

Availability: the FS Process

Summary

The #Crowdstrike outage last year showed yet again how dependent we are on IT systems. Millions of Windows systems crashed, disrupting critical services and business operations globally.

The BCS IT Leaders Forum (ITLF) held a RoundTable on 9th January at the [BCS, The Chartered Institute for IT](#) offices, on *Availability: the challenge for IT Professionals*. The RoundTable discussed what could reduce the impact of IT failures on users, the economy and society; and the challenge for IT professionals.

This brief provides an introduction to the FS Process, formulated to reduce the impact of IT failures on users, the economy and society.

Background

IT is a utility; users expect utilities to work

The RoundTable shared the knowledge that most of our business and personal activities depend on services which include digital systems, that IT is now a utility. Society does not expect utilities to fail: people expect their services to be available 24/7.

IT is built on software which is inherently fallible

However, digital systems, and hence user services, are based on software. This is a problem, because *software, unlike other widely used products, fails unpredictably*. This is because it is complex, it is subject to rapid change, and it is made up of many inter-dependent components from a multiplicity of sources. Services seem to be subject to increasing numbers and severity of outages. These affect increasing numbers of people and wider aspects of life as our dependence on digital systems increases. Software is the elephant in the room.

Software accidents leading to failure and service outages can arise from inherent software flaws, user error, cyber-attacks, or new vulnerabilities resulting from emerging technologies like Artificial Intelligence algorithms. Software failures are disruptive. Access to services may be blocked. Data may be lost, corrupted, or looted. A service outage may be ephemeral and affect only a small number of people – so ignored or attributed to random events like cosmic rays. It may also be long-lasting, affecting millions of people and lead to major damage to life and/or healthⁱ.

Safety by design is necessary but will not meet the need

Legacy systems and systems procured from external vendors are dominant in UK organisations. Software has a long shelf life – many components still in use were designed for the conditions of the 70's. This means that organisations need a “whole systems” approach - based on the capability of the end-to-end system to deliver services to users. We discuss measurement systems and the recognition of Important Business Services, in the next section.

The operational environment

It is worth describing a “typical” operational environment:

- 24/7 operation of services to users;
- Multiplicity of external suppliers (several 100's of software vendors alone);
- Complex supply chains covering many jurisdictions for services and for software components.

Achieving service resilience involves IT but not only IT

The skills and capabilities to achieve more resilient services are often broadly dispersed within organisations. Often, the gaps in knowledge and practice are only recognised after an outage.

The first steps in building a more resilient organisation need to be visible. Some very basic managerial tools such as RACIⁱⁱ provide a means for ‘getting started’ in assuring availability.

The RoundTable found that a systematic approach to skills involves assessing the need - fundamentals, knowledge and expertise. This will help in identifying gaps and disconnects within an organisation. The gaps and disconnects may be bridged by either development of internal capability or by externally procured

capabilities. There is no magic bullet that will assure that the necessary skills are available.

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. *Availability management has become a critical and demanding role.*

Organisational capabilities

Organisations can build partnership and consensus by developing ‘translators’ and attention to achieving a common language for discussing performance, between technical and non-technical people. *With a common language, it becomes easier to enlist the support of management and board level decision makers for investment in service resilience.* The RoundTable members agreed that IT Leaders could be talking to their boards with a *Cost/time to fail* graph: this shows that greater investment in service resilience buys a lowering of the risk of service failure, but that the risk can never go to zero. This visibility of the organisation’s calibration of risk could reduce insurance premiums and could in the future be a requirement to obtain any insurance at all.

Organisations also need to promote the culture of ‘safe spaces’ for people to openly discuss service resilience and its value to the organisation. This involves more open discussion of failures and outages and the early signs indicating instability or risk. One model may be to draw on some of the practices common in health and safety where there is a positive obligation to call out issues.

Organisations need to establish a ‘What If?’ approach to planning for future potential scenarios to ensure they have adequate protections in place (similar to futurist approaches but with more concrete scenarios). One way forward is to define and conduct ‘pre-mortem’ examinations of large-scale failure to address managing organisational risks.

The needs for resilience are increasing everywhere, but in some sectors more rapidly and extensively than in others. This suggests establishing norms on a sector-by-sector basis. This could reset expectations regarding skills and

behaviours, and the possibilities for publicity/transparency on failures and their impact.

The FS Process

Approach to improving operational resilience in financial services

The culmination of an extended period of thinking about how to address resilience is the Bank of England's Prudential Regulation Authorityⁱⁱⁱ definition of a four-stage process for achieving operational resilience.

That approach is referred to throughout this book as "FS Process" and is summarised below^{iv}.




FS Process

- Identify important business services (IBS).
- Set impact tolerances for these services which define how much disruption can be absorbed before intolerable harm is inflicted on the users of the services.
- Undertake regular testing against severe but plausible (which goes beyond probabilistic assessment) operationally disruptive scenarios to identify vulnerabilities.
- Take mitigating action so that services can remain within tolerance.

We suggest that this four-stage process is a key to achieving digital service resilience as it affects critical business services.

The FS Process describes "what" but does not specify "How" the Important Business Services are to be identified. We provide some `Guidance for this in Chapter 5. The choice of IBS's is a strategic decision. It affects the viability of the company directly and immediately, and potentially over a longer timescale through damage to reputation or losses claimed by customers.

So, we suggest that the important business services identified should include three where in each case the service is delivered to an external customer or collection of customers:

<i>Important Business Services</i>		
	<p>FIBS</p> <p>Financially Important Business Service</p>	<p>Those with greatest fiscal impact on the organisation</p>
	<p>RIBS</p> <p>Reputationally Important Business Service</p>	<p>Those with greatest effect on reputation of the organisation</p>
	<p>CIBS</p> <p>Customer experience Important Business Service</p>	<p>Those with greatest impact on customers</p>

Important Business Services are identified because of their importance to the organisation and the wider economy. One aspect of this importance is the impact on the organisation, their reputation and customer experience, should there be a service outage. The length of the outage which is judged to be tolerable is the Impact Tolerance.

Chapter 3 discusses Impact Tolerances, their definition and setting. The choice of operationally disruptive scenarios (bullet 3 of the FS Process) requires a view of the sources of business risk: some of these will be internal and some external. Chapter 5 includes Guidance on the characteristics of scenarios, emphasising that tests based on user error, cyber-attacks, high traffic levels, and other potential disruptors are chosen to stress the system. Scenarios are an important tool for anticipation (see below)

In order to take effective mitigating action (bullet 4 of the FS Process), the organisation will rely on well documented *business* architecture that has clearly defined linkages to the organisation's *IT* architecture that will map dependencies and interdependencies. This map allows them to understand areas such as the

value streams for the service offerings of the organisation, and aids in the identification of adequacy and gaps in the capabilities of the organisation. There are a number of tools for this^v: the CIO web site provides a useful guide^{vi, vii}

- Financial service (FS) regulations aim to improve the resilience of the FS industry by defining Important Business Services and acceptable outcomes – Impact Tolerances
- The definition of Important Business Services provides a shared language for managers and IT Professionals to agree priorities
- The process to achieve acceptable outcomes or consequences – the Impact Tolerances - is generic and a useful template for all sectors.

ⁱ <https://nationalpreparednesscommission.uk/publications/elephant-in-the-room/> and <https://nationalpreparednesscommission.uk/publications/the-elephant-in-the-room-one-year-on/>

ⁱⁱ The RACI framework is based on assigning Responsibility and Accountability with Consultation and the Informing of stakeholders.

ⁱⁱⁱ <https://www.bankofengland.co.uk/prudential-regulation/publication/2021/march/operational-resilience-sop>

^{iv} <https://nationalpreparednesscommission.uk/2021/09/operational-resilience-in-financial-services/>

^v <https://www.bcs.org/articles-opinion-and-research/fake-and-real-tools-for-enterprise-architecture/>

^{vi} <https://www.cio.com/article/196069/top-enterprise-architecture-tools.html>

^{vii} <https://www.fca.org.uk/publications/policy-statements/ps21-3-building-operational-resilience>