Operational Resilience
A holistic framework

Regulatory pressures, sprawling IT estates, advances in technology and a world of ever-present challenges to security and stability are compelling organisations to become more agile, in a manner that provides more flexibility in how they respond to systemic threats, changing marketplaces and their customer demands. Operational resilience is the ability to anticipate and manage change and/or threats whilst reducing negative impact to business objectives.

The framework identifies 12 management disciplines that effectively manage risk. Each of these disciplines must be implemented as a system, with each system integrated into one framework. It’s all about eliminating silos.
## Business Continuity Management
A management process that identifies potential threats to an organisation and the impacts to business operations if those threats are realised, includes BCR.

## Crisis Management & Communications
Addressing a crisis at a strategic level of the organisation. Includes the discipline on the strategies, key messages and comms with the various audiences and key stakeholders.

## Critical Assets & Environments
Discipline on the design, build, operations, management, governance and audit of data centers incl. associated telecommunications and storage. The discipline also incorporates facility management, safety and security capabilities.

## Financial Health & Viability
An organisation must be financially viable and provide a product or service under changing conditions. Four main areas of financial health are liquidity, solvency, profitability and operating efficiency.

## People Operations
Maximising employee productivity. Enhanced when organisations encourage a culture of resilience and leaders who can adapt to changing circumstances, includes ability to demonstrate resilience attributes.

## IT Continuity & Disaster Recovery
Minimizing the impact of disruptions around an organisation’s investments in technology and telecommunications. This includes consumption of cloud services (IaaS, PaaS and SaaS) plus developing a data strategy (nature of data stored, where, how, access and its value).

## Incident Response
Procedures in place to manage an incidents that impacts life safety and physical assets. Should consider physical security and environmental health and safety. Includes the central management of response required across the organisation (ICT, Security, Risk, etc…).

## Information Security
The practice of defending information from unauthorised access, use, disclosure, disruption, modification, recording or destruction. Both physical and electronic.

## Governance, Audit & Compliance
Ensuring best practices determined by various industry groups, oversight organisations and government agencies are known, documented and measured, with audit execution to ensure alignment with such practices.

## Risk Management
The identification, assessment and prioritisation of risks followed by coordination of resources to minimise, monitor and control the probability and/or impact of an incident or to maximise the realisation of opportunities. The objective is to assure uncertainty does not negatively impact strategic objectives of the organisation.

## Supply Chain Resilience
The discipline of implementing supply chain continuity, managing supply chain risks and ensure supply chain security. Managing threats to your supply chain, from likelihood, globalisation, shrinking product cycles, market volatility and unpredictable market cycles.

## Organisational Behaviour
Focusing on attributes of resilient organisations including attributes affective culture, coordination of risk management activities, sharing of information and knowledge, resource availability and ability to anticipate and manage change.
Think about the following considerations:

- How confident are we in strategically communicating a crisis that has a wider business impact?
- Do we have an understanding on the impact of a service outage across the business?
- How fast, controlled and efficient are we, as an organisation, in responding when a crisis occurs?
- Can our strategic partners continue to service our business needs during a crisis?
- During a crisis, are we anymore vulnerable to loss or breach or data?
- How disciplined are we in the governance, operations and management of our most critical assets & environment?

To discuss DXC’s Operational Risk Framework for ServiceNow with one of our solution experts, email servicenowpractice@dxc.com

About DXC Technology

DXC Technology (NYSE: DXC) is the world’s leading independent, end-to-end IT services company, helping clients harness the power of innovation to thrive on change. Created by the merger of CSC and the Enterprise Services business of Hewlett Packard Enterprise, DXC Technology serves nearly 6,000 private and public sector clients across 70 countries. The company’s technology independence, global talent and extensive partner alliance combine to deliver powerful next-generation IT services and solutions. DXC Technology is recognised among the best corporate citizens globally. For more information, visit www.dxc.technology.