creation:

- TORI tailor-made a scenario, suitable to the bank, its configuration and known vulnerabilities
- TORI provided a team to independently run the exercise
- The exercise was run over 4 hours, simulating 4 business days with critical decision points built in, e.g. invocation of Crisis Management, invocation of DR, Stakeholder communication, PR, Health and Safety considerations, etc.
- In total we used 28 prepared and customized injects during the exercise.
- The entire scenario output was captured and documented throughout

Outcomes

The scenario exercise made the recommendations in the previous Business Continuity assessment come alive.

Based on the captured output and observations, TORI delivered a story board of the day TORI delivered a set of recommendations, primarily in the areas of People and Process for improvement.

The crisis management team and the wider group of stakeholders became aligned as a result of the exercise.

3. “Operational Resilience and Best Practice”

Client challenge

The Client, a Tier 2 London-based European bank, wanted a Current State review and Gap Analysis of their operational resilience capability against best practice.

The client also wanted us to uplift their Policies, Framework and playbooks and to train and provide cyber simulation scenarios (war gaming) to their board.

In parallel they wanted us to establish a business services catalogue with criteria that can be used to identify critical business services and supporting people, process and technology.

What we did

We established 2 workstreams:

1. Crisis / Incident management and Training - 4 phases:

- Current State and Gap Analysis
- Creation of Framework
- Creation of Playbooks
- Training – creation, piloting & Board level “war game”

2. Business Services catalogue - 3 phases:

- Business Services Catalogue
- Definition of criteria and finalisation of catalogue
- Best Practice Reporting and review

Outcomes

The Client subsequently requested we provide an annuity service to refresh the threat vectors, framework and playbooks, to conduct a yearly security audit and provide training and war gaming