ITLF Service Resilience Paper 7

Availability: the role of RACI

Summary

Availability can be measured as a ratio of the time a solution is inoperable over some period. For instance, banks typically offer 99.5% or higher availability of online payments services.

Resilience is in general the ability of an organisation to withstand shocks. In the context of IT systems, it describes the capabilities to contain IT failures and reduce their impact on other parts of the system and or to customers. It can be measured as the average time a service takes to recover from failure and resume services to users.

Use of the RACI matrix provides clarity on:

- Accountability for setting the desired availability performance;
- Responsibility for achieving the necessary performance;
- who should be Consulted;
- who/how to be Informed of the standard which has been set and the potential actions in case of service outage.

Background

IT failures are no longer a matter of if - they're a matter of when. With high-profile cyberattacks and service outages making headlines, including the infamous Crowdstrike[1] incident, the pressure on Board Directors to manage these risks has never been greater.

Senior management is now held accountable for more than just their organisation's bottom line - they're responsible for preventing and mitigating the fallout from catastrophic IT disruptions that can wreak havoc on reputation, finances, and service delivery.

What are the hurdles to fulfilling this accountability?

[1] https://www.bbc.co.uk/news/articles/cr54m92ermgo

Lack of awareness

A recent CEO survey found that 90% of top executives believe 'it won't happen on my watch'. This mindset is dangerously outdated. As businesses integrate more third-party software, the chance of failures stemming from external systems rises. The truth is that IT failures are inevitable, unpredictable, and can affect any organisation - no matter how well-prepared it thinks it is. Directors must let go of the 'it won't happen here' myth and adopt a mindset of resilience and preparation.

Lack of systemic data

IT failures are of increasing scope and duration, but remediation is hindered by the lack of systematic data which is in place for other utilities. Following a recent roundtable on the topic, the BCS has called on the UK government to take the lead in data sharing in the public sector[2]. The ICO already uses a NIS[3] framework for reporting on data breaches by Relevant Data Service Providers and the fines which have been levied[4]. The adoption of this framework across other sectors would bring it into line with other utilities: for instance, the rail industry publishes the cost to users of service failures.

Difficulty of assigning costs

Traditional economic assessments of IT failures typically include internal costs of implementing changes. What's often overlooked is the broader cost to users from the lack of services or the corruption of data.

The NIS framework provides four metrics for the impact of IT failure: lost user hours; loss of data integrity; damage to life or health; and financial repercussions on users. Now IT is widely recognised as a utility, organisations will need to insure against claims relating to lack of availability. These metrics allow Boards to assess the extent of the risk and take appropriate insurance.

How can RACI help increase availability?

The first steps in building a more resilient organisation need to be visible. Some very basic managerial tools such as RACI provide a means for 'getting started'.

RACI stands for the four different roles in improving availability:

[2] https://www.bcs.org/media/tvudbfex/transparency-software-is-the-elephant-in-the-room-policy-brief-v5.pdf

[3] https://www.bcs.org/media/czwjt34u/availability-the-nis-framework.pdf

[4] https://ico.org.uk/

- Responsibility
- Accountability
- Consulted
- Informed

RACI Is used extensively by consultants working with organisations, as a tool to understand who is tasked to deliver what and to protect their reputation.

Responsibility

Responsibility for implementing resilience – operations including IT plus increasingly 3rd party suppliers. The metrics used for these tasks have traditionally been internal, such as MTTR[5]: increasingly the metrics used to assign responsibility will be focused on the user impact of IT failures: eg using the NIS framework. Focus on user impacts requires different internal capacity.

Improving internal capacity involves a process of upgrading of learning and skills to gain 'soft' skills, address competencies, and provide mentorship. This often benefits from the use of external standards and qualifications. The characteristics of people to deliver availability management are not easily inferred from a CV or specific qualifications. The role involves values about doing the right thing rather than performing to nominal goals; and an ability to move between larger system perspectives and details of implementation.

The value of user impact metrics will depend on the business service affected – hence the role of Important Business Services[6].

Accountability

Accountability for setting the organisation's required resilience capability – the Board is Accountable with input from the C-suite. To truly succeed in strengthening resilience, directors need to bring together teams from various departments - IT, business continuity, finance, and more - under a unified approach. One key to overcoming this challenge is developing a 'common language'. By defining Important Business Services (IBS) and Impact Tolerances, organisations can ensure that resilience is aligned with strategic objectives and that the board fully understands the importance of IT infrastructure.

[5] Mean Time to Repair
[6] https://www.bcs.org/media/2ucjm0ch/availability-the-fs-process.pdf

This may be through establishing controls: eg

- First line of defence: Control frameworks and day-to-day controls via for example implementation of Information Security / Business Continuity Management Systems e.g. ISO 27001, ISO 22301
- Second line of defence: Impartial regular Internal audits by competent auditors e.g. IRCA Certified Lead Auditors; testing effectiveness of implemented frameworks and controls
- Third line of defence: Prompt remediation by Top Management of Internal audit report findings via regular Management Review Meetings
- Fourth line of defence: Independent External audits by competent auditors e.g. IRCA Certified Lead Auditors; testing effectiveness of implemented frameworks and controls
- Fifth line of defence: Prompt remediation by Top Management of External audit report findings via regular Management Review Meetings

Consulted

People consulted may be subject experts, stakeholders inside the organisation, customers, suppliers, regulators.

Effective consultation is essential in setting achievable and desirable availability characteristics for the organisation.

Informed

Effective communication with customers can prevent unrealistic assumptions. It can also mitigate the impact of IT outages – for instance by advising of alternate ways of getting the service, or expected times of resumption of service.

Effective briefing of internal resources is built into good recovery practice – this may be through simulation, war games or memos ---. The 4 Cs of disaster recovery - Communication, Coordination, Continuity, and Collaboration - serve as the cornerstone of effective disaster preparedness and response[7].

[7] Eg https://pubmed.ncbi.nlm.nih.gov/26749291/