				soft copy. **Service/product lifecycle:** The service and product lifecycle is fundamentally at its 'greenest' when it is built for the long-term. The greatest possible environmental savings can be achieved by using resilient IP infrastructures to pursue a 'one-site, one-pipe' goal and consolidating circuits per location (reducing multiple CPE draining power and associated installation and support visits to location). We understand the Greening Government ICT strategy and the overall requirements to make Government ICT services efficient, sustainable and responsible. We will continue supporting this strategy through our ongoing environmental action plan, with these main action points: • Meet statutory and contractual obligations • Generating a company-wide culture of environmental awareness • Ensuring procedures are in place for energy conservation, control of harmful substances, air emission control, visual and noise intrusion, material recycling and disposal of waste • Ensuring effective environmental monitoring of sub-contractors based on risk assessment and contract requirements • Management planning, operational reviews, audit checks and corrective actions Activities include but are not limited to: • Using renewable electricity, recycled electrical equipment • Recycling packaging, paper, reducing office waste • Preventing contaminated soil, chemical, water waste • Using contractors for waste oil products

				Our PSN solution is based on using our existing MPLS infrastructure and ensuring compliance of that. Our approach ensures best use of assets and avoids the environmentally unsound practice of duplicating infrastructure, decreasing carbon footprint. **Measurement, management and reduction of carbon emissions:** Level 3 operates a motor vehicle fleet necessary to operate and maintain our extensive network. This has significant environmental impact; we continue to optimise our fleet performance, and reduce vehicle fuel consumption by: • Replacing older vehicles with newer, more fuel-efficient models • Using our GPS-based fleet management system to improve driver efficiency, reduce idling times, and decrease miles driven • Improving fleet average fuel efficiency Company-wide, we have deployed our own technology-based suite of collaboration services (also available to our customers) – e.g. video, instant messaging and videoconferencing – and where possible use these to reduce travel environmental impact. **Verification measures for carbon emissions and waste reduction:** We report via the Carbon Disclosure Project on emission levels 1, 2 and 3.

THE PROVISION OF SERVICES TO HM TREASURY UNDER THE PSN-C FRAMEWORK AGREEMENT

Framework Agreement Schedule 16 Call-Off Form – Annex C Security

Annex C

Security

For

HM Treasury

Security Plan

for

HM Treasury

This document version details:

Owner:	[redacted]
Version:	1.0
Status:	Draft
Date:	Jan 2014
Identity	SP_HMT_2013
Template reference	GSO/PSN/ISMS/1090

PROTECT COMMERCIAL
HM Treasury Security Plan

Document Control:

Document Location: (Master template)	**Security document library**
Document Location: (this version)	**HM Treasury document library**
The Change Authority	**(Master template):** [redacted]
Approval of customer version	**[customer]**

Change History: Master template (only to be changed by template author)

Version	Date	Reason for change	Change by
1.0	25th November 2011	Initial template Document	

Change History: Customer specific document

Version	Date	Reason for change	Change by
1.0	Jan 2014	Draft for RFP	[redacted]

Change Mechanism

Step 1: Any person seeking to alter this document must consult the author before making any change.

Step 2: The person making the alteration must indicate every change between the previous (approved) document version and the altered document version.

Step 3: The Change Authority must endorse any alterations to the template document before any wider dissemination of the altered document.

[redacted]

HM Treasury Security Plan

Approvals

Name	Role	Version	Signature
HM Treasury	Security Authority	1.0	

** The rest of this page is left blank intentionally **

[redacted]

Glossary of Terms and Abbreviations

Term or Abbreviation	Description
CESG	Communications-Electronic Security Group (part of GCHQ)
CLAS	CESG Listed Adviser Scheme
GSi	Government Secure Intranet
HMG	Her Majesty's Government
IA	Information Assurance
ICT	Information and Communications Technology
IS1	HMG Information Assurance Standard No 1 (Parts 1 and 2)
IS2	HMG Information Assurance Standard No 2
LSC	Legal Service Commission
PGA	Pan Government Accreditor
PIA	Privacy Impact Assessment
PID	Programme Initiation Document
RMADS	Risk Management Accreditation Document Set
The MTCF SAL	The MTCF Security Aspects Letter
SAM	Security Accreditation Manager
SIRO	Senior Information Risk Owner

References

Reference	Description
[1]	Cabinet Office Security Policy Framework https://www.gov.uk/government/publications/security-policy-framework
[2]	http://www.cesg.gov.uk/publications/Documents/business_impact_tables.pdf
[3]	HMG Information Assurance Standard No 1&2, Issue 4.0 April 2012
[4]	CESG Security Procedures for Telecommunications Systems and Services Issue 2.2

[redacted]
HM Treasury Security Plan

Contents

[redacted]

HM Treasury Security Plan

SECURITY PLAN

1. Introduction

1.1 This document, referred to hereafter as 'the Security Plan,' provides a high-level plain-English description of the Information Security responsibilities of The Contractor's staff, contractors and personnel involved in the PSN Connectivity Framework (PSN-C) hereafter known as 'the Service' and so protect the security of The Authority's information to which The Contractor has custody.

1.2 It also lists the responsibilities and information required from HM Treasury to enable The Contractor to discharge its responsibilities under this Plan.

1.3 To that end, the Security Plan is made available to all members of The Contractor's staff, contractors and personnel who sell, design, implement, manage, maintain the Service.

1.4 This document does not replace or supplant any other of The Contractor's policies but offers specific, additional advice where necessary on particular security aspects relating to the Service, and pointers and links to where additional information may be found, with the aim of ensuring that The Contractor complies with its contractual requirements under the Framework Agreement.

1.5 The term "The Authority" nominally refers to the Government Procurement Service but can refer to HM Treasury where appropriate.

1.6 It is assumed that HM Treasury will provide a Security Aspects Letter to the contractor.

1.7 This document describes the approach for PSN –C in general of which HM Treasury is one customer.

2. Information Security Management System (ISMS)

2.1 The Contractor is committed to developing, certifying maintaining and improving an ISO27001-compliant ISMS. The details of the current version of the ISMS, its scope, policies, procedures, work instructions and records can be viewed as part of an Audit upon request subject to non-disclosure.

[redacted]

2.2 For the Call Off contract to which this Annex C is attached, the following will be added to the scope of The Contractor's ISMS

- HM Treasury PSN WAN

2.3 The Contractor's ISMS is certified under the CESG Assured Service (Telecommunications) and independently audited in accordance with CESG Good Practice Guide no. 32.

3. Security Aspects

3.1 In the absence of HM Treasury specific Security Aspects instructions, the Contractor will use the principles laid our in the PSN Security Guidance, PSN Codes and PSNA Instructions to inform the Security Aspects of the service. To that end:

3.2 the customer shall inform Level 3 if any aspect of the service other than the traffic on the IP VPN is sensitive (IL3).

3.3 Notwithstanding any forthcoming change to the Government Protective marking Scheme The Contractor shall assign to non-sensitive assets a business impact level of 2, 2, 4 for Confidentiality, Integrity and Availability respectively.

3.4 Some non-sensitive data may be stored and accessed outside the EEA. This will be confined to information held by Level 3 provided by the customer or created by level 3 as a result of operating the service.

3.5 Customer traffic on the IP VPN shall be regarded as sensitive (IL3) and no customer traffic data will be held or transmitted outside UK borders.

3.6 Relevant parts of any RMADS produced and maintained by The Contractor during the life of the PSN-C Framework Agreement shall reflect the specific demands of the Customer for the services under consideration.

3.7 The Contractor holds information about the customer's service in its business support systems e.g. billing, inventory, orders and ticketing. These systems do not connect to or

directly affect the networks provided by Level 3 that carry the Customer's own traffic. For this reason they are outside of scope of Service RMADS

4. Security Information Dissemination

4.1 The contents of the customer's service security requirements will be published on The Contractor's intranet along with guidance on interpretation.

4.2 The Contractors Security Compliance Team, supported by senior management, shall ensure that all The Contractor's staff and contractors concerned with the Service will be provided with a security briefing on any specific security aspects of the Service, within 60 working days of the Effective Date of the MTCF Framework Agreement.

4.3 The Security briefing will cover a minimum of :

- Location of key security document;
- Any security aspects which are not 'business-as-usual';
- Security roles (Accreditor, Sponsor etc.); and
- Where to find additional guidance.

5. Accreditation

5.1 The Services will be Accredited being aligned to [3]. The Contractor employs a CLAS consultant (SIRA Practitioner) for the purpose of assisting in this accreditation.

5.2 The Accreditation governance procedures shall comply with those of the PSN Risk Management and Accreditation Reference Document (RMARD).

5.3 The Contractor's security team will be augmented from time to time by using specialist members of the CESG Listed Adviser Scheme (CLAS) and service providers approved under the CHECK Scheme when such needs arise for example as part of the annual IT Health Check.

5.4 The security measures to be implemented and maintained by The Contractor in relation to aspects of the Service within scope will be documented by the Security Accreditation Manager in a Risk Management and Accreditation Document Set (RMADS). The Security Controls adopted will be proportionate to manage the risks. As a default position for IL 2-2-4 services The Contractor will aspire to conform to the requirements of [4]. Any non-conformities will be noted in the Residual Risk Statement for the Service available to Customer on request.

5.5 Unassured offshored aspects of the service will be documented in the Residual Risk Statement and the service accreditation certificate.

5.6 RMADS are pivotal to the security accreditation process and, simply put, provide a structure which is used to assemble portfolios of documents that will collectively:

- Explain the business purpose and scope;
- Summarise the key computer systems, networks, services and locations;
- Identify and quantify risks that may damage the integrity, availability or confidentiality of information dealt with by these computer systems, networks and services;
- Describe the blend of physical, personnel, procedural and technical security controls used to manage these risks; and
- Provide regular evidence, such as security test, security inspection and security incident reports, to demonstrate that the security controls used manage these risks work effectively in practice.

5.7 RMADS will be proportionate, accurate and focussed. The format shall be agreed between The Contractor and the Pan Government Accreditor.

5.8 The risk assessment methodology in [3] is used in the RMADS. Reference [3] describes HMG's Technical Risk Assessment method – a systematic approach to documenting and quantifying technical risks that may threaten the integrity, availability or confidentiality of a computer system, network or service. Reference [3] provides HMG's Technical Risk Treatment method – a structured approach to documenting a Security Case that

describes the nature and stringency of the security controls and assurances needed to manage any risks identified by applying the method.

5.9 When Assessing Risk Treatment, The Contractor will use a Risk Tolerance Level based on the published PSN Risk Appetite Statement. The Risk Tolerance Level shall specify the level of risk as determined by the methods in **[3]** that The PGA is prepared to accept. . Any change to the Risk Tolerance level after the Effective Date is deemed a change to the PSN-C Framework Agreement.

5.10 Where aspects of the Service are held or moved offshore The Authority will be advised. Where a Privacy Impact Assessment is necessary this will be undertaken by The Authority and included or referenced in the RMADS.

5.11 The RMADS will form part of the ISMS, be available to appropriately-cleared personnel and be held and maintained by The Contractor. It will be available for inspection at The Contractor's premises as part of an Audit.

5.12 The RMADS will be approved by the Pan Government Accreditor and be structured according to ISO27001, cross-referencing if necessary to schedules within the Framework Agreement and reference **[1]**.

5.13 The existence of a current Accreditation Statement from a Pan Government Accreditor referencing the service RMADS shall be sufficient to provide assurance to HM Treasury Accreditor that risks within the accreditation boundary of the contracted service are being managed adequately.

6. Transition

6.1 Where the Service is not currently part of the ISMS, The Contractor will be responsible, using reasonable endeavours and due process, for transition of the security arrangements and responsibilities for the Service into the scope of the ISMS.

6.2 It is assumed that where sponsorship is required from The Authority to gain PGA or similar support that this will be granted in a timely manner.

7. Personnel Security

7.1 All The Contractor's employees, their agents and sub-contractors shall receive a security vetting level according to the provisions of the Security Policy Framework or equivalent for staff located overseas. This is BPSS by default, with certain roles attracting SC.

8. Security Incident Reporting

8.1 The following contact points shall be used when HM Treasury is reporting security incidents to The Contractor:

telephone 0845 015 1036 for Data Incidents.

9. Responsibilities of The Contractor

9.1 The Contractor shall maintain Accreditation for the Service and provide a copy of the Accreditation Statement upon request. For the avoidance of doubt, copies of the RMADS will not be made available but can be viewed at The Contractor's premises subject to agreement from the PGA.

9.2 The Contractor shall provide a Service Residual Risk Statement in accordance with the RMARD upon request. This shall provide HM Treasury Accreditor with summary details of the main residual risks and non-conformities, together with risk management statement and guidance on SyOPs that should be adopted by HM Treasury's staff to operate the Service securely.

9.3 For the avoidance of doubt The Contractor will not share the results of detailed ITHC reports or vulnerabilities that have been 'closed' with HM Treasury. The Pan-Government Accreditor will have access to these.

10. Responsibilities of HM Treasury

10.1 If required, HM Treasury shall undertake a Privacy Impact Assessment for each Service and provide it to The Contractor for inclusion in the Residual Risk Statement.

11. Amendment and Revision of this Plan

11.1 This Security Plan will be reviewed annually.

Test Plan for WAN Based Projects

Implementation and Migration Process

New 10Mb, 100Mb, 1000Mb FE and 1GE and 10GE Circuits

After Off-net or On-net handover the new Circuit and Router installations and test will be approached as follows–:

Stage 1 Take On

a. **Installation of new Router** at agreed date during working hours, minimum of 3 working days in advance of scheduled migration date. Level 3 shall complete CPE router installation (Router node ID) and connect it to the access circuits in working hours. This includes service Take On. New service will be installed in Customer cabinets for the new Premium Service Primary and Secondary Routers.

b. Conduct Take-on validation test and line proof – Confirm Speed/Duplex settings for both ends. (Router Node ID).

   NON SERVICE AFFECTING

   Resources:
   Level 3 Field Engineer from DI Data Customer site – (Field Engineer details notified to client)
   Level 3 DI Data Field engineer contacts MIPSA duty number (Level 3 Turn Up)
   Client to provide cabinet space for new Router –

   Note: Router to be installed and Taken-on with MIPSA. This Router will then be migrated to the new circuit and connectivity tested.

Stage 2 Take On - LAN

c. **Migration of services** at an agreed date during working hours minimum of 3 days after new Router installation. Migrate from existing WAN Circuit to new Premium Primary. Level 3 to complete agreed test of new premium service. Again confirm Speed/Duplex settings for both ends.

   Resources:
   Level 3 DI Data Field Engineer on Customer site – (Field Engineer details notified to Client)
   Level 3 Tech Support engineer – remote
   Client engineering support
   Level 3 Project Manager – via phone

UAT / User Testing (Application Testing)

(Following table is an outline example – Level 3 would expect the authority's Desktop provider to define the specific required test actions)

1	Turn off WID/PC Terminal (if on)
2	Power on WID/PC Terminal
3	Login into AD, Portal Services and Office Productivity Applications
4	Log into email systems and ensure email can be read or other apps
5	Log into MS Applications
6	Test send and receive emails
7	Print

d. **Secondary Circuit Installation**

Repeat stages a – c (Stages 1 & 2) for the new Secondary Routers/Circuits

Cutover to new Premium Services Primary and Secondary

OOH working may be required as the services are likely to be live. It is usual for Failover testing to commence at 1800 hours and finish at 2000 hours.

1. Level 3 will return to site and retest the new Ethernet Primary and Secondary circuits
2. Shutdown mid-point of primary circuit to test failover to secondary
3. UAT testing of Secondary failover
4. Restore mid-point of primary circuit and then remove LAN cable to simulate switch failure to test failover to secondary
5. UAT testing of Secondary failover
6. Reconnect primary router LAN cable
7. Final UAT on restoration of Premium resilient service

UAT / User Testing

(Following table is an outline example – Level 3 would expect the authority's Desktop provider to define the specific required test actions)

1	Turn off WID/PC Terminal (if on)

2	Power on WID/PC Terminal
3	Login into AD, Portal Services and Office Productivity Applications
4	Log into email systems and ensure email can be read or other apps
5	Log into MS Applications
6	Test send and receive emails
7	Print

EMEA Managed IPSA Testing Script

Below is an approved Testing procedure to cover all Stage 1 and Stage 2 installations. Regardless of product type. Unfortunately due to obvious differences with each device (IP addressing etc), there will be an element of human interaction with this document.

Fields that will require your input are clearly documented in [BOLD BRACKETS].

Any additional notes will be Highlighted and Stared (*).

All outputs of the below commands will then need to be documented and applied to your TTB (Technical Notes field) in EON, before TTB completion.

**** Please note ****

- A Prerequisite is that your MGMT script has been applied successfully.
- Proof read your results before clicking through your Task as a pass. To put it simply, if something fails, it's not a pass until the issue is resolved.

Once you're happy. You can go ahead and run the script on your device.

Stage 1

!
Clear counters
Y
show version
|
show ip interface brief
|
show run interface [WAN_INTERFACE]
|
show interface [WAN_INTERFACE]
|
Ping [CORE_WAN_IP] source [CPE_WAN_IP] repeat 1000 size 1000
|
show ip route
!
show ip bgp summary
!
show ip bgp neighbor [NEIGHBOR_ADDRESS] advertised routes
|
show snmp contact
|
show udp | i 162
!
show policy-map interface
|
!****NOTE****
!ADSL Output. Commands may differ dependant on IOS revision.
!For older IOS –
|

```
show dsl interface [ATM_INTERFACE] | include Speed|Err|Atten|Noise
!
!****NOTE****
!For IOS Version 15 onwards use
!
show controllers vdsl 0 | include Speed|err|Atten|Noise
!
!
!****NOTE****
!The below TCL (Tool Command Language) Script below will Stress Test your WAN link. Gradually
!increasing in packet size.  Some of these tests may fail due to Policing or CoPP on the core
!infrastructure. Speak with a Senior Engineer if unsure of results.
!
tclsh
foreach pktsize {
64
128
512
1024
1280
1500
} {
ping [CORE_WAN_IP_ADDRESS] source [CPE_WAN_IP_ADDRESS] timeout 1 size $pktsize repeat
1000
}
wr mem
!
reload
!
!
!****NOTE****
!STAGE 1 - CISCO CORE TESTS
!
show interface [WAN_INTERFACE]
!
show run interface [WAN_INTERFACE]
!
show ip route vrf [VRF] [MGMT_LOOPBACK]
!
show policy-map interface [WAN_INTERFACE]
!
!****NOTE****
! Carry out  the below command on all the core devices in your path. to ensure the same
Bandwidth is allocated across L3
!
show policy-map [MAP_NAME]
!
wr mem
!
!
!****NOTE****
```

!STAGE 1 – JUNIPER CORE TESTS

show interface [WAN_INTERFACE]
!
show configuration interface [WAN_INTERFACE]
!
show route table [RD] [LOOPBACK_IP]
!
show policy [Policy]
!
show route received-protocol bgp [NEIGHBOR_IP] Table [RD]

STAGE 2

- Prerequisite. LAN migration has taken place and all required ports are open.

Show ip int brief
!
!****NOTE****
! You will need to obtain a working sites LAN IP address.
!
Ping [LAN_IP_OF_EXSISTING_SITE] source [LAN_IP_ADDRESS] repeat 1000 size 1000
!
show run interface [LAN_INTERFACE]
!
Show interface [LAN_INTERFACE]
!
Show arp
!
!****NOTE****
! if using HSRP use the below
!
show standby brief
!
show track [x] (where ' x ' is the configuration on the primary LAN port track option)
!
!****NOTE****
!Repeat once HSRP has failed over.
!
show standby brief
!
show track [x] (where ' x ' is the configuration on the primary LAN port track option)
!
wr mem
!
!****NOTE****

!Stage 2 Core checks

!Cisco TEST

show ip route vrf [VRF] [CPE LAN IP]

Juniper Test

show route table [RD] [VRF] [CPE LAN IP]

Once stage 2 tests are complete. Confirm with on site contact all is working. Take his/her name for your documentation.

It goes without saying that if you have a stage 1 and stage 2 booked at the same time you'll need to complete the entire test document. Before completing out any paperwork.

Level 3

Business Continuity Program Overview

Corporate Business Continuity Team
Version 4.2
September 5, 2012

Subject To Change Without Notice

IMPORTANT NOTICE: This Business Continuity Program ("Program") Overview is provided as a courtesy and may not, and should not, be relied upon by any person or entity, including, without limitation, any current, past, or prospective employee, agent, customer, or vendor of Level 3 Communications, LLC ("Level 3") or any of its affiliates. This Program Overview may be modified or terminated at any time, without notice. The terms and conditions of any relationship between Level 3, or any of its affiliates, on the one hand, and any other person or entity, on the other, shall be governed solely and exclusively by any separate written agreements or other arrangements between the respective parties and not by this Program Overview, regardless of whether such agreement or arrangement is made before, on, or after the date hereof. Neither this Program Overview nor the delivery hereof constitutes a legally-binding commitment by Level 3 to maintain a Program in any particular manner.

Level(3)

Table of Contents

EXECUTIVE SUMMARY

Business continuity planning is an essential component of Level 3 Communications' business operating model. Due to the nature of the telecommunications industry, the products and services Level 3 provides are expected by customers to meet remarkably high standards for availability. Level 3 respects this responsibility and ensures a robust Policy and Program is in place to maintain uninterrupted services whenever possible and, when necessary, to recover from unavoidable disruptions quickly and efficiently.

Introduction

The Level 3® Network, an acknowledged part of our global telecommunications critical infrastructure, was built with business continuity in mind, using physical plant components and redundant systems to support continuous, uninterrupted services for our customers. Hardware, however, is only part of the solution. Advance planning to develop and rehearse strategies that capitalize on all of our capabilities and enable us to recover our services quickly remains key to Level 3's resiliency. To engage in effective planning, a cross-functional business continuity planning structure spans across all regions of the company, adhering to the business continuity policy and framework. As a result, Level 3 plans for and works everyday to deliver uninterrupted service.

Level 3's development, implementation, and maintenance of the Program's life cycle can give our customers confidence that our services will run with minimal interruptions, regardless of the event experienced.

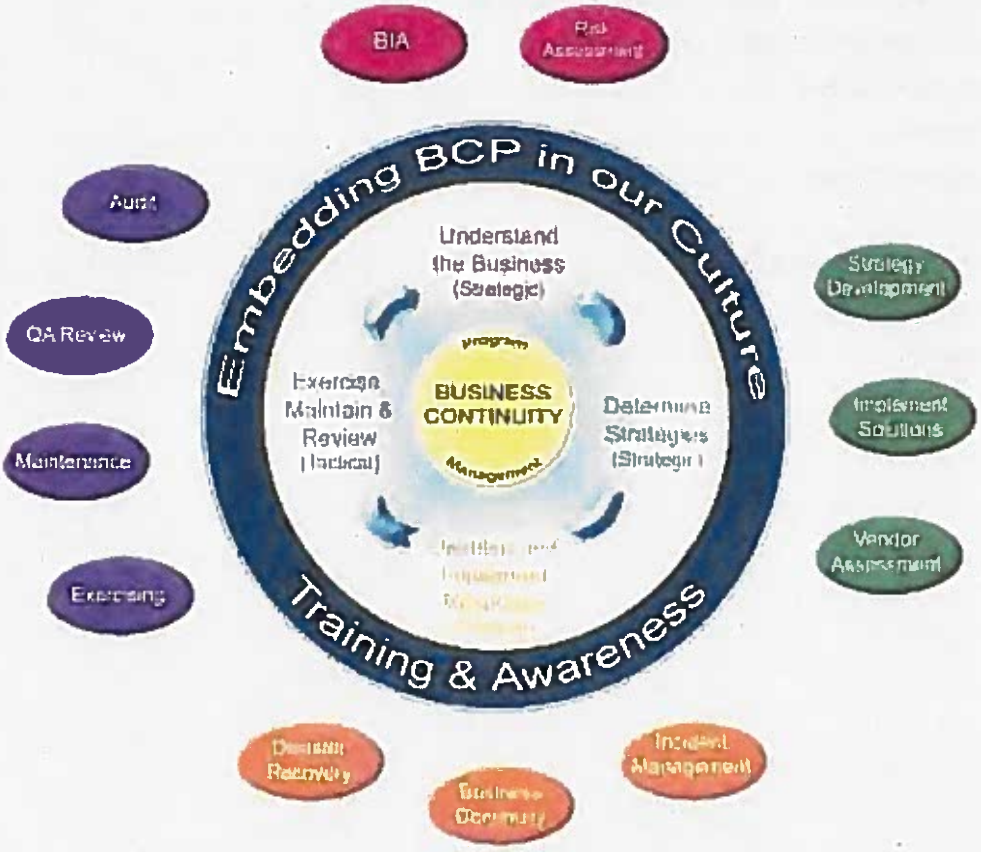


Figure 1: Life Cycle of Level 3's BCP Program

Mission

The mission of Level 3's Program is to:

- Identify the threats/hazards and their potential impacts and provide a framework for building enterprise resilience
- Safeguard employees, key stakeholders, and long-term market share in the event of an unplanned interruption to the business
- Maintain uninterrupted service whenever possible, and when necessary, effectively coordinate recovery from unavoidable disruptions quickly and efficiently
- Respond to emergency situations in a safe, effective and timely manner

Strategy

The Program has been designed to protect shareholder value by ensuring that business continuity related risk is effectively identified, assessed, and managed, and where feasible, mitigated. The Corporate BCP Team is responsible for the formulation of policy, developing the framework, and governance of the Program. Each Functional Group owning critical functions is responsible for developing, maintaining, and exercising plans.

A Business Impact Analysis (BIA) identifies criticality and determines how soon after an event processes/systems need to be available. Those time intervals are then used to prioritize the recovery and implement recovery solutions for essential operations. Business continuity planning focuses on planning for the impacts that could be caused by any scenario and defining the appropriate tactical recovery.

The key principles upon which the Program strategies and capabilities are based include:

Incident Prevention – Protecting services from threats (environment, hardware/software, operational errors, malicious attacks and natural disasters)

Incident Detection – Detecting incidents at the earliest opportunity to minimize impact

Response – Responding to incidents in the most appropriate manner providing for an efficient recovery and minimizing downtime

Recovery – Implementing appropriate recovery strategies and solutions that will ensure timely and prioritized resumption of operations

Improvement – Incorporating lessons learned from incidents, exercises and tests to enhance our level of preparedness

GLOBAL BUSINESS CONTINUITY PROGRAM

The Program is a holistic process designed to provide a methodology for identifying and assessing threats and hazards, understanding their impacts to Level 3 operations, and developing a framework for planning and responding to unavoidable disruptions. The components of the Program are outlined here.

Program Management

Program Accountability: Program management is the heart of the BCP Program. Accountability of the Program is held at the senior management level so it receives the proper focus and alignment with enterprise priorities for a successful implementation. Program management includes making sure goals have been met and providing for a continual review of the Program to ensure its continuing suitability, adequacy and effectiveness.

Resource Commitment and Training: Based on the results of the BIA and Risk Assessment, management commits the resources to execute the Program and makes sure they are trained and competent. The Program utilizes role-based training modules to train its employees. The instructional modules are designed to provide training on the Program objectives as well as an explanation of how to complete the tasks to meet the requirements.

Embed BCP into Culture: The participation of senior management is key in making sure that the BCP Program is correctly introduced, adequately supported and is properly embedded as part of Level 3's culture.

Understanding the Business

Business Impact Analysis: A BIA is conducted to identify the impacts resulting from business interruptions and provide the criteria to quantify and qualify those impacts to determine what is most critical to our operations. This analysis identifies time-critical functions, their recovery priorities, and interdependencies so recovery time objectives can be established and approved. This data then drives the priorities for continuity planning and developing/implementing recovery strategies and solutions to support the recovery time objectives.

Risk Assessment: A Risk Assessment is conducted to evaluate the threats and hazards and identify potential causes of interruptions, the probability of their occurrence, their severity and their impact when they do occur. Measures can then be identified to reduce the probability of occurrence or reduce the impact of an incident.

Risk Management: After the risk to operational disruptions is assessed and understood, Level 3 evaluates the risks and impacts it can control or influence. Management can then make informed decisions on managing unacceptable levels of risk.

Determine Strategies

Strategy Development and Implementation: The results from the BIA and Risk Assessment are used to assess and implement appropriate strategies to reduce the likelihood and impacts of incidents or disruptions. This requires identifying continuity strategies that will improve Level 3's resiliency to a disruption by ensuring critical activities continue at, or are recovered to, an acceptable level and meet agreed upon recovery timeframes. The strategies define the required resiliency solutions so that controls around incident prevention, detection, response, recovery and restoration are put into place.

Vendor Resiliency Management: Level 3 analyzes the resiliency of its critical vendors that support critical functions/processes, facilities and systems to proactively manage unacceptable levels of risk.

Develop and Implement Response

Incident Management Response Structure: Level 3 employs a multi-layer scalable response structure to efficiently respond to disruptions that span its global operations.

Plan Development: Level 3's resiliency planning concentrates on sustaining its critical business operations and its supporting infrastructure (i.e., network, people, systems, facilities, vendors, etc.). Planning focuses on the impacts that could be caused by any scenario and provides the procedures for maintaining the continuity of operations. Level 3's BCP Program includes the following suite of plans:

- Enterprise Business Continuity Plan – Company overarching strategies
- Crisis Management Plan – protect Company brand
- Incident Management Plans – provide command, control and coordination over recovery teams
- Business Continuity Plans – continue critical operations
- Facility Recovery Plans – recover critical infrastructure of facilities
- Application Recovery Plans – recover applications
- Pandemic Plans – recovery of influenza outbreaks

Exercising, Maintaining and Reviewing Response

Exercise and Maintenance: Business continuity and incident management planning is exercised and maintained to validate their viability. Level 3 exercises its plans to develop teamwork, competence, and confidence among its recovery teams. Plans are maintained in a state of readiness.

QA Reviews: To maintain a consistent level of Program execution, Level 3 conducts QA reviews on planning.

Post-Event Review: Level 3 assesses its response to and recovery from events to measure the effectiveness of its response and recovery capabilities. Post-event reviews provide the impacted/activated groups with an opportunity to seek feedback on their recovery and their incident management performance. A summary of the event incorporates any corrective actions for improvement which become part of ongoing detection, analysis, and elimination of actual or potential causes of disruptions.

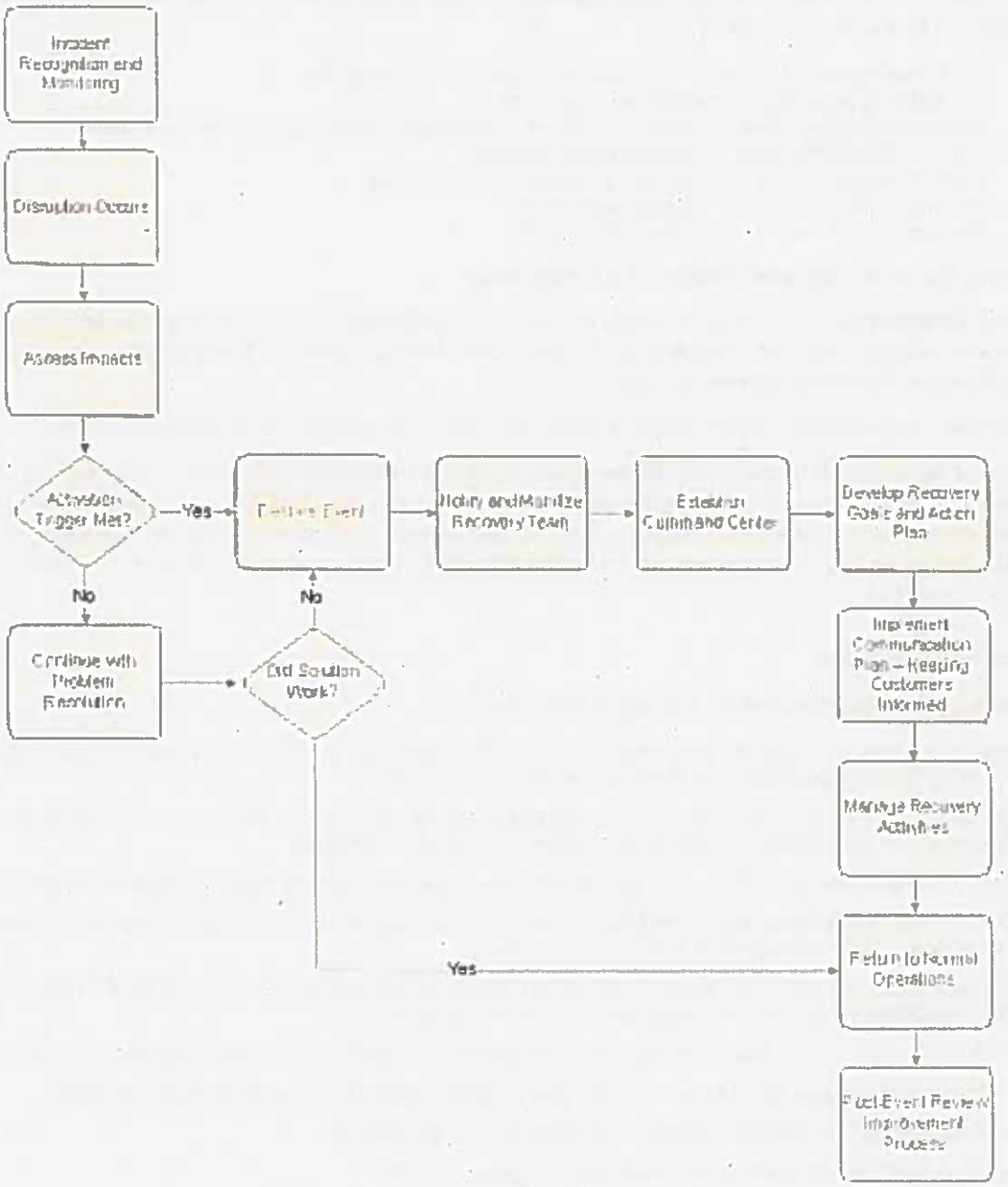
Standards and Practices

Level 3 utilizes the following standards for modeling its BCP Program:

- British Standards Institution (BSI), BS 25999: "25999-1:2006 Business Continuity Management. Code of Practice" and "BS 25999-2:2007 Specification for Business Continuity Management"
- British Standards BS ISO/IEC 27031:2011: "Information Technology – Security techniques – Guidelines for information and communication technology readiness for business continuity"
- International Standard ISO 22301: "Societal security – Business continuity management systems – Requirements"
- American Society for Industrial Security (ASIS) "Business Continuity Guideline: A Practical Approach for Emergency Preparedness, Crisis Management, and Disaster Recovery"
- American Society for Industrial Security(ASIS) /British Standards Institution (BSI) ASIS/BSI BCM.01-2010 "Business Continuity Management Systems: Requirements with Guidance for Use"
- NFPA 1600: "Standard on Disaster/Emergency Management and Business Continuity Programs" 2010 Edition
- NIST Special Publication 800-34 Rev 1, "Contingency Planning Guide for Federal Information Systems"
- BSI PAS 200:2011 "Crisis Management – Guidance and Good Practice"
- The Homeland Security Exercise and Evaluation Program (HSEEP)
- Disaster Recovery International Institute: "Professional Practices for Business Continuity Practitioners"

CONCEPT OF OPERATION – RESPONSE AND RECOVERY

Level 3 utilizes the following process for monitoring, declaring and managing recovery from events. Keeping our customers apprised of unavoidable disruptions is a high priority when triggered events require us to implement a communication plan.



RESILIENCY AND PREPAREDNESS CAPABILITIES

Level 3's preparedness capabilities and strategies include, but are not limited to:

Level 3 Network

The Level 3 network is fully route-diverse and is designed with complete "ring" protection. This design ensures that our protected services are fully path-redundant and are not susceptible to outages. The core design characteristic driving Level 3's high-level of network reliability is geographic network diversity. Each city along the network is served by two, or in some cases three, diverse paths, thus ensuring that a fiber cut along any one route will not isolate a city from the network ensuring continuity of service.

Network Operating Centers

Redundant Network Operating Centers (NOCs) geographically disbursed enabling Level 3 to identify and isolate causes of potential network disruptions and quickly coordinate resolution of system outages.

Network Facilities

All critical facilities have plans for recovering their critical infrastructure from loss of access, power, HVAC or employees, etc. We also conduct evacuation drills to protect the life safety of our employees, customers and vendors.

Technical Support Centers

Technical Support Centers are geographically disbursed and staffed 24 x 7 to provide dedicated support to our customers.

Data Centers

Alternate Processing Site: Level 3 owns and self-manages a geographically dispersed alternate data center, which is utilized when the primary processing capabilities are not available. The alternate data center is a hot site that is comparable in size, power capacity, and HVAC capacity to the primary data center. The alternate data center is equipped with the infrastructure, environment and connectivity to support recovery of its critical systems and applications for essential business functions within their recovery time objectives.

Alternate Storage Site: Numerous data replication strategies are employed by Level 3 to manage data storage in a safe and secure manner. Data from our primary data center may be replicated through various technologies to repositories located in our self-managed geographically dispersed backup data centers. This capability facilitates meeting our recovery time objectives and mitigates risk of physical access and retrieval of backup information.

Information System Backup: Level 3 has implemented a hot standby solution in its alternate processing and storage site. Periodic testing is conducted on media reliability and information integrity.

Information System Recovery: System recovery is sequenced based on the criticality of the functions the information systems support and the recovery time objectives and recovery point objectives defined by the business. Each information system's failover capability utilizes recovery solutions designed to meet those recovery objectives.

Supply Chain/Critical Vendors

Level 3 critical vendors and suppliers are asked to demonstrate their business resiliency capabilities. This provides Level 3 the ability to manage any risk to their supply chain. Level 3 incorporates its partners in its exercise program.

Pandemic Preparedness

Level 3 recognizes its responsibility to our employees, customers and shareholders to minimize the potential for business disruption and to recover operations as rapidly as possible should a disruption occur as a result of a pandemic outbreak. Through effective, ongoing preparation and planning, Level 3 employees are provided with public and private resources to enhance awareness and recommend precautions.

Level 3 maintains both Global and Business Unit Pandemic Influenza Plans, which are integrated into its Business Continuity Program. Pandemic preparedness focuses on:

- Ensuring mission critical functions remain operational
- Personnel remote access and staff reduction contingency strategies
- Providing an appropriate level of awareness for our employees and customers
- Anticipating and responding to our customer's needs and possible disruptions to our supply chain

Communications

Backup Communications: Level 3 has implemented redundant communications capabilities utilizing alternate carriers. Primary and backup conference bridges are supplied by separate vendors using diverse networks and routes. An automated paging system, utilized for notifying and communicating during an event, is also geographically redundant.

Remote Network Access: Level 3's network security architecture allows near-immediate and sustained remote access into our internal network to access critical applications and data through any ISP, regardless of provider.