A risky business

Why you can’t afford to gamble on the resilience of business-critical infrastructure
Banking on a computer system that never fails?

Recent failures in the retail banking system show how critical computerised systems are within the banking environment, not to mention the catastrophic effect failures can have on both individuals and the UK economy. Given the potentially devastating nature of any failing, the risk should have been identified, declared and mitigated to ensure that the impact of any failure would be minimised.

The Financial Services Authority (FSA), as part of its remit to govern risks within the banking sector, has oversight of the risks being taken by retail banks and can act to ensure that these risks are managed. Initially the FSA called for an assessment of infrastructure risk by the end of September 2012. Retail banks must now declare their technology risks and are subject to risk audits* either by the FSA or a nominated person, under the powers granted in section 166 of the financial services act.

Identified risks will need to be acted on and mitigated to ensure that the overall risk profile of the technology within the bank is at an acceptable level. Given the new directives making CxOs responsible for risks within their operation, and a recent fine of £500,000 imposed on Peter Cummings of HBOS for business risk failures, there is concern that a similar level of personal liability for technical risk will rest personally with the CxO.

*The FSA recently set out a tender to the major consultancies for a framework agreement. It’s expected that this framework will be used to conduct audits under section 166, reinforcing the threat of audit as the resources will be in place to carry out the work.
Identifying the five key technology risks

A key requirement is to identify, evaluate and mitigate the risks within the technology environment. This will provide both the input required by the FSA and a basis for on-going improvement within the infrastructure to reduce those risks to acceptable levels.

Applications and the underlying network infrastructure are vital to the operation of any retail bank. Any failure in either area could cause major issues for the bank, its customers and its trading partners. At the same time, new methods of working in the IT industry, including device virtualisation, are making the network a key part of the IT infrastructure, with users unable to process transactions unless communications networks are operational.

The network infrastructure also delivers voice services to customer contact centres, trading floors and enterprise services. These new delivery mechanisms increasingly expose voice services, which were operating over segregated services, to the risks inherent within the data network. Voice services are critical as they’re still many customers’ preferred way to contact their bank.

Key risk issues

Technology risks can broadly be split into five areas:

1. **Risk of failure**
   - Loss of part or all of the applications or network infrastructure, this risk is increased if the environment has not been constructed with fault tolerance as a base requirement.

2. **Process risks**
   - Failure of any part of the process required to actively manage the applications or network infrastructure. This could range from change management, fault management and escalation process to on-going capacity management processes.

3. **Security**
   - Failure or loss of assets or data due to the actions of internal staff or third parties which compromises the confidentiality, integrity or availability of the environment. This is a major area of focus in any financial services company, however the risks in the environment caused by security must be factored into the overall position.

4. **Obsolescence**
   - Increased risks due to the technology no longer being supported leading to a lack of manufacturer repair and a depletion of knowledge of the system.

5. **Business continuity and disaster recovery**
   - Systems and processes designed to support a complete failure of part of the infrastructure and to restore service using separate facilities with no loss of data. Disaster recovery can either be instant or brought on line with a planned start-up delay. For this paper the lines between disaster recovery and business continuity are blurred, both are treated as the same issue.

All of the above apply right across the environment. To understand the risks it’s necessary to split the network and applications infrastructure into its key components, evaluate the risks in each part and build up an end-to-end picture by business service. This would also identify areas where common risks occur allowing remedial action to be initially targeted to those areas delivering the greatest return.

Meeting the challenge head on

BT provides both network infrastructure and compute services for customers and, as such, can offer consulting expertise and solutions in these areas. Initially we can help identify areas of risk within the network infrastructure, with a view to providing suitable solutions to mitigate those risks and reduce them to acceptable levels.

As IT systems become more complex it’s possible for a risk in the underlying delivery system to affect wide parts of the infrastructure and lead to the loss of business services. So risks must be identified in a systematic manner, with their impact identified across the estate and not limited to the specific systems where the risk resides. We look at the five key areas to identify risks and make recommendations for improvements.

1. **Risk of failure**
   - The risk of failure of end-to-end delivery systems is normally mitigated by both building high availability into a single system and having a fallback system or capacity capable of restoring service in line with business requirements. For data services, this could be a spare router and network link or a virtual machine where software can be quickly activated. For voice services, this could include number re-routing or using of the public telephone network to route to another part of the contact centre.

   BT’s infrastructure services offer varying resilience levels designed to meet different business requirements. Resilience can be provided both in terms of physical devices and for the access circuits required to connect the site to the BT core network. Offerings range from non- resilient to fully diverse connectivity offering separation at duct, equipment and BT Point of Presence (PoP) level. We’re also delivering new technologies such as superfast broadband, which for backup purposes provides the ideal combination of cost and functionality.

   Our core networks are constructed with full resilience and true underlying diversity to minimise failure and maximise availability. We can provide multiple and diverse physical connections across the core for high availability applications, enabling BT to provide the benefits of using two separate provider networks through a single organisation which can guarantee diversity at all levels.

   Within data centres, best practice is to build a fully resilient infrastructure with automated failover to reduce service risks. With BT, this is backed up by both on-site spare parts and maintenance contracts to repair failed facilities within short timeframes (less than 1 hour is normal for manned centres). Our data centres conform to the Uptime Institute’s Tier 3/4 specification for availability.

   Systems should also be attached to the network in a resilient manner where required, allowing a single connection (or combinations of network components) to fail while maintaining service through alternative or diverse routing. This may also be accomplished by using load balancing equipment (e.g. F5 supplied by BT) to offer service through sets of systems rather than individual hosts as well as other appropriate cost-effective high availability and/or failover infrastructure.

   Identifying risk requires inspecting end-to-end flows to identify all critical components and interdependencies forming part of the service delivery. Once the relevant systems have been identified, the software and services running on those systems also needs to be identified.

   Failure may not be restricted to systems; loss of service may cause employees to be unable to continue to function thus causing service issues within the remaining environment. Failure recovery plans need to ensure that an alternate mechanism is available so that service levels to customers are maintained during these interruptions.
Process risks

Service management and service processes should conform to ITIL standards to ensure that problem and incident management processes are both appropriate and ‘fit for purpose’. BT has certified its operational capability to ITIL standards which reduces the risk of process failure.

Three process areas are particularly important for reducing risk within the environment:

**Incident management**

A robust process for managing and controlling incidents is needed to ensure that they are fixed in a timely manner (or appropriate, as minimum time fix may interfere with business as usual). BT’s processes based on ITIL standards define the full incident lifecycle, with appropriate escalation and post-incident reviews to help understand root causes and how similar incidents could be managed more effectively, improving future response and reducing the chance of recurrence.

**Capacity management**

This is becoming increasingly vital in networks where high demand applications are sharing facilities with key business applications. Understanding capacity usage and trends are vital to planning the network and ensuring that overload conditions do not prevent the business operating.

**Change management**

A significant majority of network incidents can be traced back to a change within the environment. Managing change lifecycles, including scheduling, implementing, testing and having appropriate restoration plans is critical to maximising service availability of the infrastructure. BT has proven change management methodologies, which adapt to the speed of change required and the level of risk that can be taken.

The above processes should be refined on an ongoing basis to ensure you benefit from learning and best practice in a variety of environments.

Security

Security risk management is highly developed in retail banking and is a significant area of on-going investment, both from an equipment and management systems perspective. Increasingly banks are taking advantage of all communications channels (internet, phone, email, chat etc.) for client interaction, but each of these channels requires risk management and threat assessment as they are in the public domain.

There’s also a significant threat to banks’ operations from internal staff, requiring supervision and monitoring to ensure they do not abuse privileges. There have been many recorded incidents where trusted staff have used their access to information for their own benefit, damaging both the reputation and financial position of their companies.

We can help customers with a managed security services offering where security risks are understood, controlled and managed through a BT specified and installed infrastructure. This infrastructure consists of multiple layers of firewalls and intrusion detection/prevention systems along with the management controls to mitigate risk.

We can advise on security and threat management regimes applicable to both internal staff to new legislation (e.g. PCI compliance) and conformance with the international standard for an Information Security Management System (ISMS). This is provided through professional services to identify requirements and recommend solutions.

Denial of service is also a key threat which needs to be mitigated. This threat is increasing, as highlighted by recent attacks on major global banks, and both sourced from criminal activity and state sponsored sectors. BT can help mitigate these threats with sophisticated denial of service protection systems and services.

Obsolescence

Manufacturers limit the support life for their equipment and after an end-of-life date it’s no longer possible to get their support for the equipment, although spares and engineering support are often available on the secondary market. End of life is normally reached through a series of events, as follows:

- **End of sale**
  - When the item is no longer available for purchase.

- **End of support**
  - Where no new bug or vulnerability releases of software will be made available.

- **End of life**
  - Where the equipment is no longer serviced in any form by the manufacturer.

These events are usually separated by several years, but as devices pass through the cycle the risks associated with continuing usage increase. To reduce risk it’s vital to ensure that the end-of-life cycle is known for each piece of equipment and a suitable replacement plan is made to ensure that the equipment is remediated before it becomes obsolete.
We can help plan for end of life in the following areas:

<table>
<thead>
<tr>
<th>Inventory management</th>
<th>Identifying specific assets, their end-of-life dates and current status, including both live and disaster recovery systems.</th>
</tr>
</thead>
<tbody>
<tr>
<td>EOL planning</td>
<td>Planning suitable upgrades and changes to equipment to ensure that potential end-of-life equipment is removed from the estate. This may be a simple upgrade or a complete redesign of the affected systems to take advantage of new capabilities.</td>
</tr>
<tr>
<td>Contractual support</td>
<td>Building equipment refresh cycles into service contracts.</td>
</tr>
</tbody>
</table>

We can also help customers faced with large end-of-life estates by working with the manufacturers to extend support, where appropriate, while the necessary changes take place. This may be necessary where large amounts of equipment need to be changed which can take several months.

Business continuity and disaster recovery

Business continuity (planned reaction to a service failure) and disaster recovery (reaction to an unplanned incident) are required to restore service to acceptable levels during disruptions (ranging from small-scale outages such as systems failure to large-scale issues such as complete loss of data centres). At present there are no specific requirements for either business continuity or disaster recovery centres however it’s expected that industry best practice will be imposed on individual banks to ensure timely service restoration.

By using one of our data centres, located throughout the UK, to host critical applications and systems as either live or standby capabilities we can deliver appropriate disaster recovery services. Our service includes the specification of disaster recovery processes, the build of new centres and the transfer of existing services to those centres.

When selecting a disaster recovery centre and identifying the critical business applications to be duplicated in that centre, it’s important that a single disaster will not cause service loss to both centres, or cascading failure where unpredictable impacts occur on other services. We can help with disaster recovery planning covering the following areas:

<table>
<thead>
<tr>
<th>DR architecture</th>
<th>Reaction to unexpected failures; areas covered include resilience, location of data centres and separation of facilities.</th>
</tr>
</thead>
<tbody>
<tr>
<td>BCP plans</td>
<td>Defining failure events, response to those events and how the infrastructure will be adapted should an event occur.</td>
</tr>
<tr>
<td>Utilities</td>
<td>Ensuring separation from other data centre(s) to reduce risk of simultaneous failure.</td>
</tr>
<tr>
<td>Interconnection of data centres</td>
<td>Connectivity between data centres based on BT’s high speed fibre network scaled as appropriate to DR mechanisms employed. This needs to factor in performance and latency requirements of specific services (e.g. SAN replication).</td>
</tr>
</tbody>
</table>

Data replication | Replicating critical data to critical data recovery sites to support minimal data loss during failure. |
<table>
<thead>
<tr>
<th></th>
<th></th>
</tr>
</thead>
<tbody>
<tr>
<td>Switchover mechanisms</td>
<td>Live/live or live/standby operation for the centres and relevant applications.</td>
</tr>
</tbody>
</table>

Overall, planning for business continuity and disaster recovery is a large, complex area where BT has significant expertise to help optimise recovery and costs. We have expertise in planning for business continuity in accordance with ISO 22301 the International Standard for Business Continuity Management. BT also has the facilities to host DR operations and to provide the underlying communications infrastructure to customers’ sites.
Going forward

We expect financial services requirements to continually change as best practice is adopted and services evolve, making best use of the underlying infrastructure. This evolution could either be through industry norms, the emergence of new technology or regulators implementing new regulations to minimise risk.

There is a legal requirement around information security within the UK/EU to have risk management across the estate as a regular part of the IT services infrastructure, with specific goals to reduce key business risks to an acceptable level. Risk assessment should be performed both at regular intervals and when changes are made to the estate. Removing risk is not always possible, however mitigation strategies can help to limit the likelihood of occurrence, impact and time taken to recover service to original levels.

A robust approach to evaluating risks and accepting them onto risk registers should be taken. There’s concern that internal divisions may use a risk-based approach to managing infrastructure as a way to get items escalated, by raising risks which may not necessarily have a genuine business impact.

Summary

Computerised systems are critical within the banking environment, and any failures can have a catastrophic effect on both individuals and the UK economy.

The Financial Services Authority (FSA) has called for an assessment of infrastructure risk and retail banks are subject to risk audits.

Identified risks have to be acted on and mitigated to ensure that the overall risk profile of the technology within the bank is at an acceptable level.

A key requirement is to identify, evaluate and mitigate the risks within the technology environment:

- risk of failure
- process risks
- security
- obsolescence
- business continuity and disaster recovery

Risk assessment should be performed regularly. Removing risk completely isn’t always possible, but mitigation strategies can help limit the likelihood of failure and its impact.
We can help reduce risk
Visit www.bt.com/gbfm for more information on BT for Financial Services