| Paper Title |
| --- |
| Embedding a Proactive Operationally Resilient Culture in Telecommunications |
| **Author** |
| Dr Charmaine Leech<br>Senior Director of Risk, Compliance and Governance Consulting Ltd. |
| **Date** |
| 9th July 2025 |

## Context of problem

Telecommunication services are critical to society. Outages ripple through virtually every industry. The impacts are felt across critical service provides; customer facing businesses; operationally dependent sectors; digital and media; other sectors; and most private consumers.

The importance of operational resilience has driven regulation and legislation in the sector. Measures are mandated through a combination of statutes, licence conditions and sector-specific guidance. Key obligations span the UK's Telecommunications Security Act, Ofcom's Network and Service Resilience Guidance, EU directives on network integrity and broader critical-infrastructure rules.

Regulatory compliance is not enough. The threats to, and opportunities for, operational resilience are emerging. For example, climate change is leading to more uncertain and severe weather conditions, geopolitical challenges are leading to more uncertain trade conditions, technological innovation is delivering new services at a rapid rate. Reliance of regulation to drive internal control arrangements could be argued to be dangerous- regulations will not stop an organisation being attacked by malicious actors! Organisations should, therefore, not only comply with regulatory requirements, but should also continuously adapt, enhancing control arrangements proactively to address emerging threats and opportunities.

Resilience requires investment. Organisations should invest and act before reasonably foreseeable operational disruption events occur. Investment decisions need to ensure that resources are optimally allocated to minimise losses and take advantage of opportunities.

The question is, "How do telecoms providers embed a proactive operationally resilient culture?"

**Proposed Solution Outline**

In this paper an eight-point plan is outlined.

- Identify the risks to operational resilience
- Assess the criticality of assets
- Set objectives for operational resilience.
- Monitor performance against objectives.
- Create risk informed investment cases.
- Prioritise investment asks against objectives.
- Ringfence funds for maintenance of mandated internal controls.
- Operate ongoing intelligent risk management.

In summary, this paper recommends the implementation of a risk-based operational resilience regime that ensures the exposure to operational disruption is managed within the telecom providers' risk appetite.

## Identify risks to operational resilience

Ofcom[1] defines operational resilience to be "the ability of a network or a service to resist…. disruption from a range of known and future internal and external threats…" So, the question is how can organisations have confidence that they have identified all known and future internal and external threats?

A simple solution is the adoption of an assurance map. Assurance maps provide a hierarchical categorisation of all risks to an organisation's strategy and operating model. This means they should cover all strategic perspectives,[2] namely financial; conduct; operational resilience; and capacity and growth. Within each of these broad risk categories, subcategories are established. In respect of operational resilience, risks to continuous service capability must at minimum consider the threats to the enablers of service capability. This would at minimum[3] include:

- **Physical Assets Risks:** Losses due to operational disruption costs incurred due to damage to or loss of physical assets. These should include losses caused by Power Interruptions, HVAC, Physical Asset Security Events, Flood, Fire, Extreme Weather Acts of God (Earthquake), & Loss of Access.
- **Human Resource Risks:** Losses due to operational disruption costs incurred due to human resources. These should include losses caused by Sickness/absence of Resource (absenteeism, vacancies), Labour Relations & Labour Action, Capability of Resource, Loss of Key Person, & Human Resource Security Events.
- **Technology Risks:** Losses due to operational disruption costs incurred due to failures or faults of information technology. These should include losses caused by Obsolescence, Technology Security Events (Cyber Attack), Misconfiguration & Design.
- **Third Party Risks:** Losses due to operational disruption costs incurred due to failures or faults of third-party provision. This should include losses caused by Enforced Termination, Supplier Performance (poor quality, capacity shortfalls), Trade Restrictions, and Third-Party Security Events.

[1] Statement on Network and Service Resilience Guidance Published 6 September 2024

[2] Balanced business scorecard defines the four perspectives of stratefy to be finance, consumer, systems and processes, capacity and growth.

[3] Consistent with Ofcom's Guidance[3] which stipulates that "Threats to the operation of a network or service include but are not limited to: (a) Physical threats or shocks such as fire, vandalism, or flooding and other extreme weather events; (b)Technology vulnerabilities that result from hardware and software failures or capacity/overload problems; (c) Human error that results from inadequate training/ recruitment or negligence; (d) Architecture design failings, for example when networks are subject to a single point of failure and do not have backup routes or systems available when things go wrong.

- **Data Risks:** - Losses due to operational disruption costs incurred due to failed or faulty data. This should include losses due to Completeness of Data, Quality of Data, Availability of Data.

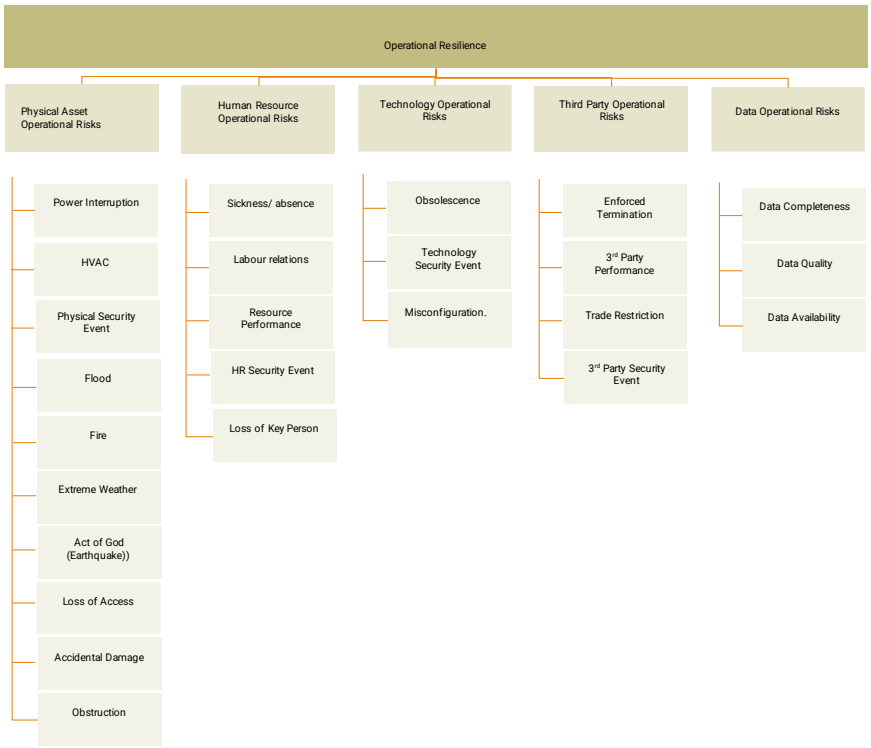


*Figure i: - Illustrative hierarchical categorisation of enterprise-wide operational risk events*

The first recommendation is to develop an assurance map that provides a hierarchical categorisation of enterprise-wide operational resilience risks.

### Assess the criticality of assets

Ofcom has defined four network domains for which failures would differ in service impact:

- Access / Last Mile: The links to the end-customer site or device.
- Aggregation / Backhaul: The links between the access network and the core.
- Core: The links that carry multiple telecoms services to customers from the core.
- Peering and non-Internet Interconnection: The links network-to-network.

These network domains therefore differ in criticality to the organisation.

In a broader context, we can consider the criticality of all enablers to business operations. To do this systematically we need to introduce a hierarchical asset categorisation. This is illustrated by figure (ii) below.

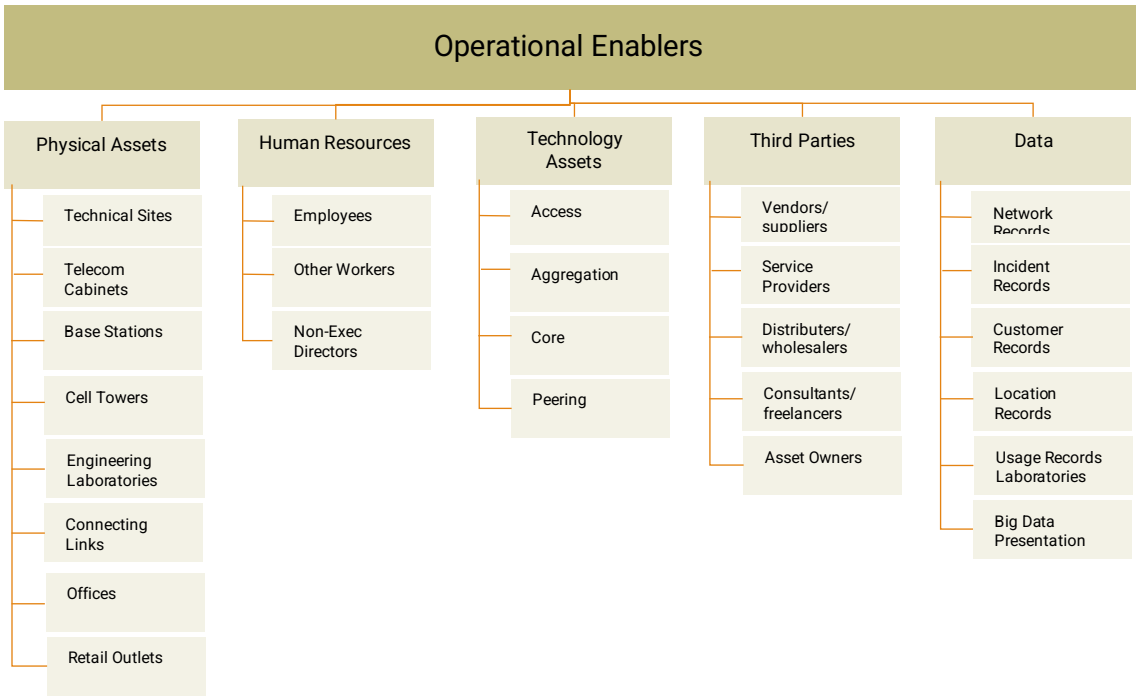


*Figure ii: - Illustrative hierarchical categorisation of operational enablers*

Further subcategories can be defined according to the needs of the organisation. For example, service providers can be subdivided into types of service provided and then service provider instance. Technology can be divided into domain and then an OSI category. As a rule of thumb, the level of granularity is dependent of the usage of the risk information. The categorisation should be sufficient to (a) drive investment decisions; and (b) define proportionate standards of mandated internal control[4] for the asset type.

[4] Categorisation does not need to go to an asset instance level if not required for decision making activity

Once an appropriate level has been established the category should be assessed for criticality depending on how many customers would be impacted by a failure of the asset.

The second recommendation is to develop an asset categorisation that provides a hierarchical categorisation of enablers to the operating model.

**Set objectives for operational resilience**

Performance of organisations should be managed across multiple dimensions, not just financial performance. The balanced business scorecard covers four perspectives. These are: Financial, Consumer; Systems and Processes; and Capacity and Growth.

Regarding systems and processes, organisations have an objective to provide continuous services, that is an objective for operational resilience. From a regulatory perspective, the overarching objective is to ensure networks or services resist disruption from a range of causes.

It is extremely unlikely, and cost prohibitive, that an organisation will be able to maintain continuity of service 100% of the time across all its services, and therefore an organisation may have some tolerance for disruption. Tolerances might be expressed in terms of (a) duration of a single outage event[5]; (b) cumulative outage duration over a given period; (c) cumulative lost customer hours within a given period; and (d) cumulative cost of business disruption events in a period[6].

Expressing tolerances in financial terms enables an alignment with the financial sustainability measures of the institution. Expected losses should be accounted for within technical provisions component of the balance sheet, whereas unforeseen losses should be covered by unrestricted reserves. This link between operational resilience risks and the balance sheet provides a case for investing, ensuring that expected losses, and losses from unforeseen shocks, do not exceed the organisations tolerance.

The organisations' tolerance for disruption may vary at an asset category level. This is dependent upon the service impact of a risk event associated with an asset failure, that is it is driven by the criticality of the asset. This means that tolerances may need to be defined by asset category.

The third recommendation is to define an objective for operational resilience and to define tolerances for operational disruption events for different asset categories.

[5] This should be reflected in disaster recovery plans where the plan should deliver restoration of services within the business' tolerance for duration of outages.

[6] There is a cost associated with an outage depending on the impact on services and the maintenance and repair costs. Estimates for an hour's outage vary between £100k and £540k depending on criticality within the network

**Monitor performance against objectives**

Monitoring performance against objectives is important because it (a) identifies problems early; (b) boosts accountability; (c) informs better decisions; (d) enables continuous improvement; (e) provides greater transparency and oversight.

Usually providing management information comes at a cost. Fortunately, driven by regulations, telecoms providers have already collated records about crystalised operational resilience risk events. [7] The data is happily ready for use for monitoring against risk appetite. Organisations have an opportunity to use this data to drive management action. Usability however is dependent on the ability to stratify the data to the risk and asset categories.

Monitoring incident records overtime against the established tolerances for operational resilience should enable management action to be triggered in accordance with the organisations risk appetite. If a single incidents duration is outside of duration tolerances it should result in enhancement of response measures (disaster recovery plans), whereas if the financial tolerance is breached it should result in strengthening of preventative measures- including, but not limited to, redundancy and lifecycle management controls.

Further organisations should learn lessons from incident occurrence. It may be that the organisation was aware of a weakness in internal control arrangements, a vulnerability, which it has not addressed proactively. The result is an actual loss event that could have cost the organisation more than implementing preventive measures would have.

It is important to emphasise that effective monitoring is not solely about collecting data but about transforming that data into actionable insights. For monitoring to truly drive value, organisations must establish clear reporting structures and escalation pathways. This ensures that deviations from tolerances are not only identified swiftly but are also communicated to the right decision-makers who can authorise timely interventions.

To maximise the value of monitoring, organisations should establish clear processes for regular review and escalation. This includes setting up dashboards that visualise incident trends, tolerance breaches, and areas where performance is either meeting or failing to meet defined objectives. Engaging key stakeholders in periodic reviews ensures that insights derived from monitoring are acted upon, rather than left as passive observations. Targeted

[7] Ofcom's General Conditions of Entitlement (GCOs) impose obligations on all UK communications providers (both network and services) to establish, maintain and retain records of security or resilience incidents. The core provisions are set out in Condition C2 (Security and Integrity of Networks and Services) and Condition C4 (Timely Notification of Service Failures and Major Incidents). Records should contain a description of the incident's nature, its scope and severity (services/locations affected, number of users, duration of outage).

reporting to governance committees—such as risk or audit committees—can further reinforce accountability and drive timely interventions.

Equally important is fostering a culture where near-misses and minor incidents are reported and analysed, not just major disruptions. By doing so, organisations can capture early warning signs and identify systemic weaknesses before they escalate into significant events. This approach ensures that operational resilience is not merely reactive but forms an integral part of the organisation's continuous improvement cycle.

Furthermore, regular reviews of both the tolerances and the monitoring framework itself are necessary to ensure continued alignment with evolving business objectives, regulatory requirements, and the dynamic risk landscape.

Leveraging advancements in data analytics and automation can further enhance the organisation's ability to detect emerging patterns of risk, measure performance in near real-time, and simulate the potential impact of operational disruptions before they occur. This proactive approach supports a culture of continuous improvement, where lessons learned from past incidents directly inform updates to controls, processes, and investment priorities.

Ultimately, robust performance monitoring reinforces the link between operational resilience and strategic value creation, offering management a clear line of sight between risk management practices and long-term financial sustainability.

The fourth recommendation, is therefore, to monitor incident occurrence against established tolerances for business disruption events.

**Create risk-informed investment cases**

Any investment ask should be accompanied with a strong business case. A robust business case lays out why a project matters, how it delivers value, and what it takes to succeed. Defining financial value is key to making a persuasive and strategic case for action.

The question is, how do organisations define the financial value of a project whose primary objective is to achieve operational resilience? This can be achieved by using insights provided by risk management. Risk assessment should provide an assessment of the financial impact of loss events at different confidence levels. Using historical incident data organisations can determine the expected financial impact of operational disruption events (simply by using the average rolling 12-month loss over the last 5 years). This should inform the amount that needs to be provisioned for expected losses due to operational risk events. Historical incident data can also provide organisations with an estimate of the capital required to cover an unforeseen risk event, at a given level of confidence. This amount should be accounted for in the unrestricted reserves. Estimation of this capital requirement can be done using probability distributions.

Two financial parameters can therefore be used to inform investment cases for measures that deliver operational resilience:

(a) provision for business disruption events; and

(b) capital required for unforeseen business disruption events

Clearly this can be augmented by consideration of regulatory or legislative financial penalties including:

(a) Regulatory monetary fines for non-compliance with Ofcom's Network and Service Resilience[8] measures.
(b) Contractual penalties from breach with contractual terms with wholesalers and other distributers.

The challenge, therefore, requires a nuanced approach, one that balances the intangible benefits of resilience—such as reputational protection and stakeholder confidence—against the more quantifiable costs of potential disruptions. By integrating these calculations into the investment case, organisations can demonstrate not just the cost of inaction, but the tangible value of mitigation.

The fifth recommendation is to develop risk informed investment cases for operational resilience measures – that is dovetail risk management with investment decision making.

[8] Communications Act 2003 (as amended by the Telecommunications (Security) Act 2021 and related regulations),

**Prioritise investment asks against objectives**

When multiple proposals compete for limited resources, the one with the strongest financial upside is often prioritised. Prioritising investment asks is important to direct funds and effort toward projects that offer the greatest return. With constrained capital, organisations need to optimally allocate resources to (a)minimise losses and (b) take advantage of opportunities.

When shaping these investment priorities, it is crucial to maintain a dynamic framework that assesses risks in the context of changing business landscapes and external threat environments. This means that risk-informed investment cases should remain agile—regularly refreshed to account for emerging risks, shifts in regulatory scrutiny, and evolving technological dependencies.

Decision-makers should collaborate closely with operational managers, risk specialists, and finance teams to ensure that risk assessments are grounded in operational realities and that investment proposals are both strategically aligned and financially robust. Stakeholder engagement is key: gathering input from those responsible for operational delivery ensures that investments target the most pressing vulnerabilities while also capitalising on opportunities for efficiency and innovation.

Furthermore, it is important to recognise that not all risks or assets warrant the same level of investment. Effective prioritisation requires a granular understanding of asset criticality, risk exposure, and the efficacy of existing controls. By building transparent, data-driven rationales for each investment, organisations can justify the allocation of funds and clearly demonstrate how each measure supports broader resilience objectives.

This collaborative, risk-sensitive approach to investment planning should be complemented by a transparent prioritisation process that weighs both strategic objectives and practical constraints. Organisations may benefit from establishing systematic criteria—such as risk reduction potential, regulatory alignment, and operational necessity—to evaluate competing proposals. By applying these criteria consistently, leadership can ensure that limited resources are channelled toward initiatives with the greatest overall organisational impact.

The sixth recommendation is the to develop systematic criteria for evaluating competing investment asks and apply these criteria consistently.

**Ring fence funds for Board mandated internal controls**

A further dimension to effective resource allocation is the clear demarcation of funding for board-mandated internal controls. These controls—often grounded in regulatory guidance or essential organisational principles—represent the baseline of risk management. Even as organisations weigh various proposals on the basis of potential returns or strategic alignment, it is critical to distinguish investment asks that arise from gaps in these mandated controls. Such requirements should not be subject to the same competitive evaluation as discretionary projects; instead, they demand immediate response and guaranteed funding to preserve compliance and safeguard core operations.

To enable disciplined execution, organisations should establish dedicated budgetary provisions for the timely remediation of mandated control deficiencies. This ensures that any lapse identified—whether due to evolving business processes, technological obsolescence, or new threat intelligence—can be swiftly addressed, preserving the integrity of governance frameworks and maintaining the confidence of both regulators and stakeholders. By ringfencing resources for this purpose, leadership reinforces a culture of accountability and a proactive stance toward risk, sending a clear signal that foundational controls are non-negotiable and central to the organisation's resilience strategy.

Above all, the process for distinguishing between discretionary investments and those required to remediate mandated control gaps must be rigorously transparent. While it is prudent to weigh the relative merits of competing investment asks, organisations must resist the temptation to subject foundational control requirements to the same resource constraints or delays as other projects. These controls, defined through board policy and further refined in local engineering standards, serve as the bedrock upon which all other risk management activities are built. Their prompt implementation is not only a matter of regulatory compliance, but also a practical imperative for sustaining business continuity and stakeholder trust.

In tandem with these commitments, leadership should regularly review and update internal control documentation, ensuring that policies and standards remain aligned with emerging regulatory expectations and shifting threat environments. Clear escalation pathways for reporting and remediating deficiencies further reinforce accountability and enable a proactive stance when new vulnerabilities are detected. Through this disciplined approach, organisations achieve a balance between agility in discretionary investment and unwavering responsiveness to mandated controls.

The seventh recommendation is to ringfence funds for mandated internal control arrangements.

**Ongoing operational risk management**

Intelligent operational risk management should deliver ongoing operational resilience. The outputs of operational risk management should dovetail with investment decision making to support coordinated and economical application of resources to minimize, monitor, and control the probability and/or impact of unfortunate business disruption events or to maximize the realization of opportunities.

Operational risk management is not about creating a long list of risks or operational issues and then taking the top few for reporting purposes. This approach has been taken by many organisations for a prolonged period and has failed to protect organisations from crisis events.

We can learn from highly regulatory sectors such as financial services. In these sectors risk management consists of several activities which dovetail with decision-making processes.

Risk management activities include:

- Objective Setting: - Establishment of risk management strategy including risk appetite.
- Emerging Risk Identification: -Horizon scanning to identify threats and opportunities.
- Risk Assessment: Quantitative and qualitative assessment of risks on a current and forward-looking basis.
- Risk Monitoring: Monitoring of parameters of risk and current issues to identify any fluctuations in exposure or proximity.
- Risk Control: Establishment of minimum standards of control in policy documentation.
- Risk Reporting: Annual reporting of exposure to risks on a quantitative and qualitative basis
- Risk Response: - Response planning for and crisis management of materialised risks. this includes capital contingency plans, business continuity plans, insurance recovery arrangements.

Whilst this looks like a significant amount of activity, establishing a framework upfront means that this activity can be undertaken systematically and in some instances it can be automated.

The final proposal, therefore, is to develop a robust enterprise-wide risk management system that dovetails with decision-making and provides outputs that inform the allocation of financial and other resourced.

**Summary**

Telecommunication services are critical to society. In recognition of this there are developments in regulation and legislation to drive operationally resilient networks. Development of a risk-based proactive operational resilience regime can provide institutions with the tools they need to manage operational resilience and can provide governing bodies with the information required to manage the capital allocation in a manner that promotes operational resilience.

**Author Biography**

Charmaine began her career in risk management within the financial services sector. The insurance sector found itself in financial crisis which resulted in the introduction of Solvency II, a regulatory programme to implement a risk-based solvency regime. Charmaine has recently worked with a focus on translating the risk-based solvency regime approach to other sector including telecoms and the public sector.