NICC ND1643 V5.1.1 (2017-12)

NICC Document

GUIDELINES ON THE MINIMUM SECURITY CONTROLS FOR INTERCONNECTING COMMUNICATIONS PROVIDERS

NICC Standards Limited

The Old Rectory
Church Street
Weybridge
Surrey KT13 8DE

Tel.: +44(0) 20 7036 3636

Registered in England and Wales under number 6613589

Contents

Intellectual Property Rights

IPRs essential or potentially essential to the present document may have been declared to NICC. Pursuant to the NICC IPR Policy, no investigation, including IPR searches, has been carried out by NICC. No guarantee can be given as to the existence of other IPRs which are, or may be, or may become, essential to the present document.

Foreword

This NICC Document (ND) has been produced by the NICC Security Working Group.

Introduction

Communications Providers (CPs) interconnect with each other as a result of either regulatory requirements or commercial imperatives. In these situations each CP's security is partially dependent on the security of the other. One CP could cause an adverse effect for the other, either deliberately or by omission or neglect.

Each CP should defend their networks and systems against likely threats. However each CP should only have to apply a proportionate defence. CPs should not have to incur disproportionate costs to defend their network from actions or omissions by an interconnected CP. The controls defined in this standard should be enforced as the minimum standard of security by all CP's that interconnect in the provision of publically available telecommunication services.

This Guidance aims to:

- Provide information on the implementation of a minimum set of security controls that will be to the benefit of all interconnecting CPs. It will assist a CP from incurring an excessive cost in protecting their own network (i.e. the costs that would be incurred if they had to interconnect with CPs who had no security controls);
- Enable all CPs to satisfy the regulatory obligations defined in UK Law and overseen by Ofcom. Explain the applicability of the controls on all types of Interconnection, including physical and electronic, indicating where some controls are only relevant in certain circumstances.
- The preparation by a CP of a document that describes the implementation of the security controls defined in this guidance document will enable the CP to demonstrate they have taken appropriate measures for another interconnecting partner that may request evidence. The document can also be used as demonstration of the implementation of the minimum controls if evidence is requested by Ofcom.

For clarity, Ofcom are acting to support NICC in establishing the Guidance within the UK. The guidance document is intended for organisations implementing commonly accepted information security controls and is also intended for use in developing industry and organisation specific information security management guidelines. All guidance activity is retained by NICC, with NICC secretary acting as the first point of contact for enquiries.

Contact details: email secretary@niccstandards.org.uk

1 Scope

The Guidance applies to any organisation that is a CP and has a direct Interconnection with another CP.

The controls can apply to the following types of interconnect:

- SIP, SIP-I, SIP-T and H323 based interconnects, or similar IP session based interconnects;
- Interconnects supporting broadband/NGA access; and
- Connection services, for example IP, Ethernet, MPLS and TDM.

The Guidance encompasses the following areas:

- Systems
  - Interconnect Boundary Devices (see section 1.2);
  - Management systems which directly communicate with and are used to manipulate the configuration of Interconnect Boundary Devices;
  - Procedures supporting these;
- Locations
  - The secure perimeters within which the Interconnect Boundary Devices and their management systems are located.

- Personnel
  - Personnel who have right of access to the shared area; and
  - Personnel who have access permissions permitting configuration changes, or other privileged access to Interconnect Boundary Devices.

The following have been considered and have been deemed out of scope:

- Internet Peering;
- Internet Transit; and
- Personnel (for example a visiting engineer from a supplier) who are always supervised by a person in scope of the Guidance.
- Environmental equipment

1.1 What is an Interconnection?

The term Interconnection is defined as the linking (whether directly or indirectly by physical or logical means or by a combination of physical and logical means) of one public electronic communications network to another for the purpose of enabling the persons using one of them to be able:

- to communicate with users of the other one; or
- to make use of services provided by means of the other one (whether by the provider of that network or by another person).

1.2 What is an Interconnect Boundary Device?

Any device containing a functional protocol-peer is an Interconnect Boundary Device. Each functional protocol should have either a single protocol-peer or a resilient set of protocol-peers on each side of the Interconnection.

All of the devices in such a resilient set are Interconnect Boundary Devices. Because protocol-peers may be directly connected or remote, Interconnect Boundary Devices may be local to the interconnect point or remote.

Devices such as those offering 'packet inspection' are not considered to be part of the protocol peering arrangement.

Devices with full protocol implementations, e.g. a proxy firewall are considered to act as a protocol peer.

2 References

2.1 Normative references

The following referenced documents are indispensable for the application of this document. For dated references, only the edition cited applies. For non-specific references, the latest edition of the referenced document (including any amendments) applies.

Not referenced in this ND but for further information -

- Ofcom guidance on security requirements in sections 105A to D of the Communications Act 2003

2.2 Informative references

[I1] ISO 27001:2013 Information technology – Security techniques – Information security management systems — Requirements (See note)

[I2] ISO 27002:2013 Information technology – Security techniques – Code of practice for information security management (See note)

Note: Permission to reproduce extracts from British Standards is granted by BSI under Licence No. 2008ET0029British Standards can be obtained in PDF or hard copy formats from the BSI online shop: www.bsigroup.com/Shop or by contacting BSI Customer Services for hard copies only: Tel: ++44(0)345 086 9001, Email: cservices@bsigroup.com.

The Licensee is permitted to make the publication available for download on the NICC website. This permission does not cover any other editions of the publication. On no account shall the extracts used be included as part of any other work not permitted under this licence. This permission relates to the extracts listed above. Where the standard is updated and/or if there is a requirement for further reproduction of extracts you will need to make a new application. Only English Language use of the extracts is permitted.

3 Definitions and abbreviations

3.1 Definitions

For the purposes of this document, the following terms and definitions apply:

Interconnection: The term Interconnection is defined as the linking (whether directly or indirectly by physical or logical means, or by a combination of physical and logical means) of one public electronic communications network to another for the purpose of enabling the persons using one of them to be able:

- To communicate with users of the other one; or
- To make use of services provided by means of the other one (whether by the provider of that network or by another person).

Interconnect equipment: Equipment involved in providing an interconnect.

Interconnect scope: The complete set of personnel, procedures, physical areas and electronic equipment within scope.

Physical Security areas: The physical security areas referred to in the ND1643 Controls are categorised into one of the following three types:

- Type A - An area owned and controlled by another CP who is in scope for ND1643, where other providers have unsupervised access. (E.g. BT MUA, Telehouse facilities etc.);
- Type B - An area owned and controlled by the CP being audited which is shared with other providers, who have unsupervised access. This area would be a type A area in their audit; or
- Type C - An area containing interconnect equipment which is not covered by A or B. Physical security must be controlled by the CP either directly or through subcontractors of the CP.

Secure perimeter: A room, cage, or rack effectively controlled by an access control mechanism (e.g. lock) restricting access to authorised personnel.

Shared area: Any area where the staff, or subcontractors of one CP, has physical access to equipment supporting another.

All equipment within a shared area: Equipment located within a shared area, whether or not the equipment is involved in an interconnect.
Note Environmental equipment remains out of scope for this.

Environmental equipment
Equipment located within a shared area, including but not limited to air conditioning, chillers, lighting etc.

3.2 Abbreviations

For the purposes of the present document, the following abbreviations apply:

BSI	British Standards Institute
CAS	CESG Assured Service

CP	Communication Provider
EU	European Union
H323	An ITU signalling protocol
IP	Internet Protocol
IPR	Intellectual Property Rights
ISO	International Standards Organisation
MPLS	Multiprotocol Label Switching
MUA	Multi User Area
ND	NICC Public Network Signalling Specifications
NDA	Non-Disclosure Agreement
NGA	Next Generation Access
NGN	Next Generation Network
NGNuk	Next Generation Network UK
NICC	NICC is a technical forum for the UK communications sector that develops interoperability standards for public communications networks and services in the UK
Ofcom	Office of Communications
SIP	Session Initiation Protocol
SIP-I	SIP with encapsulated ISUP
SIP-T	SIP for Telephones (SIP-T). SIP-T is used to carry ISDN signalling inside of SIP messages (in the body)
TDM	Time Division Multiplexing
UKAS	The United Kingdom Accreditation Service

For the purposes of the ND1634 Controls document, the following abbreviations apply

CV	Curriculum Vitae
HTML	Hyper Text Mark-up Language
ID	Identity
PDF	Portable Document Format
vLAN	Virtual Local Area Network

4 Control Requirements

In order to demonstrate adoption of this Guidance a CP should implement the relevant controls defined in Section 5, Controls.

5 Controls

By implementing all of the following controls, CPs may reduce the risks at sites where CPs are interconnected.

Guidance on Management Controls					
ND 1643 Control No.	**Significance**	**Control Objective/ Control**	**Guidance**	**Source**	**ISO 27002:2013 reference**
1	High	Documented scope	Maintain a documented scope that explains what and how the controls defined in this guide have been implemented. It should meet the scoping requirements as defined in this document.	ND 1643	
2	High	Documented scope	The documented scope should enable an independent reviewer and others to clearly identify the personnel, assets, suppliers and third parties, physical locations and secure perimeters.	ND 1643	
3	High	Documented scope	Relevant information on what is in scope should be made available to an interconnecting operator who requests it.	ND 1643	
4	High	Documented scope	A list of interconnects covered by the scope should be maintained, and this list should be available for review with an interconnect operator on demand.	ND 1643	
5	Medium	**Information security policy document**	An information security policy document should be approved by management, and published and communicated to all parties who implement the security controls advised in this guide. The policy should include measures for each of the recommendations of this document.	ISO 27002	5.1.1
6	Medium	**Information security policy document**	The policy should explain how your organisation implements the recommendations that are advised by the guidance.	ISO 27002	5.1.1
7	Medium	**Roles and responsibilities**	Communications Providers (CP) should be able to show that security roles and responsibilities are defined and documented.	ISO 27002	6.1.1

Guidance on Management Controls

ND 1643 Control No.	Significance	Control Objective/ Control	Guidance	Source	ISO 27002:2013 reference
8	High	**Screening**	CPs should carry out the applicable pre-employment checks on new workers subject to applicable legislation, for example: • Seek references • Check accuracy of applicant's CV • Confirm claimed professional qualifications • Complete an independent identity check • Check right to work: nationality and immigration status • Perform Criminal records checks.	ISO 27002	7.1.1
9	Medium	**Screening**	If the checks produce any anomalies or causes for concern then senior management should be involved in the consideration of the employment of the individual in question and if they remain in employment with the organisation then records of the consideration should be kept.	ISO 27002	7.1.1
10	High	**Access control policy**	An access control policy should be established, documented, and reviewed based on business and security requirements for access. The access control policy should apply to all relevant equipment, systems and sites within scope. It should cover: • The process for formal authorisation of access requests. (It is expected that the role responsible for operating access control must verify the identity of the individual, that access is appropriate for the individual's role, that management has approved the request and that the individual has had the appropriate security training/briefing.) The review of access rights at least annually. • The removal of access rights when an individual leaves or	ISO 27002	9.1.1

			moves to a role where access is no longer appropriate.		

Guidance on Management Controls

ND 1643 Control No.	Significance	Control Objective/ Control	Guidance	Source	ISO 27002:2013 reference
11	High	**Management of information security incidents**	Management responsibilities and procedures should be established to ensure a quick, effective, and orderly response to information security incidents. CPs should be able to describe the management responsibilities and procedures for a quick, effective, and orderly response to information security incidents affecting assets within scope.	ISO 27002	16.1.1
12	High	**Management of information security incidents**	The incident response procedures should take into account the possible impact on other interconnecting CPs, and include notification of any security incident affecting a shared area or an interconnect boundary device.	ISO 27002	16.1.1
13	Medium	**Compliance with relevant security policies and standards**	Managers should review, at least annually, the implementation of the applicable security controls defined in the guidance within their area of responsibility. If any issues are found as a result of the review, managers should: • determine the causes of the issue; • evaluate the need for actions to ensure that the issue does not recur; • determine and implement appropriate corrective action; • review the corrective action taken to ensure it is effective in addressing the issue. Results of reviews and corrective actions carried out by managers should be recorded and these records should be maintained.	ISO 27002	18.2.2

Guidance on Operational Controls					
ND 1643 Control No.	**Significance**	**Control Objective/ Control**	**Requirement**	**Source**	**ISO 27002:2013 reference**
14	High	**Third Party Agreements**	A CP may contract a third-party to implement some of the controls for which guidance is provided in this document. The current contract with the third party should clearly cover the relevant security requirements, and also cover the right to audit.	ISO 27002	15.1.2
15	High	**Third Party Agreements**	A CP may contract a third-party to implement some of the controls for which guidance is provided in this document. Any new or renegotiated contract with the third party should clearly cover the relevant security requirements, and also cover the right to audit.	ISO 27002	15.1.2
16	High	**Third Party Agreements**	Third party agreements should ensure that obligations are passed on further down the supply chain. The CP should monitor the enforcement of the security controls for which guidance is provided in this document in relevant third party agreements.	ISO 27002	15.1.3
17	High	**User authentication for external connections**	Administrative access to interconnect equipment from remote locations should be secured and controlled to prevent unauthorised access and configuration of the interconnect equipment.	ISO 27002	6.2.2
18	High	**Removal of Access Rights**	The access rights of all employees, contractors and third party users to systems within scope should be removed upon termination of their employment, contract or agreement, or adjusted if their role changes. CPs should ensure appropriate asset recovery/ disablement (computers, access tokens, keys etc.) for assets which facilitate access to equipment, systems and sites within scope. Account	ISO 27002	8.1.4 9.2.6

			closures should follow employment terminations.		

Guidance on Operational Controls					
ND 1643 Control No.	**Significance**	**Control Objective/ Control**	**Requirement**	**Source**	**ISO 27002:2013 reference**
19	High	**Removal of Access Rights**	Contracted third parties should implement a process to inform the CP of Personnel changes that impact access rights to in scope systems. Note: This control should be included in relevant third party agreements.	ISO 27002	7.3.1
20	High	**Removal of Access Rights**	CPs should implement a process to remove all access rights for suppliers who no longer require access.	ISO 27002	9.2.6
21	High	**Removal of Access Rights**	Where accounts are created on a interconnect partners equipment the interconnect partner should also be notified to close or modify access permissions as appropriate. The CP should ensure that they have a process for the removal of access rights, both physical and logical, in the event of employment termination or role change. This process may be manual or automatic, or a combination of both, and should be completed in a timely manner.	ISO 27002	9.2.6
Definitions	**Physical Security**		**For definitions of Type A, B and C physical facilities see ND 1643 Section 3.1 Physical security Areas**		
22	High	**Physical Security Perimeter**	A physical security perimeter should exist and be resistant to forced entry.	ISO 27002	11.1.1
23	High	**Physical Security Perimeter**	Locked racks, or caged areas, should be used for installations of racks in area types A and B.	ISO 27002	11.2.1
24	Medium	**Physical Security Perimeter**	The CP should have robust processes/policies in place to ensure that: • Employees display the appropriate photo ID cards, when required to by their organisation or the host's security policy. • Employees remain within authorised areas within sites.	ISO 27002	11.1.2

Guidance on Operational Controls					
ND 1643 Control No.	**Significance**	**Control Objective/ Control**	**Requirement**	**Source**	**ISO 27002:2013 reference**
25	Medium	**Physical Security Perimeter**	In a shared area equipment should be labelled effectively with a unique identifier. This helps prevent accidental modification of the wrong equipment. CPs may decide to put an identifier other than the company name on the equipment to help reduce the risk of a targeted attacked.	ISO 27002	11.2.1
26	High	**Physical entry controls**	CPs should lock or otherwise physically restrict access to area types B and C. Unsupervised access should only be granted to authorised individuals who have an operational need for access.	ISO 27002	11.1.2
27	High	**Physical entry controls**	A process should be in place for granting and removing access, whether the perimeter is controlled by the CP or a third party.	ISO 27002	9.2.6 and 11.1.2
28	Medium	**(Environmental) Equipment Maintenance**	All equipment under the control of the CP should be correctly maintained to minimise the risk of adverse impact on the environment containing other - CP's equipment	ISO 27002	11.2.2
29	Medium	**(Environmental) Equipment Maintenance**	The owning CP should set minimum equipment standards necessary to reduce the chance of electrical and fire safety incidents. Without such measures being taken catastrophic equipment failure (for example a fire or electrical fault) in a shared area may adversely influence the facility and other users.	ISO 27002	11.2.4
30	Medium	**Operating Procedures**	CPs should be able to demonstrate consistent operating practice for activities on equipment in scope.	ISO 27002	12.1.1

Guidance on Operational Controls					
ND 1643 Control No.	**Significance**	**Control Objective/ Control**	**Requirement**	**Source**	**ISO 27002:2013 reference**
31	Medium	**Change Management**	A change control process should exist. It should be applied to changes to the configuration of equipment within scope, and include: authorisation for changes, review of planned changes and maintaining a log of changes.	ISO 27002	12.1.2

Guidance on Technical Controls					
ND 1643 Control No.	**Significance**	**Control Objective/ Control**	**Guidance**	**Source**	**ISO 27002:2013 reference**
32	Medium	**Network controls**	The network should be configured so that only agreed traffic may cross the interconnect and originate from interconnect boundary devices. Except where direct communications are required, CP should maintain logical separation of the interconnect partner from other external sources (e.g. other interconnects, the Internet). Filters, SIP proxies, firewalls, vLANs or other technology may be used to maintain this separation.	ISO 27002	13.1
33	Medium	**Network controls**	Network design or architecture documentation should exist and cover the equipment within scope.	ISO 27002	13.1
34	Medium	**Audit logging**	Audit logs recording user and administrator activities (e.g. logon, logoff, configuration changes), and security events (e.g. failed authentications) should be produced and kept to assist in future investigations and access control monitoring. Logs should be retained for at least 90 days.	ISO 27002	12.4
35	Medium	**Audit logging**	If equipment cannot automatically log activity then the change management process should be used instead or to supplement the required information (see Control 31).	ISO 27002	12.4.1
36	Medium	**Control of technical vulnerabilities**	The CP should obtain timely information about technical vulnerabilities affecting the interconnect equipment and evaluate and address threats arising from these vulnerabilities.	ISO 27002	12.6.1

Guidance on Technical Controls					
ND 1643 Control No.	**Significance**	**Control Objective/ Control**	**Guidance**	**Source**	**ISO 27002:2013 reference**
37	Medium	**Control of technical vulnerabilities**	The deployment of vulnerability management solutions should follow change management processes. CPs should have a policy and procedures for vulnerability management. Records should be kept of vulnerabilities identified and whether they were patched, worked-around or dismissed as unnecessary to fix.	ISO 27002	12.6.1

History

Document history		
2.1.1	01/07/2010	Replaces the original edition, includes a number of improvements to clarity, auditability and pragmatism.
3.1.2	01/03/2012	Updated from V2.1.1 to latest NICC legal information and requirements from NGNuk.
3.1.3	30/07/2012	To clarify the inclusion of TDM, as per Ofcom guidance.
3.1.4	24/08/2012	Minor editorial and font changes made.
4.1.1	14/09/2015	Published with changes to the Scope, main sections and the Controls spreadsheet
5.1.1	21/12/2017	Published as Guidelines document while retaining the same ND number for consistency.