White Paper

Continuity or Bust!

Submitted by:
Neil Walker
Principal Consultant

Office: +44 (0) 333 202 1018
Email: neil.walker@foxit.com

Introduction

Every service failure is an important 'moment of truth' – an opportunity to make or break your reputation with the business (or as a business).

This white paper sets out considerations to help with the early stages of an overall IT Service Continuity Management (ITSCM) process. It focuses on how IT service providers should assess risk and have a response strategy in place to provide agreed levels of service should a worse-case scenario happen.

The damage

It was the latter part of last year when Fox IT posted 'The Cost Of (A) Failure' citing the £50m fine handed to a well-known UK bank following a well publicised service failure in 2012. The same bank has suffered other systems outages preventing customers from using cards, cash machines and online banking services.

*"Modern banking depends on effective, reliable and resilient IT systems. The problems arose due to failures at many levels to **identify and manage the risks** which can flow from disruptive IT incidents and the result was that customers were left exposed to these risks."*

Tracey McDermott, director of enforcement and financial crime at the FCA

Within days of the item being posted on Fox IT's website, yet another event caught the headlines with dozens of flights cancelled and many others delayed after a major computer failure grounded planes in London and the South of England. Passengers faced widespread disruption after a serious computer failure at the UK's air traffic control centre led to flights being grounded or diverted.

UK Transport Secretary Patrick McLoughlin said the disruption was unacceptable and the air traffic control company NATS managing director apologised for the disruption.

The centre has been subject to a number of computer glitches in recent years, one of the worst on Saturday 7th December 2013 - when thousands of passengers were left stranded when hundreds of flights were grounded following a technical fault.

With IT being vital to most (if not all!) business processes, IT professionals cannot cross their fingers and hope bad luck doesn't visit their organisation, but rather take steps to ensure that risks and IT service management processes are assessed and plans put in place to restore service to an agreed level, minimising the disruption as much as possible.

The bigger picture

The failures above are not unique; other organisations have also been hit by IT problems which have affected customer-facing services, causing regulatory penalties, reputational damage and loss of customer confidence (and business!).

IT service stability is reliant on many influences, some that can be envisaged, some not so predictable. Effective IT Service Management (ITSM) offers a planning and control framework to ensure potential failures are avoided as much as possible or their effects mitigated. Those who invest in building and operating integrated processes as part of their management system see a significant reduction in system downtime, thereby resulting in stable platforms for business processing. Typical focus areas include:

- IT Service Continuity Management (ITSCM)
- Major Incident Management
- Proactive Problem Management
- Change Management
- Release Management
- Service Validation and Testing
- Availability Management
- Capacity Management

In today's highly competitive and service oriented business environment, organisations are judged on their ability to continue to operate and provide service at ALL times.

Business (and IT) continuity as one

The objective has to be (hopefully) the prevention of failure or at the very least the management of risks so that customers are protected and service restored as soon as possible.

Let's take a look at some definitions to clarify what we are talking about.

> Business Continuity (BC) is defined as the capability of the organisation to continue delivery of products or services at acceptable predefined levels following a disruptive incident. *(Source: ISO 22301:2012)*
>
> Business Continuity Management (BCM) is defined as a holistic management process that identifies potential threats to an organisation and the impacts to business operations those threats, if realised, might cause, and which provides a framework for building organisational resilience with the capability of an effective response that safeguards the interests of its key stakeholders, reputation, brand and value-creating activities. *(Source: ISO 22301:2012)*
>
> The goal of ITSCM is to support the overall BCM process by ensuring that the required IT technical and service facilities (including computer systems, networks, applications, data repositories, telecommunications, environment, technical support and Service Desk) can be resumed within required, and agreed, business timescales. (*Source: ITIL [1], Service Design)*

Technology is recognised as a fundamental component of most business processes, and continued or high availability of IT is critical to the survival of the business as a whole. As automation continues universally, ITSCM will not only be considered integral to BCM but the pair will merge as one.

Key steps

To understand exactly the importance of IT to your organisation and therefore the strategy needed for continuity management, the first steps are to undertake a business impact analysis (BIA) and risk assessment.

Note: For brevity I am deliberately choosing to step over the process 'Initiation' stage activities (e.g. policy setting, scope, roles, responsibilities, reporting, etc.) in this paper; not because they are unimportant but in reality I find them to be iterative and they tend to be derived after the following stages have been at least attempted.

1. BIA

A BIA will identify a number of key factors that will enable effective decisions to be made when considering risk reduction and recovery options, and these factors include:

- What are the financial impacts of a loss to each business process?
- What are the non-financial impacts?
- How that damage or loss will escalate as time progresses:
    - What is the maximum outage than can be tolerated?
    - How long would it take to clear the backlog of work?
    - How much data loss could be tolerated?
    - What is the minimum level of service required?
- Are there any business critical periods?

[1] ITIL® is a registered trademark of AXELOS Limited

- Are there any future business developments which may affect business continuity parameters?
- What are the minimum human resources, facilities and services required to enable vital business processes to continue?
- What is the business priority of each of the services being delivered?

The output from the exercise can be presented in a number of formats (e.g. worksheet, graphic) and it will show the detrimental effect on the business when a service becomes unavailable for a period of time and enables the impact to be quantified in business terms.

2. Risk Assessment

This assessment looks at the level of likely threat exposure, and the extent to which your organisation is vulnerable to that threat. Therefore it can be defined as two quantifiable components:

Impact – the extent to which an organisation is vulnerable to a threat.

Probability – the likelihood of a threat materialising.

The main benefits of the assessment are:

- Risks are proactively identified instead of being ignored
- Risks are prioritised so that the most effective use can be made of limited resources
- Steps can be taken to reduce the likelihood of occurrence and the potential consequences
- A culture is developed where risks are openly identified, discussed and managed.

The outcome is best presented in a graphical risk profile with each risk plotted on a grid pattern. This helps to focus attention on the most severely impacting and most likely risks at the same time as defining those that can be considered 'acceptable risks'.

It is important to remember when doing this that risks could have a positive or a negative effect. Failure to make a change to exploit an opportunity for example, could be a risk in itself.

Following the assessment an analysis can be performed to determine appropriate risk responses or risk reduction measures to manage each risk. The responses should be implemented to reduce either the impact or the probability, or both.

A reactive approach to dealing with risks is no longer acceptable. Directors have a 'duty of care' to shareholders, service users, employees and creditors and could find themselves personally liable if found to be negligent.

3. Strategy

Once the analysis has been done, an appropriate strategy should be developed in line with the business needs. The strategy will need to balance the risk-reduction, recovery and continuity options with cost; where the cost of deploying any measures will have to be weighed against the likelihood and cost to the business of that particular risk materialising.

The continuity options that need to be considered when developing the strategy are:

- **Do nothing** – based on what we've already reviewed in this paper this option may seem highly unlikely. However, there could be scenarios where this could be chosen e.g. where a solution to restoring service is imminent. Of course, it could be attractive due to low cost! If there is a conscious decision to use this option it needs to be well documented and signed-off to prevent recriminations should a failure happen.
- **Perform manual workarounds** – for very low impact services which can be lived without for a period of time. The option can be effective as an interim solution but has little benefit for complex processes. It is relatively cheap but training, accurate procedures and testing are imperative. It can also suffer with insufficient staff being available (with regard to the catch-up and recovery).
- **Reciprocal arrangements** – an arrangement with another organisation using similar technology to use their equipment. An example I have experienced is where two

service providers shared the provision of Service Desks in different locations. Normal operations saw load balancing across the desks but the continuity plan involved one desk taking the entire load in the event of a failure at the other. Again this option is relatively cheap.

- **Gradual recovery** - also known as cold standby, this solution is used for systems that typically don't need to be restored for 72 hours or more. This is the provision of a computer environment but without any computer equipment in it, meaning that the required computer equipment has to be installed and then the relevant services and data built on to it. Rental costs need to be considered and good back-up procedures are necessary (plus there's a need to ensure that back-ups are not stored in the operational environment!). The testing possibilities of this option can be limited.
- **Intermediate recovery** - also known as warm standby, this typically involves the re-establishment of critical service within a 24 to 72 hour period. This is a computer environment with equipment in it, which will need the relevant services and data recovered on it but where full recovery can usually be achieved within 48 hours. Due to the complete infrastructure being present the costs of this option are considerably higher. Good back-up procedures are necessary and regular testing is imperative.
- **Fast recovery** – sometimes referred to hot standby, this option typically has a target recovery time within 24 hours. This is similar to the intermediate option, but where live data is mirrored to the facility.
- **Immediate recovery** – with near instantaneous if not immediate restoration of service. This is where an organisation has duplicate systems running in parallel, at different sites, mirroring critical business systems. This facilitates an immediate and seamless takeover of running services by one site when the other site fails.

The strategy that best fits an organisation is likely to include a combination of risk response measures and a combination of the above recovery options.

A standard framework, such as M_o_R (Management of Risks) should be utilised when performing these activities. The strategy developed is likely to be a combination of the above risk reduction and continuity options (depending on the earlier assessments that have been performed), whilst ensuring that the relevant strategies are cost-justified.

Finally, remember to include the chosen option(s) and expected performance levels in your Service Level Agreements (SLA).

Summary

We have seen how service failures can cost a business financially, harm its reputation and cause a loss of customer confidence (and possibly loyalty). When such failures are protracted due to a lack of contingency awareness and planning the damage is compounded.

Now is not the time to put your head in the sand but steps should be taken to ensure risks and IT management processes are assessed and corrective action taken to be prepared.

Finally, some key thoughts and messages for you to takeaway:

- Education and awareness – This ensures all staff are aware of business and service continuity and that these aspects are part of their normal work. Make sure everyone knows what to do and how to do it!
- Regularly communicate the ITSCM objectives within the Business / Customer areas
- Perform (and regularly repeat) a BIA and strategic alignment with BCM
- Perform assessments and analysis (both process and risk)
- Based on the output from the assessments, prioritise improvement actions and activities
- Review how major incidents are managed. The effectiveness of the Incident Management process and Service Desk can strongly influence the overall recovery period
- Include Disaster Recovery and non-standard working in SLAs to align with business requirements and manage expectations
- Initiate (if not already done) proactive Problem Management to minimise risk

When the time comes…and it will come… how will you respond?

Neil Walker

Principal Consultant at Fox IT

About Fox IT

Fox IT®[2] has been a leading Information Technology Service Management (ITSM) and governance business for over 30 years. We provide a range of practical and effective consultancy solutions designed to create agile, proactive, responsive IT organisations providing excellent IT services in alignment with our clients' goals to support and drive continuous business innovation. We achieve this by empowering your people with best practice training, developing and implementing the right operational processes and using properly configured and integrated tools to enable IT Services transformation.

To discuss how we can assist you in transforming your IT services or in obtaining ISO/IEC 20000 certification please call us now on +44 (0) 333 202 1018.

Please come and join in the latest ITSM conversations on our social media pages:

Facebook: www.facebook.com/FoxIT.ITSM

Twitter: @FoxIT_ITSM

LinkedIn Company Page: www.linkedin.com/company/fox-it

LinkedIn Group: https://www.linkedin.com/groups/Fox-IT-ITSM-Today-7456241/about

[2] Fox IT ® is a registered trademark of Fox IT SM Limited