NPCC National Police Chiefs' Council

POLICE DIGITAL SERVICE

CYBER STANDARD DOCUMENT

BUSINESS CONTINUITY

ABSTRACT:

This Standard specifies the minimum requirements regarding business continuity. It aims to provide PDS (Police Digital Service) and policing with clear direction to implement a business continuity strategy, enabling operations and services to endure adverse events.

ISSUED	November 2023
PLANNED REVIEW DATE	August 2024
DISTRIBUTION	Community Security Policy Framework Members
STANDARD VALIDITY STATEMENT This document is due for review on the date shown above. After this date, the document may become invalid. Members should ensure that they are consulting the currently valid version of the documentation.	

Document Information

Document Location

PDS - National Policing Policies & Standards

Revision History

Version	Author	Description	Date
0.1	Sarah Falcous	Initial draft	12/07/22
0.2	Sarah Falcous	Review of draft after comments	21/07/22
0.3	Sarah Falcous	Review of draft after comments	3/8/23

Approvals

Version	Name	Role	Date
1.0	National Cyber Policy & Standards Board	National authority for cyber standards	30/11/23

Document References

Document Name	Version	Date
BS EN ISO 22301:2019	2014	
ISF - Standard of Good Practice (for Information Security)	v2022	07/2022
ISO 27002:2022 - Information security, Cybersecurity and privacy protection – Information security controls	v2022	02/2022
CIS Controls	v8	05/2021
NIST Cyber Security Framework	v1.1	04/2018
CSA Cloud Controls Matrix	v4	01/2021

Terms	Name
BC	Business Continuity
BIA	Business Impact Assessment
CERT	Computer Emergency Response Team
C, I, A	Confidentiality, Integrity, Availability
CIS	Center for Internet Security
CM	Crisis Management
CSF	Cloud Security Forum
CSP	Community Security Policy
DR	Disaster Recovery
GSCP	Government Security Classification Policy
HA	High Availability
HoD	Head of Department
IA	Information Assurance
IAO	Information Asset Owner
ICO	Information Commissioner’s Office
IoC	Indicator of Compromise
ISF	Information Security Forum
IT	Information Technology
ITHC	Information Technology Health Check
ISO	International Organisation for Standardisation
MASL	Minimum Acceptable Service Level
MTPD	Maximum Tolerable Period of Disruption
NCISO	National Cyber Information Security Officer
NCPSB	National Cyber Policy and Standards Board
NCPSWG	National Cyber Policy Security Working Group
NCSC	National Cyber Security Centre
NCSP	National Community Security Policy
NIST	National Institute of Standards and Technology
NMC	National Management Centre
OOH	Out of Hours
PDS	Police Digital Service
POC	Point of Contact
PIR	Post Incident Review
PXR	Post Exercise Review

Terms	Name
RAID	Redundant Array of Independent Disks
RPO	Recovery Point Objective
RTO	Recovery Time Objective
SIRO	Senior Information Responsible Owner
SLA	Service Level Agreement
SoGP	Standard of Good Practice
SPOF	Single Point of Failure
SWG	Security Working Group
SyAP	Security Assessment for Policing
TTX	Table Top Exercise

Contents

Document Information 3

Document Location 3

Revision History 3

Approvals 3

Document References 3

Community Security Policy Commitment 7

Introduction 7

Owner 7

Purpose 8

Audience 8

Scope 9

Requirements 9

1. Business Continuity Strategy 9
2. Business Continuity Programme and Planning 10
3. Technical Resilience 12
4. Crisis Management 15
5. Disaster Recovery 18
6. Continuous Testing and Improvement 19

Communication approach 21

Review Cycle 21

Document Compliance Requirements 21

Equality Impact Assessment 21

Community Security Policy Commitment

National Policing and its community members recognise that threats to policing information assets present significant risk to policing operations. National policing and its community members are committed to managing information security and risk and maintaining an appropriate response to current and emerging threats, as an enabling mechanism for policing to achieve its operational objectives whilst preserving life, property, and civil liberties.

This standard in conjunction with the National Policing Community Security Policy Framework and associated documents sets out National Policing requirements.

Introduction

The Business Continuity Standard aims to provide members of the policing community of trust with clear direction in planning a robust business continuity strategy and programme. The results of this planning can be implemented during times of crisis, resulting in a calm and efficient response. From a technical perspective, this ensures that critical applications continue to work, with minimal disruption to policing operations.

The Information Security Forum (ISF) Standard of Good Practice for Information Security 2022 (SoGP) states the objective of business continuity:

"The objective of business continuity is to provide [policing senior leadership] with assurance that critical business processes (whether automated or not) will continue operating at acceptable levels by focusing on the availability of information and infrastructure."

From the establishment of a strategy, a business continuity programme can be created. Aspects that should form this programme are:

- Business Continuity (BC) plan.
- Crisis Management (CM) plan, detailing immediate response to a crisis.
- Disaster Recovery (DR) plan, including alternative sites and backups.

These examples and other related actions regarding business continuity are the focus of this document and are detailed throughout.

Owner

National Chief Information Security Officer (NCISO).

Purpose

The purpose of this standard is to assist community members in demonstrating compliance with the following NCSP policy statements:

- Develop a policing-wide business continuity strategy and programme, which is supported by a resilient technical infrastructure and an effective crisis management capability.
- Develop, maintain, and regularly test business continuity plans and arrangements (sometimes including disaster recovery plans) for critical operational processes and applications throughout policing.

A robust business continuity strategy and programme should ensure confidentiality, integrity and availability of policing systems and data is protected, even during an adverse event or crisis.

This document is intended to support any Business Continuity processes and planning, already in place by UK Police Forces in compliance with the Civil Contingencies Act 2004.

This concept is echoed in NCSP principles 4, 5 and 6, which specifically addresses confidentiality, integrity, and availability as integral to the foundation of all information security activity. In addition, the requirements stated in this standard are mapped across the following industry standard frameworks:

- ISO 27002:2002
- CIS Controls
- NIST Cyber Security Framework
- Information Security Forum (ISF) Statement of Good Practice (SoGP)
- Business Continuity Institute (BCI) 'Good Practice Guidelines' and align to BS EN ISO 22301:2019 in developing and maintaining Business Continuity strategies and plans.

Audience

This standard is aimed at:

1. **Technical Staff** i.e. all staff across the policing community of trust who build and implement IT systems, either on behalf of national policing or at a local force level.
2. **Senior Management.** Business continuity particularly requires the attention of policing senior leaders and staff, as it is approval at this level which will drive the success of a business continuity strategy.
3. **User Community (Non-Technical).** While this standard focuses on technological and digital solutions, it is also pertinent that non-technical staff consume this standard. This standard requires the attention of the whole user community, as it is likely all personnel will play a part in guaranteeing business continuity in times of crisis, whether they provide a technical function or not.

Scope

1. This standard applies wherever policing information is processed or stored, National policing IT systems, applications, or service implementations.

2. The security control requirements laid out in this standard are vendor agnostic and applicable for all IT systems, applications, or service implementations that are provisioned for policing community of trust use.

3. The requirements of this standard should form part of third-party supplier contractual obligations where Policing information is processed or stored on behalf of any member of the policing community of trust.

4. The requirements of this standard can be considered as part of any agreements with third parties who are not suppliers, who have access to Policing information.

Requirements

Reference	Minimum requirement	Control reference	Compliance Metric
1. Business Continuity Strategy	A **business continuity strategy** must be in place and owned by a senior leader who has strategic authority on behalf of the Chief Officer Group / executive board or equivalent. The strategy must describe the: • Strategic direction for business continuity planning • How the force / organisation approaches business continuity, including how the work is structured, owned and resourced. • Alignment to force / organisational culture and operating environment • How the BC plan will be communicated and available to all interested parties • Objectives to ensure delivery of the key obligations under the National Community Security Policy (NCSP).	ISF SoGP: BC2.3 ISO27001/2 13.1.2, 17.1.1 NIST: ID.BE.4, RC.CO.2, RS.CO.1	A business continuity strategy approved by senior leadership is in place and maintained.

Reference	Minimum requirement	Control reference	Compliance Metric
2. Business Continuity Programme and Planning	A **Business Continuity Programme** must be devised which includes: • Technical resilience across systems and infrastructure. • An organisational review, identifying business functions, core service providers and critical support services. • A centrally managed Crisis Management (CM) capability. • Co-ordination of BC, CM and DR plans with testing across the police force(s) and supporting organisations. **Business Impact Assessments (BIAs)** must be in place for separate functions or departments across a police force or supporting organisation. BIAs should be reviewed annually and when significant changes have occurred. BIAs are owned by respective business function owners and agreed in line with the BC strategy. BIAs are used to identify critical and important operational and core activities. The BIAs must consider: • **Asset identification and inventory** including identifying and prioritising critical assets. • **Impact to policing**, such as financial, operational, reputational and strategic impact on the C, I and A of data. • **Availability requirements**. These include:	ISF SoGP: BC1.2, BC1.4, BC2.1 ISO 27001:2022 5.29, 17.1.1, 17.1.2 NIST: ID.BE.4, PR.IP.5, RS.AN.4, RS.CO.1, RS.CO.2, RS.CO.3, RS.CO.4, RS.CO.5, RS.MI.2, RS.RP.1	A complete business continuity programme and plan signed off by senior leadership is in place and maintained. Business Impact Assessments are current and approved by senior leadership. Refer to PDS Threat and Incident Management Standard for more information.

Reference	Minimum requirement	Control reference	Compliance Metric
	• Recovery Point objective (RPO) - The point in time to which data must be recovered after an outage. • Recovery Time Objective (RTO) – The overall length of time an information system’s components can be in the recovery phase before negatively impacting the organization’s mission or mission/business processes. • Maximum Tolerable Period of Disruption (MTPD) - The amount of time mission/business process can be disrupted without causing significant harm to the organization’s mission. • Minimum Acceptable Service Level (MASL) e.g. 99.999% Many policing systems are reliant on cloud providers and managed service providers. Availability requirements may be reliant on the contracted SLAs etc that have been pre-agreed. These must be understood and incorporated into the BIAs. Using the BIA information, a **Business Continuity plan** must be written. Individual BC plan based on impact will ensure that business can continue should a service suffer a significant disruption. The BC plan must consider different risk-informed scenarios where operational services are compromised, with alternative arrangements considered for each. For example: • Total loss of communications • Total loss of premises • Loss of key members of personnel • Pandemic		

Reference	Minimum requirement	Control reference	Compliance Metric
	Other aspects that should be included in a BC plan are: • Command and Control i.e. nominated individuals who can make key decisions. • Emergency response checklist • Communication cascade. • An offsite location of the BC plan and other key documentation should be stored securely in a separate location (virtual or physical) in case a primary location is rendered unavailable. These aspects should be coordinated with the overall CM plan.		
3. Technical Resilience	From the outset, systems must be built in alignment with the availability requirements set in the BIA. Technical resilience aims to enable policing systems to maintain an acceptable level of service during an adverse event. Technical resilience can be achieved by maintaining robust applications; infrastructure; networks and communications, which are supported by alternative or duplicate facilities. **Application and hardware resilience.** Applications & infrastructure must be made resilient by implementing the following processes and procedures: • **A procurement process** must be created which ensures that software & hardware	ISF SoGP: BC1.2, BC1.3 ISO 27001:2022 5.3, 5.29 ISO27001:2022 : 13.1.2 NIST: ID.BE.5, PR.DS.4, PR.PT.5	ITHC can provide evidence of resiliency. Evidence of BC and DR testing can prove resiliency. Policing Community members should have access to NMC's Threat Intelligence reporting, which are written from a policing perspective. Guidance on threat intelligence techniques and writing a Cyber Incident Response

Reference	Minimum requirement	Control reference	Compliance Metric
	is purchased in accordance with industry recognised compliance standards. Applications & hardware that are procured should be up to date. The use of legacy and unsupported products is discouraged. • **A patch management process** must be established to ensure that the latest version of software and firmware is tested and applied to applications & hardware in a timely manner. • **Maintenance & servicing procedures** must take place regularly, according to manufacturer's specifications where possible and conducted by qualified and correctly vetted personnel. • **A fault reporting process** must be created and describe methods to report, record, respond and repair faults in a timely manner, by qualified and correctly vetted personnel or by automated processes. **Infrastructure resilience.** Critical applications must be highly available, and its underlying infrastructure must be fault tolerant: **High Availability (HA).** HA is the use of redundant technology components to allow a system to recover from a failure after a brief disruption. The following actions must be considered to remove Single Points of Failure to achieve a HA state: • Multiple locations, such as hot sites • Re-routing of network traffic • Load balancers • Failover servers		Plan is provided in the PDS Threat and Incident Management standard.

Reference	Minimum requirement	Control reference	Compliance Metric
	Fault-tolerance. Fault-tolerance is the ability of a system to suffer a fault but continue to operate, with zero service disruption. The following actions can be considered to achieve fault-tolerance: • Multiple power supplies • Multiple processors • Multiple Disk Drives • Disk Configurations such as RAID • Installing alternative network devices. **Telecommunications resilience** should be considered in the following ways: • Providing duplicate or alternative connection points to external carriers. • Arranging alternative communications methods, such as satellite, radio, 4G / 5G comms (including differing mobile providers) etc. **Cyber Resilience.** The first stage of cyber incident response is 'Preparation,' which promotes the prevention of cyber-attacks e.g. ransomware attack. In addition to technical activities, such as patch management, there are other cyber specific activities that can be undertaken to achieve resilience: • Threat intelligence sources must be regularly reviewed for Indicators of Compromise (IoCs) that are relevant to policing systems. • If protective monitoring exists, there should be regular engagement with the provider, such as NMC, to ensure workspaces are tuned with the most up-to-date and relevant information.		

Reference	Minimum requirement	Control reference	Compliance Metric
	These preparation activities should align to a wider Cyber Incident Response Plan, that details how to detect and respond to a cyber-attack.		
4. Crisis Management	**Plan.** A Crisis Management (CM) plan must be created, which can be used to form an immediate and appropriate response to a crisis. The CM plan must incorporate: **People.** A CM team must be established. The role of this team is to respond to major incidents quickly to reduce business impact, with reference to reputational damage. The CM team should be comprised of: • Selected senior leaders of the relevant policing community body. • Nominated HoDs. • Nominated incident responders and incident managers. • Communication specialists (public relations). • Legal specialists. The team may be supported by a Computer Emergency Response Team (CERT) for IT related events. **Process.** Processes and procedures must be created for effective crisis management. These processes must include: • **Definition.** A definition of a crisis and the conditions under which the CM team must convene.	ISF SoGP: BC1.1, BC1.2, BC1.4, BC2.1 NIST: PR.IP.1, RC.CO.1, RC.CO.2, RC.CO.3, RS.CO.1, RS.CO.4	Evidence of BC and DR testing can prove resiliency. Refer to PDS Threat and Incident Management Standard for more information.

Reference	Minimum requirement	Control reference	Compliance Metric
	• **Roles and responsibilities** of each CM team member. • **Communications procedures** must be established with contact details of key individuals stored appropriately. This will include the CM team and other POCs, such as IT team, key supply chain contacts, industry regulators. Communications cascades must be updated and tested on a regular basis in preparation for a crisis. • **Change Management procedures**. The CM team must have the authority and expertise to enforce emergency changes, following change management procedures. • **Legal procedures.** The CM team must have the authority and expertise to react to legal and regulatory breaches and inform appropriate bodies, such as ICO. • **Media response procedures.** The CM team must have the authority and expertise to respond to media interest and reduce reputational damage. • **Post Incident Review (PIR) procedures**. The CM team is responsible for co-ordinating a PIR after a crisis has been resolved. Steps the CM team must take are: ○ **Confirmation.** The CM team must obtain confirmation that applications and infrastructure are restored correctly to their previous state.		

Reference	Minimum requirement	Control reference	Compliance Metric
	○ **Root Cause Analysis.** The CM team must review the causes and effects of the crisis. ○ **Security Control Review.** Security controls must be reviewed and improved to guard against a further occurrence. Any agreed changes should be tested and documented, following Change Management procedures. ○ **Training and Education.** The CM team must identify training gaps for personnel resulting from poor practice or missing procedures. ○ **Reporting.** The PIR must be documented in a report. ○ **Illegal Activity Reporting.** The CM team must ensure that any illegal actions that may have contributed to the crisis, are reported to the correct authorities. ○ **Collaborative Working.** The CM team should consider sharing findings with other community members. **Location.** A central location (commonly known as a 'war room') must be established for the CM team to convene at short notice to collaborate and formulate a response to crisis. This location may be in-person or virtual, but contingencies must be considered as the nature of the crisis may render preferred locations unavailable. **Time.** A crisis can occur on any day at any time. Consideration must be given to OOH response procedures and must be included in the CM process.		

Reference	Minimum requirement	Control reference	Compliance Metric
5. Disaster Recovery	**Plan.** A Disaster Recovery (DR) plan must be created to detail actions to be taken to recover after a crisis. The DR plan is likely to be invoked after the BC and CM plans and focuses on longer term unavailability of key assets. The DR plan must consider: **Location.** Critical applications must be able to operate even with the loss of underlying infrastructure, such as: • Total loss of primary location. • Loss of office accommodation. • Damage to data centres e.g. cabling, environmental controls etc. • Loss of public utilities e.g. water, electricity. In the event of relocation, the same level of protection (C, I and A) is expected be applied to data, as would have in the primary location. **People.** Succession planning must be incorporated to consider scenarios when key individuals are unavailable. **Data.** The DR plan must consider prolonged unavailability of data for critical processes. This may include: • **Backups** may need to be implemented to restore key data. A backup plan must be created and should be available to adhere to in this instance. • **A Destruction / Decommissioning plan** must be created and referred to for	ISF SoGP: BC1.4, BC2.2 ISO 27001:2022 5.29, 7.11, 8.14 ISO27001/2: 11.2.2, 17.1.1, 17.1.2, 17.1.3, 17.2.1 NIST: PR.IP.1	Evidence of BC and DR testing can prove resiliency.

Reference	Minimum requirement	Control reference	Compliance Metric
	disposal of any equipment or data no longer required or damaged.		
6. Continuous Testing and Improvement	**Testing strategy**. Testing should be based on individual community member's recovery requirements. There are 5 grades of BC, CM and DR testing that can be conducted: • **Read-through test.** BC, CM and DR plans and processes are distributed and reviewed to confirm the information stated remains valid and document versions can be updated. • **Table-Top Exercise (TTX).** This test comprises of a role-play of a crisis scenario, for example, ransomware attack or pandemic outbreak. A moderator is assigned, and each department responds to different situations, using the BC, CM and DR plans as a reference. • **Simulation test.** Similar to a TTX, however, response measures that are suggested, are then tested. This type of testing can also include blue / red teaming. • **Parallel test.** Can be applied if there are alternative recovery sites. Regular operational activity continues in the primary site, but personnel are relocated to the alternate site to carry out BC and DR procedures. • **Full interruption test**. The primary site is shut down and the alternate site is designated as responsible for operational activity.	ISF SoGP: 5.3 ISO27001/2: 17.1.1, 17.1.2, 17.1.3 CIS v8.1: 17.7 NIST: PR.IP.10	Evidence of BC, CM and DR testing can prove the level of testing that has taken place. Evidence of Post Incident Reviews can also show evidence that continuous improvement has taken place.

Reference	Minimum requirement	Control reference	Compliance Metric
	Frequency. BC, DR and CM plans must be tested regularly, at least on an annual basis. A mixture of testing is encouraged but is likely to be dependent on operational impact. For example, a full interruption test may not be appropriate to conduct more than once per year, where TTXs can be conducted more often, without affecting operational activity. **Schedule**. A testing schedule must be produced with different levels of testing and different scenarios carried out throughout the year. Testing must be realistic and consider catastrophic scenarios. Scheduling throughout the year ensures that business continuity is at the forefront of organisational development and promotes a proactive approach. **Post Exercise Review (PXR).** Lessons learned must be identified from any testing or exercise. Results of the exercise must be documented and if there are any actions to be taken, they must be assigned to named personnel and recorded, to provide accountability. Comparison with baselines and other exercises should be completed to spot patterns of strength and weakness.		

Communication approach

This document will be communicated as follows:

- Internal peer review by the members of the National Cyber Policy & Standards Working Group (NCPSWG), which includes PDS and representatives from participating forces.
- Document review by NPCC Business Continuity Group
- Presentation to the National Cyber Policy & Standards Board (NCPSB) for approval.
- Formal publication and external distribution to PDS community, police forces and associated bodies.

For external use (outside PDS), this standard should be distributed within IT teams to help complete an initial gap analysis which can inform any implementation plan. This implementation plan can be shared with force SIROs / Security Management Forum. Consideration should also be given to raising awareness amongst force personnel of the implementation of this standard where it may affect them.

Measurables generated by adopting this standard can also form part of regular cyber management reporting.

Review Cycle

This Policy will be reviewed at least annually (from the date of publication) and following any major change to Information Assurance (IA) strategy, membership of the community, or an identified major change to the cyber threat landscape. This ensures IA requirements are reviewed and that the policy continues to meet the objectives and strategies of the police service.

Document Compliance Requirements

(Adapt according to Force or PDS Policy needs.)

Equality Impact Assessment

(Adapt according to Force or PDS Policy needs.)