Business Continuity and IT Disaster Recovery

TA Industry Guidance

This document is for the use of TA Forum members only and is for guidance purposes. This document must not be copied or distributed without written consent from the TA Forum.

Contents

This document is for the use of TA Forum members only and is for guidance purposes. This document must not be copied or distributed without written consent from the TA Forum.

1. Introduction

The purpose of this paper is to provide guidance to our members in respect of the core processes that should be considered in relation to operational and IT resilience.

2. Governance & accountabilities

An Operational and IT Resiliency framework should be established and maintained to comply with applicable industry standards and regulatory requirements for all regions in which the TA operates.

Through this framework, the TA must articulate its resiliency vision and core values to all interested parties and ensure that strategic direction, coherence and clarity are adequately embedded in all resiliency decision-making.

Roles and responsibilities along with appropriate resiliency governance also need to be included within the framework, which provides baseline expectations for the development, implementation and maintenance of continuity, response and recovery capabilities for the TA.

3. Business continuity planning

The TA needs to establish and maintain executable and validated Business Continuity Planning solutions to ensure a confident readiness and recovery response to mitigate risk-impacts from a disruption event. These include:

3.1 Alternative procedures

The TA needs to evidence alternate procedures for all critical tasks in the event of system failure with the aim to deliver an uninterrupted service to their clients and investors.

Against each critical task the TA will set out the following information as part of their alternate procedures

- Business outage scenario
- Business owner(s)
- Alternative procedure
- Agreed owner for each task within the alternate procedure
- Key internal and external contacts
- Impact if service is interrupted (including Regulatory and SLA impact)
- Communication Plan

This document is for the use of TA Forum members only and is for guidance purposes. This document must not be copied or distributed without written consent from the TA Forum.

- Testing (invoke alternate procedure or conduct table top exercises)
- Review date
- Senior business leader sign off

Each critical task should be reviewed on a regular basis and signed off by a senior business lead at least annually.

If acting as TA provider then the Fund Manager / ACD should review these procedures as part of their annual review.

3.2 Site arrangements and live testing

BCP Recovery Sites

Contracts are maintained with third party specialists for the provision of workplace recovery services and locations. These workplace recovery locations provide access to IT networks and all key systems and applications, in the event that it becomes necessary to invoke a Business Continuity plan. Seats are provided on a dedicated or syndicated basis.

A SLA needs to be in place with the recovery site for the provision of the contracted desks. The number of desks is determined by the way of a business impact analysis.

On a regular basis (at least annually) performance tests of the facilities and IT set up process are conducted during normal office operating hours using live work. The objectives are as follows.

- To provide a number of work stations with a live desktop image at the recovery site with connectivity to the company's network.
- To test the capability of the site to access the company's network; servers; file infrastructure; applications; internal and external websites and third party portals.
- Each business line to carry out their critical activities from the site to confirm that the business can operate normally during such an outage.
- A lesson learned document will be completed ensuring all identified gaps are tracked through to resolution.

This document is for the use of TA Forum members only and is for guidance purposes. This document must not be copied or distributed without written consent from the TA Forum.

Alternate Office Locations

If a TA has more than one office in the region staff from critical functions will be redeployed in the event of a site outage. Staff in non-critical function would be asked to vacate their workspace in order to accommodate these employees.

Teams will test system access in nearby locations on an ongoing basis to ensure they are able to process live work. Software and hardware must be in place if the primary office is unavailable. This will include card readers, contact centre equipment etc.

Remote Working

Certain outages can mean that employees are unable to travel to a primary or secondary location i.e. adverse weather, contagion, civil unrest, terrorist attacks. In this situation the TA would invoke cross regional recoveries but should allow for staff to work remotely. This could either be from home or a site with a WIFI connection.

Remote working can be via a laptop or a virtual desktop where the employees profile is stored in a datacentre away from the primary location. Testing to be conducted on a monthly basis to ensure the company's network; servers; file infrastructure; applications; internal and external websites and third party portals are available.

An official remote access test to be carried out annually to ensure the company's system infrastructure is able to cope with a large number of employees accessing the system remotely on a particular day.

Recovery options should not include remoting into a desktop in a user's primary location. It should be assumed that an outage would remove power from that location.

3.3 Cross regional

This is where a TA operates a dual site location where if one site were to experience a disaster or an outage then the other site can continue to operate with no disruption in service. For this to be viable the offices must be located far enough apart to not be affected by the same issue, i.e. power grid failure, adverse weather, political unrest, terrorist activity, contagion etc.

Cross regional testing to occur on all critical tasks for a period of 24 to 48 hours. Testing should occur annually, although more frequent testing is recommended. The primary location should have no access to these critical tasks in order to replicate a real life scenario. If regulatory and SLA deadlines are put at risk the test should stopped and a re-test planned. A risk item should be opened to track the successful completion of the re-test.

This document is for the use of TA Forum members only and is for guidance purposes. This document must not be copied or distributed without written consent from the TA Forum.

Where a location is taking on critical work from another location as part of a test or a real life outage, staff completing non-critical tasks in the receiving location should be re-assigned to the critical tasks to ensure regulatory and SLA deadlines are met. These employees should be trained on these critical tasks and given refresher training on a quarterly basis. Due to segregation of duties that link to the user's system access, DR profiles will need to be setup and activated on the day to ensure these users can support critical tasks.

4. IT resilience/disaster recovery planning

4.1 Application recovery

Recovery Time Objective ("RTO") and Recovery Point Objective ("RPO") are two key metrics that organisations must consider in order to develop an appropriate disaster recovery plan that can maintain business continuity after an unexpected event.

RTO is a metric that helps to calculate how quickly you need to recover your IT infrastructure and services following a disaster in order to maintain business continuity.

RPO is a measurement of the maximum tolerable amount of data to lose. It also helps to measure how much time can occur between your last data backup and a disaster without causing serious damage to your business. RPO is useful for determining how often to perform data backups.

TA's can work on a hosted service; have internal IT structures and / or agreements in place with a number of suppliers all with different RPO and RTO options. The time requirement without critical services or the time to the last recovery point needs to be agreed by each member with guidance from their vendors and the clients they support.

A TA reviews their IT infrastructure, services and list of applications and assigns an agreed RTO to each of them on an individual basis. Each application will then be failed over on a regular basis (at least annually) and tested by the business to ensure they achieve their RTO. Any that fail should be re-tested and a risk event opened to track all issues through to resolution.

All RTO's need to be reviewed annually to ensure they are relevant and signed off by a Senior Manager.

This document is for the use of TA Forum members only and is for guidance purposes. This document must not be copied or distributed without written consent from the TA Forum.

4.2 Data centres recovery

Each TA will have their IT infrastructure, services and applications stored in a data centre. A secondary data centre will also be operational and act as a contingency site in case of an outage. Where systems are hosted by an external vendor, the vendor will be required to have a similar setup. Where possible data centres should not be located within the TA or Vendors business office as any location outage could mean both the office and IT infrastructure, services & applications are unavailable.

The data centre will ensure all essential data is replicated in real time across systems with backups stored in case of an outage. Full data sets, including all history, are maintained.

Failover of IT infrastructure, services and applications from the primary data centre to the secondary data centre needs to occur on an annual basis. As mentioned in section 4.1 each application will have an agreed RTO to meet.

Failure to meet an RTO should be re-tested and a risk event opened to track all issues through to resolution.

4.3 STP – DR Capabilities

Due to potential large volumes for STP the BC Plan should include DR capabilities in the event of STP failure. Each organisation should work with their STP providers to create a plan for such events.

In the event of a provider outage a business decision will be made around invoking BCP scenarios to cover dealing.

Investors will want confirmation that deals have been received and placed via the STP provider. If this is not received they may decide to use alternative routes to place the deals.

As a result the TA will need to factor into their alternate procedure

- How they communicate with these investors
- What will happen if the system 'comes back up'
- Will deals start automatically feeding into the system once the issue is resolved
- Will these deals have already been placed via the TA's alternate procedure or been received via a different STP or manual route?
- How will the TA identify and remove duplicated deals before reporting positions

This document is for the use of TA Forum members only and is for guidance purposes. This document must not be copied or distributed without written consent from the TA Forum.

Identifying potential workarounds are vital. The STP provider may be able to assist with sending files manually or allow you to download information directly from their portal. The outage may not be with the STP provider when downstream processes are to blame.

The TA should look to utilise templates which will help with bulk uploads. Quality monitoring will be important to identify any issues, e.g. duplicate deals.

It is essential contact details are up to date with all STP providers.

5. Threat-specific contingency plans

5.1 Cyber Plans, Access and Data Control

5.1.1 Measurement & Effectiveness

Within the financial industry we fully understand that our customers and their clients want to gain assurance over the controls in place to protect the information we hold and the service we provide. To this end organisations should maintain compliance with leading industry data security standards and practices to secure end user data.

5.1.2 Ensuring Compliance

A clear understanding of responsibility not only for following the highest level of industry guidance regarding the implementation and control of information security but also for our own policies and guidelines covering all aspects of how we should behave and what we need to do to ensure the confidentiality, integrity and availability of our information systems and data.

5.1.3 Increasing Awareness

A well-informed workforce is the most powerful defence against security breaches, a significant number of information security incidents occur through a lack of knowledge and incentive. Well informed and trained staff will report and act on threats and incidents that automated process could hope to detect.

5.1.4 Controls

Physical Access
Comprehensive physical security controls need to be in place to protect the premises. This should include smaller sites and onsite security presence at major sites. All restricted areas are secure and physically protected from unauthorised access (both internally and externally), damage and interference. All restricted areas and building

This document is for the use of TA Forum members only and is for guidance purposes. This document must not be copied or distributed without written consent from the TA Forum.

exits/entries are under surveillance. Access to company offices is controlled using an ID card system. Each employee uses their personally issued ID card to gain access.
All visitors must be by pre- arrangement and report to reception, they are signed in on arrival, they are provided with a temporary visitor badge and lanyard which must be visible and are escorted at all times when on site.

5.1.5 Infrastructure

Requirement for a specific investment budget for technology infrastructure projects, covering strategic change, end of life, cost efficiencies, automation and new product releases etc. Regular backups should be performed; they are secured and replicated between disk storage units and housed securely.

5.1.6 Protection in Layers

These should include web application firewalls, vulnerability scanning, anti-virus, code review and pen testing. Intrusion prevention systems should be deployed throughout the network at strategic locations. All organisations should actively monitor industry security authorities, product and service providers.

5.1.7 Testing

Regular testing needs to be conducted by an independent / authorised third party. Test results and any subsequent actions should be resolved and completed in a timely manner.

5.1.8 Access to Data

An access administration policy should be in place that defines requirements to ensure that the right people have the right level of access entitlements to the right systems at the right time. A System Account and Password policy that defines minimum length, complexity and use of passwords, enforcement of periodic password changes and password history should be in place. Such policies should be reviewed and approved annually by Senior Management.

5.1.9 Segregation of Duties

Role based access control model linked to a unique ID which enforces the principles of segregation of duties, least privilege and avoids conflicts of interests. Staff are only permitted to be in one role at a time. Role owners and data owners are required to review access on a regular basis and all processes are reviewed by Security and Audit.

This document is for the use of TA Forum members only and is for guidance purposes. This document must not be copied or distributed without written consent from the TA Forum.

5.1.10 Access Provisioning

Access provisioning is completed through an established process for all the users based on their roles and relevant approvals. De-provisioning ensures that access is revoked upon termination of employment for any member of staff within 24 hours of leaving the company. Any individuals who are transferred to a new role will have their access reviewed and modified to ensure access is appropriate to their role. The new line manager is to review and validate whether the access provided is in line with their new role.

5.1.11 Employee Policy

Employees are trained to lock their workstations whenever they leave their desks. Devices should be automatically locked after an agreed short period of inactivity. All laptops and corporate mobile devices are encrypted and password protected.

5.1.12 Email Protection

Email monitoring in order to prevent data leakage, track email activity and block, or alert, if emails are found to have breached policy regarding the inclusion of personally identifiable information, confidential or proprietary information and emails that have "unreadable" attachments. These emails are captured and reviewed, allowing for retrospective forensic examination of the content.

5.1.13 Policies & Processes

Security standards and policies aligned to ISO 27001. The policies cover the standard industry practices for a secure operating environment. They are reviewed annually and are approved.

Well defined policy details requirements for the appropriate use of corporate Information Systems, Telephone, Facsimile, Internet, Intranet, Online Services, Email and Voicemail. All employees are required to acknowledge that they have read and understood this policy.

Risk based controls are applied in accordance with the data classification. Customer data is classified at the highest level and protected accordingly.

Remote access is only provided for approved requests and is suitably protected. Once authenticated, access is provided via a secure connection and the ability to copy or print data should be disabled.

Exchange of data and software between external organisations is strictly controlled and only made on the basis of formal agreements.

This document is for the use of TA Forum members only and is for guidance purposes. This document must not be copied or distributed without written consent from the TA Forum.

5.1.14 Third Party Management

Responsibility for the protection of data extends to suppliers and service providers, where external arrangements are required to be reviewed as part of policy, which define the necessary oversight and due diligence actions to be performed.

6. Incident Management Framework

6.1 Management team, structure and roles

An incident management framework should be established that focuses on determining the impacts of a disruption, developing a strategy for response, and managing the recovery of impacted systems or processes, along with coordinating the efforts of recovery personnel charged with carrying out that strategy.

The agreement of an incident management organisational structure is an important element of the incident management framework. Suggested roles and responsibilities within this organisational structure are confirmed below. All responsibilities during an incident are related to the role being carried out by that individual and not to their rank or other roles within BAU. This approach ensures that whenever a primary member of the team is unavailable, all of their responsibilities are fulfilled by an alternate during the incident management.

This document is for the use of TA Forum members only and is for guidance purposes. This document must not be copied or distributed without written consent from the TA Forum.

Role	Responsibility
Incident Management Team	Comprised of the undernoted designated roles along with senior critical business service leads (normally heads of location) to provide support and help decision making within the management of an incident
Incident Commander	Provides overall management and authority over an incident
Incident Coordinator	Overall responsibility for the coordination of an incident taking direction from the incident commander
Operational Leads	Partners with the Incident Commander and Incident Coordinator to clarify and validate the operational issue(s), provides regular updates re impact and supports the required resolution
Client Lead	Partners with the Incident Commander and Incident Coordinator and engages with clients using agreed pre-prepared communication templates
Technology Lead	A key business partner who provides technology recovery of critical business services, operating with the business service via established technology incident management processes
Enterprise Resiliency Office	A key business partner who coordinates an enterprise response to incidents in conjunction with the lines of business, including executing on recovery and providing updates to key stakeholders
BCP Coordinator	Ensures BCP plans are in place and maintained for critical business services

An incident management playbook should also be created and maintained as part of the incident management framework. The playbook details the key resources, personnel and actions required to respond to an incident with the objective of ensuring the continuity of critical business services.

This document is for the use of TA Forum members only and is for guidance purposes. This document must not be copied or distributed without written consent from the TA Forum.

7. Communications and stakeholder management

7.1 Stakeholder Communications

The organisation shall determine the need for internal and external communications, including implementing and maintaining supporting procedures/protocol/strategies relevant to the incident including:

1. On what it will communicate (via pre-approved templates where possible)
2. When to communicate
3. With whom to communicate, which may include:

    a. Internal stakeholders
        i. Employees
        ii. Parent company (if applicable)
        iii. Client
        iv. Vendor

    b. External stakeholders
        i. Emergency services
        ii. Clients
        iii. The Media
        iv. Regulators (FCA/ICO)
        v. Fund accountants
        vi. Trustees
        vii. Pricing agents
        viii. Depositories
        ix. Insurers/insurance brokers
        x. External lawyers/legal support
        xi. Staff welfare services
        xii. Other key critical suppliers or outsourcers (e.g. Calastone, Euroclear)

    c. Other defined interested parties

The organization should have a process in place for receiving, documenting, and responding to communication from interested parties in consideration of their requirements. This process must be achievable during a disruptive event.

This document is for the use of TA Forum members only and is for guidance purposes. This document must not be copied or distributed without written consent from the TA Forum.

7.2 Communications

Employee Communication

A call tree should be in place for advising, updating and activating employees by telephone. This can be done manually or using an automated system.

Automated systems allow TA's to interact with employees via a standard telephone message to a work, home or mobile device. This can then be followed up by text message, e-mail or notification via an app. It provides quick and widespread communication at a key time and allows an employee's response to be recorded and reported back to the Incident Management Team in real time. Although an automated system is beneficial it is not essential.

It is important that each TA has details of its employees online and in hard copy. An outage may not allow access to computers, laptops, networks or drives. The Incident Management Team need to be able to contact all of its employees during an outage not only to advise but to ensure that they are safe (also see 8.1).

Employees contact details should be updated on an ongoing basis. If possible this should feed from a HR central system to ensure records are maintained in one central place. Employees should be asked regularly to review their contact details and confirm they are correct. Under GDPR regulations employees need to be allowed to opt out of these communications if they so wish.

Regular Testing

Bi-annual tests should be held to ensure automated and manual call trees work and include all current employees.

Employee acknowledgements need to be recorded and monitored. Industry standards are currently within 2 - 4 hours for staff replies (shorter timelines for specific crisis management staff members).

In order to pass a test a TA should be able to communicate and obtain employee acknowledgement. A recommended pass of rate of 70% is recommended. All failures should be investigated to ensure issues can be resolved if required.

Third Party Suppliers and Key Business Partners

- Ensure regularly updated organisational structure charts are communicated.
- Contact details for key business partners to be held. To include out of hours contact details and escalation points.

This document is for the use of TA Forum members only and is for guidance purposes. This document must not be copied or distributed without written consent from the TA Forum.

- The TA to hold contact details for all vendors; suppliers; clients; trustees; fund managers; fund accountants, legal entities and regulators. List to be available electronically and in hard copy for use during a BCP event / system outage. To include out of hours contact details and escalation points. During an outage these groups (or a sub section of these groups) should be updated on a regular basis using a pre-defined template.

- Key internal contacts to be provided to vendors; suppliers; clients; trustees; fund managers; fund accountants, legal entities and regulators to ensure issues at their end are communicated to the correct people in a timely manner

8. Staff Welfare

8.1 Duty of Care

Putting your employees' well-being at the top of the list in your disaster recovery planning will help them recover quicker and be more productive when they return to work. So, what should you do or put in place?

- Have your employees' contact information readily available and updated.
- Contact them as soon as possible, and find out if they're safe and accounted for.
- Offer flexible working practices e.g. working from home, flexible hours/adjust working patterns whilst BCP is in force.
- Consideration to be given to other people issues that might occur e.g. transport home, staff displacement/relocation arrangements (can organisation offer alternative accommodation?)
- Check in with them on a regular basis, and stay up to date with their individual situation.
- Keep them informed of next steps.
- Open a bridge line so that employees can ring in and get the latest information from one central location.
- Promote Employee Assistance Programme (other support e.g. counselling, financial advice etc.) if employees have been affected emotionally in any way to the disaster/emergency.
- Encourage managers to set up meetings so their teams can talk to each other about what happened.

This document is for the use of TA Forum members only and is for guidance purposes. This document must not be copied or distributed without written consent from the TA Forum.

- Remember that everyone is an individual and will have unique situations and needs – this is not a time to use a blanket solution. It doesn't work in a disaster. Be flexible.

- Plans should provide for a range of responses, including a group debriefing to take place 48 to 72 hours after an event, plus follow-up support including access to telephone counselling for individuals. In the case of catastrophic events affecting many employees, organisations should consider a large group meeting or crisis seminar, held in a temporary building. This should provide practical information but also cover employees' potential psychological reactions and provide staff with the opportunity to join a formal debriefing at a later stage.

Severe Weather

In devising a severe weather and disruptions to public transport policy, employers should seek to balance the need to minimise disruption to their business and the need to ensure the health and safety of employees. Whilst a large part of severe weather preparations will be included elsewhere in BCP documents some points below should be raised in terms of duty of care

Employers should not encourage employees to travel in severe weather. Although an employer would not normally be liable for the acts of its employees when travelling to and from work, the courts have shown an increasing willingness to hold an employer liable for the acts of its employees taking place outside working hours where the act is closely connected with what the employer authorised or expected of the employee in the performance of their employment.

A few points to consider below:

- Employees should use their best endeavours to attend work in all circumstances. However, it is not the organisation's intention that employees put themselves at unnecessary risk when trying to attend work. Members of staff should use their own judgment and, if unable to attend work, contact their line manager as soon as possible.

- Organisations should decide on a case-by-case basis whether or not it is appropriate for employees to leave work early. When making this decision, they should take into account the employee's circumstances (e.g. distance from their home to work and the mode of transport), the employee's views and the needs of the organisation.

- Can we offer flexible working practices e.g. nearby accommodation, working from home, flexible hours/adjust working patterns to lower the risk of employees travelling?

This document is for the use of TA Forum members only and is for guidance purposes. This document must not be copied or distributed without written consent from the TA Forum.

9. Training and awareness

9.1 Staff training

Each TA should ensure staff training on BCP is conducted on a regular basis and evidenced for future client / audit reviews. This should include

- Building evacuation plans (including yearly tests)
- Understanding how roles / teams would recover in a building outage
- Details of the DR site(s) *
- Understanding cross regional plans (if applicable) ensuring training is up-to-date
- The need to take laptops home on a daily basis
- Awareness of alternate procedures and input in review sessions
- Ensuring employee contact details are up-to-date
- Access for all employees to the BC plan.
- Recovery team members (in non-critical roles) to be trained on critical tasks on a regular basis in order to perform this role during an outage

* Visiting the DR site should occur at least annually with 50% attendance of the allocated seats. Testing should occur on live work and test plans should be completed giving relevant feedback. Any failures should be re-tested and a risk event opened to track all issues through to resolution.

Incident Management Team members should have additional training and ongoing review sessions in order to understanding their roles in an outage. Lessons learnt reviews should occur after all large outages and processes updated where required.

This document is for the use of TA Forum members only and is for guidance purposes. This document must not be copied or distributed without written consent from the TA Forum.

10. Third party vendors

The TA should define and list all vended systems. They should fully understand what process the vended system supports and how the vended systems interact with their own systems both autonomously or through manual processing

A process map of all system interactions both internally and vended should be maintained with easy access so that a prompt impact study can be made off the back of any system issues experienced

The TA should have clear relationship contacts with the vendor ensuring wide coverage of support hours as well as back up personnel should first point of contact fail. A defined escalation protocol should be in place and reviewed bi-annually to ensure contact points are accurate, relevant and up to date.

The TA and vendor should have clear and relevant SLA's in place in terms of turnaround time and focus depending on differing levels of issue severity. The SLA should be cross directional to ensure both parties meet their obligations successfully when needed.

The TA must have a DR/BCP fail over plan in place and documented with the vendor additionally complimenting any bespoke specifics the vendor may support outside of an off the shelf product.

The plan should be reviewed by both parties annually or after any event inducing the BCP with any adjustments mutually agreed, implemented to the plan and signed off with relevant version control.

After any BCP event a write up of the issue that occurred, the processes undertaken to resolve, reoccurrence prevention and lessons learnt should be documented and placed on file for the purpose of improving the BCP plan and for reference should a similar incident occur in the future

An annual test should be undertaken with the vendor to ensure the capabilities detailed within the plan are indeed possible, accurate and do not have any significant/material impact on usual timelines associated to the vended system use. The BCP test should see the failover of the live production system to the DR system. Testing of the DR system should be completed within the agreed RTO ensuring data is consistent of that in the live system. Any that fail should be re-tested and a risk event opened to track issues through to resolution.

Where vended systems are hosted within the TA's own infrastructure these systems should form part of the company's own BCP plans and tested annually through DR server fail over processes as well as offsite DR location tests

This document is for the use of TA Forum members only and is for guidance purposes. This document must not be copied or distributed without written consent from the TA Forum.

11. Continuous improvement

11.1 BCP Review

The organization shall, at least annually, conduct a comprehensive review of the BCP and any supporting documentation to ensure it remains suitable and fit for purpose. Interim reviews and approvals should be completed in response to any significant change, internally or externally, that may impact the arrangements in the plan being effective.

The plan should follow a structured review and approval process where senior management can demonstrate engagement/input.

As part of the formal sign off Senior Management must consider the following points:

- Have all employees received the relevant BCP training?
- Can key systems and application be recovered within the agreed RTO?
- If the primary site is unavailable is there a plan in place to recovery at an alternative site or for employees to work remotely? Has this been tested within the agreed RTO?
- If all employees in a location are unavailable can work be picked up in different location to ensure key deliverables are met? Has this been tested over a 24 to 48 period?
- Do you have a process in place to contact all of your employees in the case of an incident?
- Have your vendors successfully completed DR testing? Have business leads reviewed the data and signed it off?
- Do you have an exit strategy if your vendors are no longer able to provide their service?
- Do you have alternative procedures in place for all critical processes? Have these been reviewed and signed off by business leads?
- Are effective Cyber Plans in place? Have these been tested?
- Is there an effective Incident Management process in place?
- Do the Incident Management team have key details to hand both electronically and in hard copy?
- Are all outstanding risks documented and being tracked through to resolution?
- Are key individuals being held accountable? Is this being tracked through the annual review process?

This document is for the use of TA Forum members only and is for guidance purposes. This document must not be copied or distributed without written consent from the TA Forum.

11.2 Lessons Learnt / Review Sessions

Whenever the incident management playbook is invoked, a subsequent process should be undertaken to review the incident, the mitigating actions that were taken by the incident management team (during the incident) and any lessons that were learned. It should also include a review of affected technology that will consider end to end application flows, critical internal and external dependencies and application infrastructure as they related to the issue.

A template should be agreed (example is shown in Appendix A). The template should be completed by the Incident Co-ordinator and reviewed by the Incident Management Team, Technology and the BCP leads. A meeting should then be held with that group to discuss content and agree required actions to improve the incident management process. Actions would be tracked by the Incident Management Team.

Any updates to alternative procedures should be made and then communicated to all relevant parties.

If failures were identified outside of the business then meetings should be held with vendors; suppliers; clients and industry counterparts to ensure gaps are minimised / closed.

12. Important Information

This document is for the use of TA Forum members only and is for guidance purposes. Members may have additional BCP requirements depending on their client's risk approach. This document must not be copied or distributed without written consent from the TA Forum.

Appendices

Appendix A

Event (or Test) Exercise Documentation including Lessons Learned Feedback

Critical Business Service – Senior Manager	
Date of Incident / Exercise:	

Attendees[1]:

Event Description:	**Event Objectives:**

Describe Communication Plan / Material Feedback From Clients Or Any Other Key Stakeholders related to handling of the Incident:

Describe Timeline / Detection / Impact Assessment / Prioritisation:

• **Describe Containment / Mitigation:**

[1] For each attendee, include department and role to assist evaluation that appropriate senior managers and SMEs involved

Lessons Learnt

Observations to Investigate In Order to Improve Incident Management Process / Playbook:		
No	**Items**	**Owner**
1		
2		
3		
4		

This document is for the use of TA Forum members only and is for guidance purposes. This document must not be copied or distributed without written consent from the TA Forum.