NODE4 PARTNER INCIDENT RECOVERY PLAN

INTEGRATED MANAGEMENT SYSTEM

Policy and Procedure

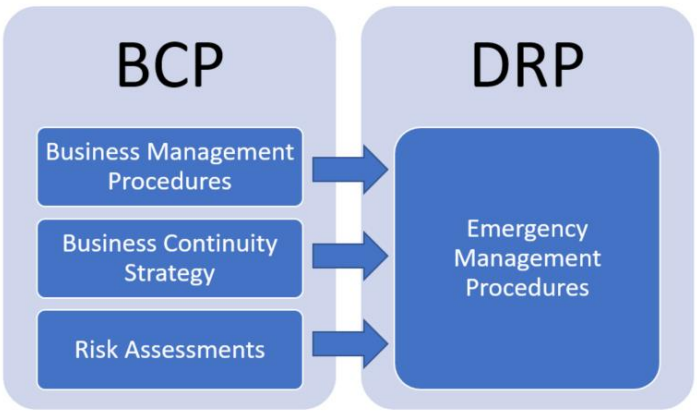
Partner Only

22/11/2022

Version Control			
Issue Version	Date of Creation or Summary of Change	Change Date	Name
5.0	Full review and rewrite	15/11/2022	Alyson Cooling
5.1	Review	25/05/2023	Alyson Cooling

Issue Version	Comments	Approval Date	Director/Manager Name

Definition



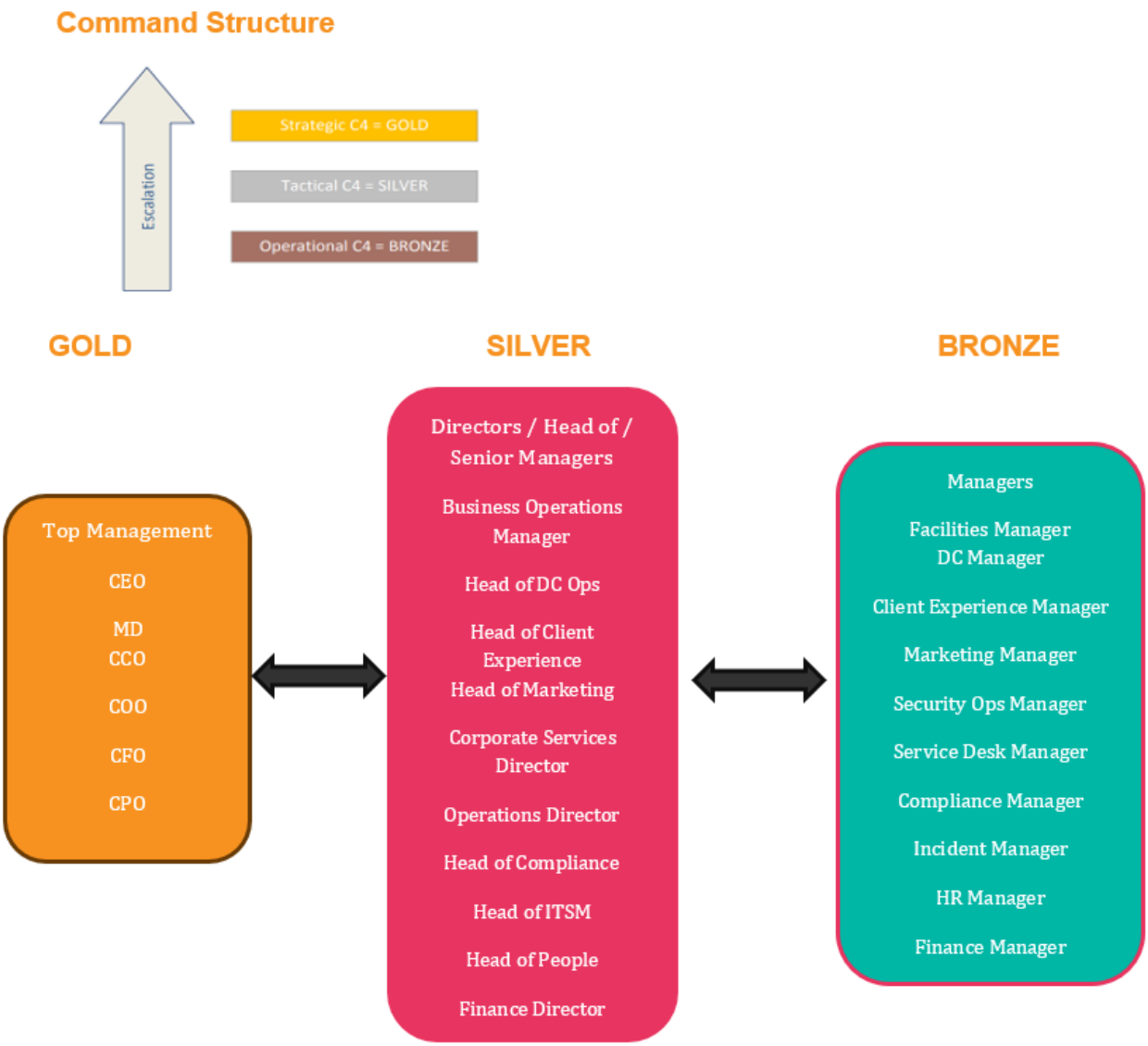
Business continuity describes how the business prepares itself and manages an incident through risk, impact and strategy enabling the continuity of business operations.

Disaster recovery are the steps taken to manage, access the right people, technology, and infrastructure after an incident.

Command Structure

Internal Notification Calling Tree

The calling tree below outlines the key teams involved in DR and the team leaders. The Incident Manager will decide which teams need to be involved.



Disaster Recovery Plan Scope

For this plan, a disaster is defined as loss or damage to all or part of the data centre, infrastructure or offices which would have a high business impact on Node4's ability to provide services to customers.

Elements of disaster recovery (DR) may be invoked if an event raises risk exposure levels significantly before any actual loss of service. This will ensure that the appropriate levels of management are engaged and that the necessary resources are available to help mitigate risks. (E.g., warning of a flood, power interruption etc.).

All Node4 owned sites are included in this scope, namely

- DC1, Pride Park, Derby DE24 8HZ
- DC2, Pride Park, Derby DE24 8HZ
- DC3, Wakefield
- DC4, Northampton

Other sites not under the direct control of Node4 may suffer an outage or disaster that could affect services. These sites have been included in the risk assessments and the risks mitigated where possible by having alternate locations (e.g., dual Point of Presence (POP) for internet breakout, multi-homed internet transit and diverse fibre connections).

Power, HVAC, Fire Suppression, Network, Server, and Security Infrastructures at all sites is included in the scope

Assets Included

This plan is primarily concerned with restoring the operation of core Node4 services and does not include individual DR plans for customers and their equipment (collocated servers, WAN links, etc.). Any customer DR plans that are the full or partial responsibility of Node4 will be documented separately. Due to the nature of services supplied, restoration of Node4 systems on the same site will also cover customer equipment.

Part of the management of a DR scenario involves liaison with customers and controlling access of visitors to site during an incident.

Trigger Events

Events at any Node4 site that would trigger one or more elements of DR or business continuity:

- Total loss of connectivity to one site
- Fire or flood at any site
- FM200 or IG55 Gas suppression discharge
- Loss of building in other circumstances
- Loss of Uninterrupted Power Supply (UPS) backed power
- Loss or extended period of severely reduced cooling capacity
- Extended loss of mains power (>24hours)

Incident Management Responsibilities

Incident Managers have been appointed to contain the situation in which the Business Continuity (BC) and DR Plans are to be deployed. Several incident Managers have been identified to ensure supporting availability if a singular individual cannot be contacted. Their remit is to minimize the impact on service, establish communications with other key personnel and to minimise the time in which normal operations can be resumed.

In addition, nominated Incident Managers' contact information is held by the BT Redcare Contact Centre and Derbyshire Constabulary.

In the event of alarm activation outside of normal business hours, the nominated Incident Managers will be notified, if neither were able to attend the facility, responsibility will be passed to the most senior manager on the corporate hierarchal chart.

The Incident Manager will:

- Assess the scope of the disaster and root cause where possible
- Establish a line of communication to all DR Team Managers
- Ensure emergency services are alerted where necessary and have access to the facility
- Inform stakeholders and customers of the incident and provide regular updates of the situation
- Co-ordinate all staff activities relating to the incident
- Informing Node4's insurance company of the incident
- Control access to the facility for customers

Incident Management – Customer PCI Breach

It is Node4's requirement by the **card brands** to investigate and to assist the merchant in containing any **breach** after receiving a **breach notification**.

A PCI breach wouldn't necessarily initiate an immediate response by the DR team but they may be consulted in relation with a customer.

As a Service provider, Node4 always advise customers to contact their acquirer directly, who will inform the payment card brands.

The Data Controller (the customer) should make the ICO aware within the first 72 hours of a payment card breach. Node4's DPO must be contacted in the event of any payment card data breach.

The Data Controller (the customer) should consider contacting Action Fraud to report the crime as soon as possible.

DR Team Responsibilities

The DR Teams have specific areas of responsibility in a DR scenario to handle communications, system recovery etc. Not all teams will be needed for all scenarios. The appropriate DR teams will be contacted by the Incident Manager as soon as possible following an incident.

Each individual team manager is responsible for mobilising as many team members as is necessary/possible to deal with the situation. Team members may work remotely from home or from another Node4 site during the incident depending on the situation. Some staff may be required onsite to aid recovery.

Infrastructure Team

- Co-ordination of repairs to physical infrastructure (power, cooling, fire suppression, building fabric)
- Co-ordination of temporary infrastructure (e.g. temporary generator sets, fuel supplies etc.)
- Liaison with emergency services
- Control of access to building for staff and customers
- Maintenance of a sufficient standard of physical security

Considerations

Staff and Customer Safety are the primary concerns if the physical infrastructure of the building has been compromised.

Customer Communications Team

- Fielding of customer enquiries by telephone or email
- Updating of websites, tickets, emails, SMS and other communication mechanisms
- Handling/prioritisation of remote hands requests

Considerations

Where possible, technical staff should be left to restore services as quickly as possible without dealing directly with customer issues.

Customers should be directed to a central information source (usually n4status.com) to obtain updates from a consistent, reliable source.

Communications team members must ensure that they give a consistent view of events and avoid speculation or unauthorised comments.

Customer Communication Channels

Node4 have several methods of communicating directly with customers. In a DR scenario, one or more of these channels may be temporarily unavailable, and alternatives should be used. The preferred line of communication is via www.n4status.com

System	Primary Hosting Location	Backup / Alternate Location	Comments
Telephone System	Derby	Alternate Node4 DC	0845 123 2222 and 0845 123 2229 can be redirected by KCOM
Email	Derby	Alternate Node4 DC	
Ticket System	Derby	Alternate Node4 DC	
http://N4status.com	IOVPS (London)	Alternate Node4 DC	Hosted outside Node4 Network. Can be updated over the internet (3G if necessary). Preferred

			communications route.

Press and Media Relations Team

- Issuing statements to press/dealing with enquiries/interviews
- Vetting of statements posted on status sites etc.

Network Recovery Team

- Re-establish connectivity and deal with re-routing of traffic
- Liaison with network providers on faults

Systems Recovery Team

- Recovery of internal Node4 systems (email, CRM, SharePoint, Billing Systems etc.) and restoration of data from backups

Telephony Recovery Team

- Re-establish telephony services and liaise with Telco providers on faults

Resources

The following resources have been considered throughout the creation of the Disaster Recovery Plan

- That the plan has procedural effectiveness 24 hours a day 365 days a year
- That the deployment of the plan may be required outside of normal business hours
- That two Incident Managers, holding senior roles within the company, will manage the incident
- DR Teams will manage communication and technical roles.
- Nominated staff will have knowledge of the location of the Disaster Recovery Plan and the back-up copy to deputise or manage the incident if the appointed Incident Managers were unavailable.

Further considerations

- That the Integrity of the service has been compromised to such an extent that Node4 are unable to meet their contractual obligations
- Normal redundancy/resilience precautions have failed to maintain services (except in the event of a prolonged power outage requiring fuel top-ups)
- Backups of the application software and data are intact and available

- Service and maintenance agreements with hardware and software suppliers are up to date, and both active and passive incident containment machinery are operative
- The incident only affects one data centre.

Risk Analysis

Risk assessments are performed as part of ISO27001 and quality management systems.

The risks considered will include incidents that could lead to a full or partial invocation of the DR plan. The DR plan is part of the ISO27001 and quality management systems.

To reduce the probability of a malicious attack on Node4's Data Centres and to limit the impact on the operational capabilities of the organisation the following active precautions have been taken.

- Node4 Network topology and diverse data centres will allow re-routing of network traffic in the event of a site loss
- Core network equipment and servers are distributed or replicated between sites
- Network connectivity equipment is situated at TeleHouse, and Global Switch, London and TeleCity, Manchester, served by physically diverse fibre connections
- Node4's buildings are safeguarded by a perimeter security fence, CCTV, fire alarms and swipe card technology
- The buildings are secured 24/7 with business continuity for staffing considered.
- The data centres are protected by a self-contained gas suppression system containing FM200 gas and a redundant uninterruptible power supply unit (UPS) and a N+1 diesel generator bank
- Backup hardware is tested by the Technical Manager on a monthly basis.
- The network infrastructure, both physical and logical, has sufficient protection from attack
- The buildings have assessed by local Fire Officers

Temporary Co-location and Office Facilities

Wakefield and Northampton Data Centres have sufficient rack space to accommodate Node4 systems and hardware from Derby.

Northampton and Wakefield have enough office space and the capacity for staff to work in either location or from home.

General Internet transit is available from all three sites, via diverse POPs.

In addition to DC3 and DC4, Node4's 2 data centres in Derby (DC1 and DC2) have separate infrastructures including

- Power supply and backup UPS / Generators
- FM200 Fire Suppression

- Cooling / CRAC Units

Internet connectivity for DC1 relies on DC2. Internet connectivity at other sites is independent (part of MPLS)

Key network components are distributed between the data centres, where possible, providing extra resilience in Node4's core infrastructure. Core network equipment is split between sites and servers are virtualised and distributed. Backups are made across the WAN to each alternative site.

DC3 – Wakefield and DC4 - Northampton are in geographically diverse locations. The DC's are linked to Derby via redundant, diverse fibre connections, in the event of the loss of any one site or fibre link, network traffic can be rerouted. Core services will be distributed as much as possible between sites and MPLS network, multiple POPs will allow routing to be reconfigured in case of an emergency.

DR facilities spread between both data centres can be offered as an option for customer equipment.

Data Backup Process

All core network device configurations, VM images, databases and other business data are backed up on a regular basis. This information is transferred offsite to ensure physical diversity of data. The frequency of backups and retention depends on the nature of the information. This data includes hardware information, network documentation and network diagrams along with all configuration scripts for network devices appertaining to both customer networks (where appropriate) and to Node4's core network.

These backups are verified as part of the daily checks performed by the tech support engineers and are stored in a fire-safe

Core network servers in both data centres are imaged regularly, and the snapshots are backed up as part of this process.

Customer data may also be backed up and stored offsite as part of a full or partially managed DR Service.

Information Security Requirements of DR / BC

Annex A17.1 of ISO27001:2013 states that information security continuity shall be embedded in the organisation's business continuity management systems. Node4 will maintain the controls to ensure the required level of continuity for information security during a disruptive situation.

The DR/BC plan in this document does not involve the use of 3rd party facilities or infrastructure to host people, systems, corporate or customer information for the duration of an incident.

Each Node4 facility is subject to the same set of Information Security policies and procedures and each is connected to the existing network and controlled by the same physical and logical controls.

Remote working is covered by policy and physical equipment transported between sites as part of a DR/BC incident will in line with media transfer policies. This includes the use of secure couriers, transfer with authorised Node4 employees or use of trusted 3rd parties such as Technimove.

If the nature of the incident increases Information Security risk by reducing redundancy levels of infrastructure, HA of systems or offsite backup appropriate mitigation or risk acceptance will be implemented.

Stages of Disaster Recovery and Business Continuity

During an incident advice and guidance given by emergency services and experts will be followed alongside and, in some cases, superseding the Disaster Recovery Plan.

1: Notification and Activation Stage

The Incident Manager will assess the incident and activate all or parts of the Disaster Recovery Plan using the following criteria.

- Triggering events and conditions according to type, severity, impact, and duration
- Analyse and evaluate the circumstances to ensure that activation criteria has been met
- Ensure that all facilities, systems, and staff are available to support plan activation
- Establish a command centre location and communication procedure

Once the criteria have been established the following can be used to form an impact assessment

- Any advice from Emergency Services or Government Organisations
- The structural integrity of the building and whether safe access is obtainable
- Whether mains power exists and whether UPS and generator back up is in operation or bypass/standby
- Telephone and Internet connectivity
- Air conditioning function and capacity
- Whether further interruptions to service are probable and the decision to delay BAU including restoration of service to avoid intermittent faults.

2. Restoration

Once actions have been established by the incident manager including any decisions to relocate an orientation plan for the following should be considered.

- Teams should perform tasks from the plan which includes logistics, expectations and a reporting structure
- An overall co-ordinator should be appointed who will co-ordinate team updates and verify any deviation from the plan
- Date stamped issues and resolutions should be tracked using Recovery Time Objectives (RTO) and the Recovery Point Objective (RPO). The DR manager should implement active time management to ensure issue resolutions maintain momentum
- Define, communicate, and perform regular restoration updates to all interested parties.

Recovery point objective (RPO) and recovery time objective (RTO) are among a data protection or disaster recovery plan's most important parameters. The recovery time objective (RTO) is the amount of real time a business as to restore its processes at an acceptable service level after an incident to avoid intolerable

consequences associated with the disruption. Recovery point objective (RPO) is defined as the maximum amount of data – as measured by time – that can be lost after a recovery from an incident, failure, or comparable event before data loss will exceed what is acceptable or tolerable to an organization.

3: Recovery Stage

The Incident Manager will identify and communicate to DR Managers the need to respond to and assess any damage including new and emerging threats.

These will include

- subsystem damage
- restoration of services from the affected facility or managing relocation to the alternative geographical DC locations and backups performed.
- The need to purchase replacement equipment.
- An assessment of criticality to customers and internal departments to reduce or mitigate any losses
- Dynamic risk assessments should be conducted for physical security perimeters and CCTV
- Validate functionality prior to restoration of communications involving telephony, networks and systems, determine any potential points of data loss
- Continue with defining communication to all interested parties, using the internal calling tree as required

4: Business Continuity Plan and Business as Usual (BAU)

The purpose of the Business Continuity Plan (BCP) is to ensure that there is continuous business operation in the event of an infrastructure or service outage.

The Incident Manager will use the plan to.

- Recover data, infrastructure, and services to enable a continuity of service to all interested parties
- Communicate to all stakeholders the status including interested parties such as the insurance company
- Ensure all fire control equipment, security and Health and Safety systems are fit for purpose.
- Allow the business to operate at full capacity after recovery has taken place

Appendix

Payment Card Brand details supplied below:

American Express

Website: http://www.americanexpress.com/datasecurity

Email: AmericanExpressCompliance@trustwave.com

MasterCard

Website: http://www.mastercard.com/sdp

Email: sdp@mastercard.com

Visa america

Visa Europe

Website: http://www.visaeurope.com/ais

Email: datasecuritystandards@visa.com - for member and merchant requirements

Email: pcidsseurope@visa.com - for service provider requirements