

NICC ND 1443 V2.1.1(2022-06)

NICC Document

Guidelines for the Security of All-IP Telephony (All-IPT) Service in the UK Telecommunications Network

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

NICC Standards Limited

NOTICE OF COPYRIGHT AND LIABILITY

© 2022 NICC Standards Limited

The present document may be made available in more than one electronic version or in print. In any case of existing or perceived difference in contents between such versions, the reference version is the Portable Document Format (PDF). In case of dispute, the reference shall be that printing on NICC printers of the PDF version kept on a specific network drive within the NICC.

Users of the present document should be aware that the document may be subject to revision or change of status. Information on the current status of this and other NICC documents is available at:

<http://www.niccstandards.org.uk/publications/>

If you have any comments concerning the accuracy of the contents of this document, please write to:

The Technical Secretary, NICC Standards Ltd,
PO Box 3090, Eastbourne, BN21 9HA

secretary@niccstandards.org.uk

Copyright

All right, title and interest in this document are owned by NICC Standards Limited ("NICC") and/or the contributors to the document (unless otherwise indicated that copyright is owned or shared with a third party). Such title and interest is protected by United Kingdom copyright laws and international treaty provisions.

The contents of the document are believed to be accurate at the time of publishing, but no representation or warranty is given as to their accuracy, completeness or correctness. You may freely download, copy, store or distribute this document provided it is not modified in any way and it includes this copyright and liability statement.

You may not modify the contents of this document. You may produce a derived copyright work based on this document provided that you clearly indicate that it was created by yourself and that it was derived from this document and provided further that you ensure that any risk of confusion with this document is avoided.

Liability

Whilst every care has been taken in the preparation and publication of this document, neither NICC, nor any working group, committee, member, director, officer, agent, consultant or adviser of or to, or any person acting on behalf of NICC, nor any member of any such working group or committee, nor the companies, entities or organisations they represent, nor any other person contributing to the contents of this document (together the "Generators") accepts liability for any loss or damage whatsoever which may arise from the use of or reliance on the information contained in this document or from any errors or omissions, typographical or otherwise in the contents.

Nothing in this document constitutes advice. Nor does the transmission, downloading or sending of this document create any contractual relationship. In particular no licence is granted under any intellectual property right (including trade and service mark rights) save for the above licence to download copy, store and distribute this document and to produce derived copyright works.

The liability and responsibility for implementations based on this document rests with the implementer, and not with any of the Generators. If you implement any of the contents of this document, you agree to indemnify and hold harmless each Generator in any jurisdiction against any claims and legal proceedings alleging that the use of the contents by you or on your behalf infringes any legal or other right of any of the Generators or any third party.

None of the Generators accepts any liability whatsoever for any direct, indirect or consequential loss or damage arising in any way from any use of or reliance on the contents of this document for any purpose.

The NICC Standards Web site contains the definitive information on the [IPR Policy and Anti-trust Compliance Policy](#)

Contents

Intellectual Property Rights	5
Foreword.....	5
Introduction	5
1 Scope	6
2 References	6
2.1 Normative references.....	6
2.2 Informative references	6
2.3 Conventions.....	7
3 Definitions, symbols and abbreviations.....	8
3.1 Definitions	8
3.2 Abbreviations.....	9
4 All-IP Telephony Architecture overview	11
4.1 All-IPT CPE	13
4.2 DECT & CAT-iq	13
5 Threats to the All-IP Service	14
5.1 Threats	14
5.1.1 Fraud.....	14
5.1.2 Misuse of Service	15
5.1.3 Denial of Service	15
5.2 Mitigations and controls	15
5.3 Threat Sources and actors	16
6 IPT Service Security Dependencies	17
6.1 DNS	17
6.2 CPE Testing and Security	17
6.3 All-IP and Emergency calls	17
7 IP Voice Security Areas/Implementation	18
7.1 IPT Platform Security	18
7.2 CPE Security Implementation.....	19
7.3 CPE security assessment.....	19
7.4 IPT Signalling Security.....	20
7.5 IPT Media Security	20
8 IP Voice Cryptographic Security	21
8.1 Cryptographic Methods	21
8.1.1 Public Key Infrastructure.....	22
8.1.2 Symmetric Encryption	22
8.2 Cryptographic Tunnelling Methods.....	22
8.2.1 Use of IPSec	22
8.2.2 Use of TLS.....	23
8.2.3 Use of SRTP	23
9 Generic Security Controls	24
9.1 Access Controls	24
9.2 Good Practice information and guides.....	24
9.2.1 Cyber Essentials Scheme	24
9.2.2 NCSC 10 Steps to Cyber Security	24
9.2.3 Fraud Mitigation Documentation.....	24
9.3 Threat intelligence and Threat actor classification	25
9.4 Vulnerability Management	26
9.5 Understand IPT assets.....	26
9.6 Business Impacts	27
9.7 Controls and organisational structure	27
9.7.1 Typical controls	27
9.7.2 Security Event Management	28

9.7.3 Change Control.....	28
9.7.4 Root Cause Analysis.....	28
9.8 Response and Escalation.....	29
9.9 Security Operations Centre SOC	29
9.10 Privacy	29
History	31

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 jointly produced by NICC Security and All-IP Task groups.

Introduction

All CPs must secure their voice services over the access network. This document gives guidance on the areas that must be considered when securing an All-IP Telephony [All-IPT] service. All-IP Telephony is a service based on VOIP technology intended as a replacement for fixed line PATS service (i.e. a voice service available to the public for originating and receiving calls).

The purpose of this document is to offer security best practices to be used by the industry and anyone involved in the design, operation and management of All-IP Telephony services

As technology evolves, so do the threats of malicious activity; for example the evolution of artificial intelligence, may compound today's challenges in securing networks. Adverse events could arise from an intended action or simply poor practice. As such, the All-IP Telephony (All-IPT) Service must use security best practice in the UK Telecommunications Network. It is often the lack of basic security hygiene that leads to a malicious activity and as such the document will aim to highlight fundamental areas of security best practice as well more technology specific items.

1 Scope

This document makes recommendations for security best practice to be implemented by the CP providing All-IPT services on its network platform (including IPT CPE).

All-IP Telephony is a fixed line PATS replacement service, so its scope is restricted to conventional telephone instruments. It does not include smart devices that are not fixed to a location. Likewise SIP soft phone client running on wired/wireless broadband internet is also out of scope for the purposes of this document.

NNI interfaces are out of scope for this document; for detail relating to this see normative reference [2].

This is a guidance document; any NICC or other normative specifications referred to in this document should be treated as authoritative.

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.

- [1] BSI Standard ISO 22301 Business Continuity Management
- [2] NICC ND1647 SIP-NNI Basic Voice Architecture.
- [3] NICC ND1704 End-to-End Network Performance Rules & Objectives for the Interconnection of NGNs.
- [4] FCS Fraud Mitigation Standard Specification.
- [5] NICC ND1438 Voluntary Code of Practice. Mitigating Theft of Service from End User Voice over IP Communications Systems.
- [6] NICC ND1431 Guidance on CPE Compatibility on NGN and NGAs
- [7] 3GPP TS 33.210 3G security : Network Domain Security (NDS) IP network layer security
- [8] 3GPP TS 33.310 3G security : Network Domain Security (NDS) Authentication Framework

2.2 Informative references

- [i1] National Cyber Security Centre. 10 Steps to Cyber Security. Updated: 09 Aug 2016.
- [i2] National Cyber Security Centre. Introduction to the NIS Directive. Updated: 30 Apr 2016.
- [i3] National Cyber Security Centre. Security operations centre (SOC) buyer's guide. Updated: 24 Sep 2016.
- [i4] Information Commissioners Office. Data Protection impact assessment.
- [i5] Information Commissioners Office. Data protection by design and default.
- [i6] GOV.UK Cyber Essentials Scheme: overview.

- [i7] National Cyber Security Centre: Self-help for Cyber Essentials.
- [i8] TUFF – Telecommunications UK Fraud Forum (CSG (linked to TUFF)).
- [i9] Action Fraud – National Fraud & Cyber Reporting Centre.
- [i10] Cifas – ”Fraud Prevention organisation.
- [i11] ACFE – Association of Certified Fraud Examiners.
- [i12] DECT.org CAT-iq Certified products.
- [i13] ETSI Network Function Virtualisation
- [i14] NIST Special Publication 800-81-2. Secure Domain Name System (DNS) Deployment Guide.
- [i15] Cyber Security Information Sharing Partnership (CiSP).
- [i16] CBEST Intelligence-Led Testing - Understanding Cyber Threat Intelligence Operations
- [i17] NCSC-CyBOK Cryptography Knowledge area

2.3 Conventions

The ETSI Key words are applicable throughout this document.

3 Definitions, symbols and abbreviations

3.1 Definitions

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

All-IP Telephony [All-IPT] Service	All-IPT is a fixed line PATS replacement service.
CBEST	CBEST is a framework to deliver controlled, bespoke, intelligence-led cyber security tests. The tests replicate behaviours of threat actors. Setup for the financial services sector but offering excellent documentation resources for wider industry.
Denial of Service	Often a malicious attempt to make a host(s) or network resources unavailable to genuine users temporarily or indefinitely by disrupting the intended functioning of the system(s), for example by flooding it with access/connection requests.
European Union (EU) General Data Protection Regulation (GDPR)	(GDPR) (EU) 2016/679 is a regulation in EU law on data protection and privacy for all individuals within the European Union (EU) and the European Economic Area (EEA).
Fully Integrated Architecture	Framework based on real-world experience, to provide strong focus on business requirements and drivers, and all aspects of the architecture and all architectural decisions are traceable.
Hashing Functions	A hash is an outcome of the cryptographic algorithm mathematical function that takes an input string and generates an outcome that is irreversible unique string of alphanumeric characters such that no two hash outcomes are ever the same irrespective of length and format of input string. Examples of hashing algorithms are: MD5, RIPEMD, Whirlpool, SHA-1, SHA-2 and SHA-3.
Hybrid Architecture	Using a mix of technologies and platforms but having a centralised approach.
NFV	Network functions virtualization (NFV) defines standards for compute, storage, and networking resources that can be used to build virtualised network functions.
PATS	Publicly Available Telephone Service (PATS) means a service made available to the public for originating and receiving, directly or indirectly, national or national and international calls through a number or numbers in a national or international telephone numbering plan.
PIN Codes	Personal Identification Number: may be numbers only, or combination of numbers and letters, dependant on the CPE device type.
PKIX	PKIX is an IETF (Internet Engineering Task Force) working group with the goal of supporting public key infrastructures (PKI) based on X.509 on the Internet
Red Team	Taken from a military term. Defined loosely, red teaming is the practice of viewing a problem from an adversary or competitor's perspective.
Salt	Salt cryptography. A "salt" is a value used to modify a hash of a password.

SD-WAN	Software-defined wide area network (SD-WAN) is a specific application of software-defined networking (SDN) technology applied to WAN connections, which are used to connect networks.
SDES	Session Description Protocol Security Descriptions for Media Streams is a way to negotiate the key for use within Secure Real-time Transport Protocol (SRTP).
SIM/e-SIM	Subscriber Identification Module (SIM), widely known as a SIM card, is an integrated circuit that is intended to securely store the international mobile subscriber identity (IMSI) number and its related key, which are used to identify and authenticate subscribers on mobile telephony devices. An embedded-SIM (eSIM) is a form of programmable SIM that is embedded directly into a device.
SIP	Session Initiation Protocol. It is a client server/client client communication protocol that is used to set up, maintain and tear down communication sessions, in current scope – voice sessions between IP telephony platforms.
Theft of Service	The unauthorised use of system functions with the intent of financial gain or restricting legitimate use of system resources.
Threat Actor	A threat actor or malicious actor is a person or entity that is responsible for an event or incident that impacts, or has the potential to impact, the safety or security of another entity.
Two factor authentication	Two factor authentication is a second layer of security used to make sure that people trying to gain access to a system are who they say they are. Firstly, a user will usually enter their username and a password. Then, instead of immediately gaining access, they will be required to provide another piece of information. This second factor could come from one of the following categories: <ul style="list-style-type: none"> • Something you have (e.g. mobile phone) • Something you are (e.g. biometrics)
Voice mail system	A system that provides for a number of “mail boxes” to which callers are directed, when the respective users are unavailable. The “mail boxes” are for the recording of messages from callers. It is usual for voice mail systems to provide a notification to the user that message(s) are waiting. Voice mail systems are often integrated with a call routing or similar apparatus in a manner that enables a caller to dial further digits to select an alternative user.

3.2 Abbreviations

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

ATA	Analogue Telephony Adapter
B2BUA	Back-to-back user agent
CAT-iq	Cordless Advanced Technology – internet quality. Enables the DECT (Digital Enhanced Cordless Telecommunications) telephony standard to be used with VoIP and other internet-based services
CA/RA	Certificate Authority / Registration Authority
CMP	Certificate Management Protocol
CRL	Certificate Revocation List
CP	Communications Provider
CPE	Customer Premises Equipment

CSR	<i>Certificate Signing Request</i>
DECT	<i>Digital Enhanced Cordless Telecommunications</i>
DH	<i>Diffie-Hellman (a method of secure key exchange)</i>
DMZ	<i>De-Militarised Zone</i>
DNS	<i>Domain Name System</i>
DNSSEC	<i>Domain Name System Security Extensions</i>
DoS	<i>Denial of Service</i>
DDoS	<i>Distributed Denial of Service</i>
E2E	<i>End to End</i>
IDS	<i>Intrusion Detection System</i>
FCS	<i>Federation of Communication Services</i>
IP	<i>Internet Protocol</i>
IP-PBX	<i>Private Branch Exchange connected to a telephony Network over the Internet Protocol</i>
IPS	<i>Intrusion Prevention System</i>
IPSec	<i>Internet Protocol Security</i>
IPT	<i>Internet Protocol Telephony</i>
ISP	<i>Internet Service Provider</i>
ITSP	<i>Internet Telephony Service Provider</i>
ITSPA	<i>Internet Telephony Services Providers' Association</i>
LAN	<i>Local Area Network</i>
NNI	<i>Network to Network Interface</i>
ONT	<i>Optical Network Termination</i>
OCSP	<i>Online Certificate Status Protocol</i>
OSS	<i>Operational Support Systems</i>
PATS	<i>Publicly Available Telephone Services</i>
PDU	<i>Protocol Data Unit</i>
PEM	<i>Privacy Enhanced Mail</i>
PII	<i>Personal Identifiable Information</i>
PKI	<i>Public Key Infrastructure</i>
PSK	<i>Pre-Shared Key</i>
RSA	<i>Rivest–Shamir–Adleman (a method of secure key exchange)</i>
RTP	<i>Real-time Transport Protocol</i>
SBC	<i>Session Border Controller</i>
SDES	<i>Session Description Protocol Security Descriptions</i>
SIP	<i>Session Initiation Protocol</i>
SRTP	<i>Secure Real-time Transport Protocol</i>
TLS	<i>Transport Layer Security</i>
TR069	<i>(Technical Report) Management interface for CPE</i>
VOIP	<i>Voice over IP</i>
PBX	<i>Also known as PABX. Private Automatic Branch Exchange</i>
UNI	<i>User to Network interface</i>
X509	<i>ITU-T standardised format of the certificate file</i>

4 All-IP Telephony Architecture overview

The specific architecture used to implement an All-IPT service will be determined by the owning Communication Provider (CP). For the purposes of this document, a generic architecture model is assumed, as shown in Figure 1 below.

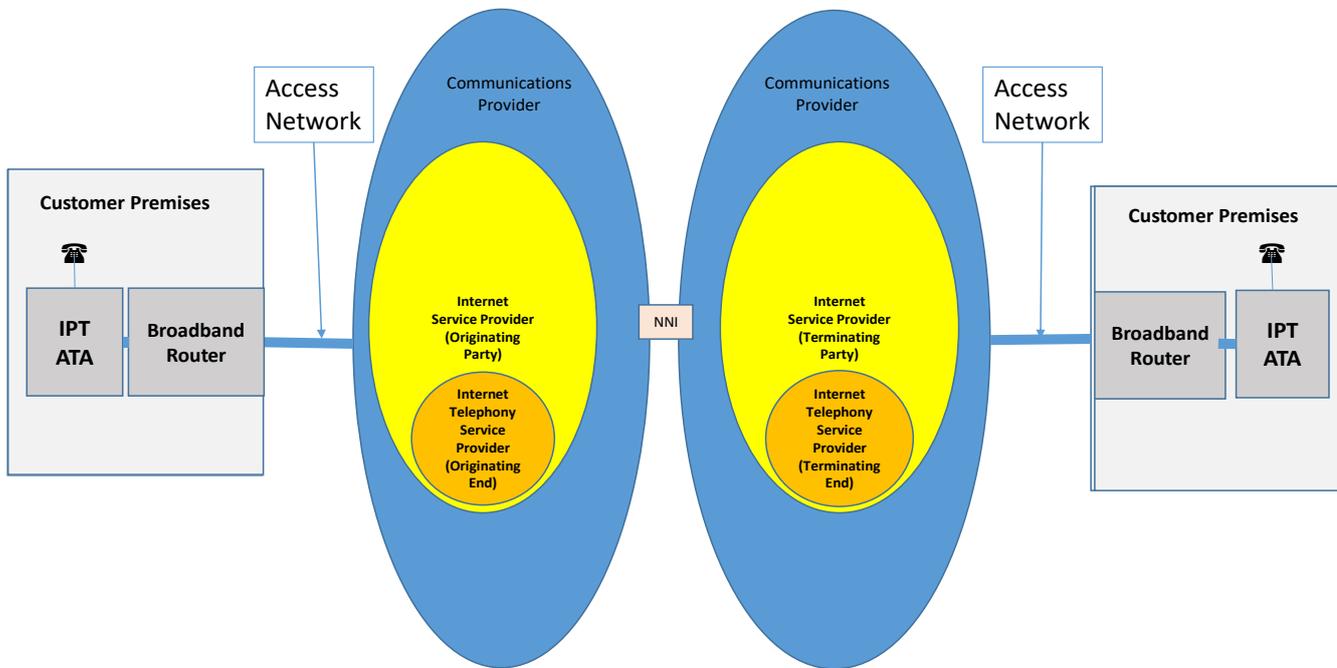


Figure 1: Generic Architecture

Typically, CPE to IPT Platforms use;

- SIP for signalling, and
- RTP for media

with an option to use TLS to secure SIP signalling and SRTP for added media security.

The end-to-end All-IPT architecture comprises the following functional blocks;

1. IPT ATA i.e. a SIP aware telephony endpoint connecting the customer's telephony equipment to the All-IPT service. [Supplied and managed by owning CP]
2. Fixed line broadband home router interfacing with ISP/ITSP.
3. Telephony platforms of the IPT Communication Provider network.

Within the scope of this document, it is assumed the telephony instrument connecting to the SIP endpoint (via the ATA) would be a traditional telephone instrument (wired or cordless). Also, the SIP aware endpoint shall be a standalone or broadband router with built-in ATA.

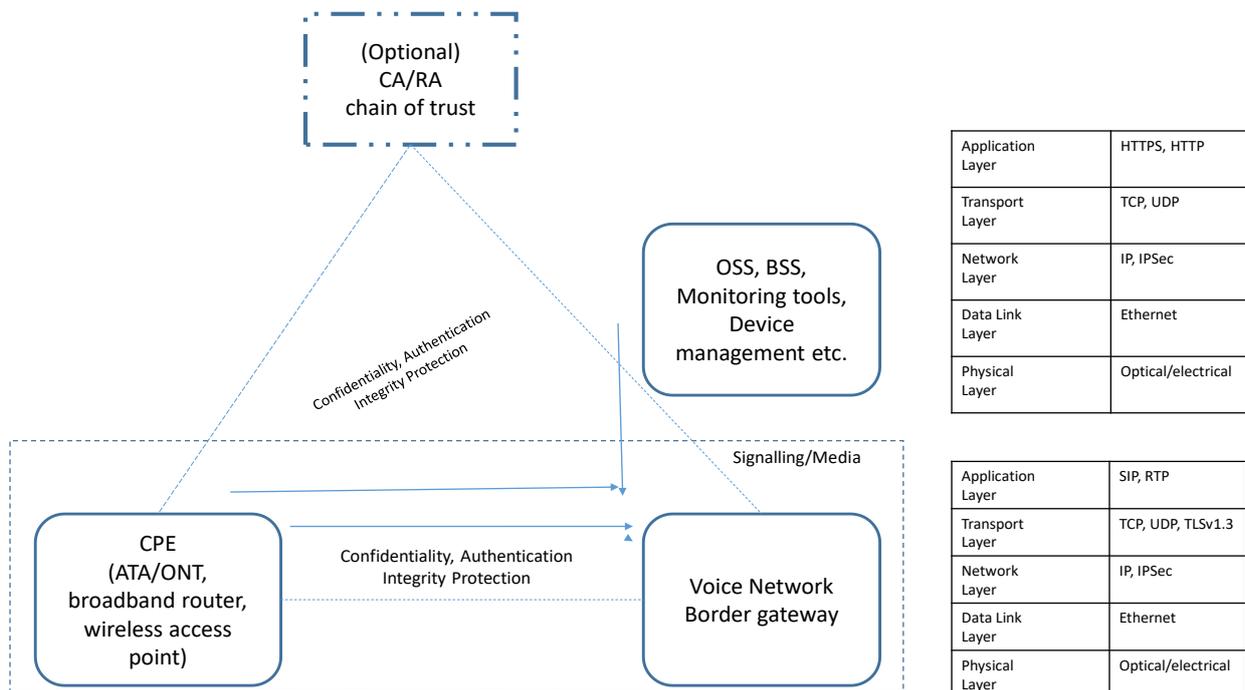
Within the internet telephony provision there are a number of key components:

- Border Gateways – protecting the service provider from the Access Network and the connection point for the customer’s broadband router for the IPT service.
- Customer Authentication Database – Used to authenticate customer’s credentials and set up a chain of trust between the CP network and the customer’s broadband router. This may include a CA (Certificate Authority).
- SIP Server – this communicates using SIP signalling between the ATA and the rest of the network to set up telephone calls.
- DNS – CP’s may have their own DNS servers to speed up IP address resolution in their network.
- OSS to monitor and control elements within the network.

Networking technology relating to NFV or SD-WAN are recognised as being potential building blocks of an end-to-end IP telephony service but beyond the scope of this document. See normative reference [i13]

The telephony user could be served by a single Communication Provider or could be served by two separate Communication Providers where the IP transport is provided by one CP, but telephony service is provided by another CP.

Figure 2: Key interfaces



The key interfaces involved are as follows:

Client End	CP End	Interface	Purpose
CPE	Voice Network Border Gateway (Voice SBC)	SIP, RTP TLS\SIP, SRTP	Control plane and User Plane
CPE	Device Management Server	TR69, HTTPS XML type exchange	Configuration management and Provisioning
CPE	O&M Systems	SNMP alarm traps	Operations & Support Fault Reporting and Monitoring

4.1 All-IPT CPE

There are a number of typical implementations for the end customers to connect telephone instruments to an IP voice service.

- 1) Use a separate Analogue Telephony Adaptor (ATA) that takes a LAN connection from the customer home broadband router and provides a means to connect a phone to this additional external device.
- 2) Using a device where the ATA is integrated within the home broadband router and a telephony port is presented on this integrated unit.
- 3) Use a DECT based ATA, where DECT is also integrated in the home router. Allowing the call device to be anywhere in range of the DECT transmitter.

4.2 DECT & CAT-iq

DECT based handsets are a common feature in many solutions, and therefore some knowledge of the standards in that area would be an advantage. CAT-iq is a standards-based technology owned by the DECT Forum. Within this forum there are certification processes to cover the CAT-iq certification process in addition to DECT Security certification process. NB: CAT-iq 2.1 integrates both into a single certification. See Informative reference [i5].

5 Threats to the All-IP Service

5.1 Threats

A threat is the intent to do harm in some way such as destroy something or weaken or deprive someone of something. This, in the IP domain, is typically done by exploiting a vulnerability, such as poorly written code or a defect within the code.

National Cyber Security Centre (NCSC) define a cyber threat as:

“Malicious attempts to damage or disrupt devices, services and networks - and the information on them”

For more detail and references see section 9.3 of this document.

The information and telephony being transported over IP has a potential of being compromised in various ways resulting in potential loss of secrecy, integrity, authorised access to the network and unlawful misuse of the data. These may result in financial, reputational, legal and regulatory punitive measures and loss of confidence of shareholders and customers.

For an All-IP Telephony service, a key risk to the service is loss of revenue and or reputational damage through unauthorised use of the service.

By moving away from a traditional circuit switched Telephony system, where the data and control planes are in the main isolated, to an IP based telephony system the threat landscape will increase significantly due the exposure to external IP interconnects and even the internet (via gateways).

Key threats to IPT are;

1. Fraud
2. Misuse of service
3. Denial of service

To invoke the above threats, enabling actions such as “Man in the middle actions” or “Reconnaissance actions” may be invoked.

“Man in the Middle actions” are actions which allow an attacker to act as a look-alike end point or platform to capture information. This information could be used to impersonate or adversely affect the customer’s service or use the service fraudulently.

“Reconnaissance actions” are those actions which allow the configuration or data to be acquired for future use to potentially attack the service.

5.1.1 Fraud

Fraud is the ordering or use of a service with no intent to pay. This results in either the Communication Provider losing revenue, or a different subscriber being charged for the service (if, for example the fraudster is using the subscriber’s credentials).

The National Crime Agency (NCA) has statistics that show fraud using Cyber means is growing significantly.

5.1.2 Misuse of Service

The Misuse of service is any action performed against the service to adversely affect the IPT Customer or IPT CP. This could be instigated by an unauthorised user either hacking a legitimate user's access or attempting to harvest and use information that would be used to misuse services.

5.1.3 Denial of Service

Denial of Service (DoS) is an (often malicious) attempt to make a host(s) or network resources unavailable to genuine users temporarily or indefinitely by disrupting the intended functioning of the system(s), for example by flooding it with access/connection requests.

Typically, DoS attacks take one of these forms;

1. Targeted DoS attacks to a platform which could include TCP/IP, DNS and SIP attacks.
2. Distributed DoS (DDoS) attacks, where multiple endpoints are used to produce an advanced form of service denial.

To protect against DoS there is a need to ensure that only "Authenticated" devices should make calls using IPT. Depending on implemented architecture, this should either be explicit, (e.g. end device must be explicitly registered) or some method of implicit authentication (e.g. end device has been previously authenticated).

This is particularly important for emergency contact service numbers (i.e. 999). To maintain availability (for individual and the whole service) there is a need to balance customer availability against denial-of-service potential to the emergency service.

5.2 Mitigations and controls

The solutions to mitigate the associated threats to an All-IPT service are significantly different to that of a traditional fixed line telephony service where, historically, all the control traffic was isolated within the telephone exchange perimeter. An All-IPT may expose control traffic, such as SIP, to the customer endpoint demarcation. This creates far bigger challenges for security of the IPT service and presents a larger attack surface.

Typical mitigations would consist of: -

1. Identity and credit checks as part of the ordering process.
2. Access control on service portals to restrict users to only access information to which they are entitled.
3. Use of user identification, authentication and authorisation controls; for example, by logging into the CP's website with username and password.
4. Access control on services accessed through the telephone handset, such as for voicemail and other supplementary services, for example, by enforcing the user to enter a PIN to access the service.
5. Design considerations to ensure that only allocated and identified CPE/broadband lines can be used by the IPT to provide a specific customer service, for example, by binding authorised CPE to the broadband line ID and possibly the IP address, in order to authenticate IPT service. This would provide confidence in location information for 999 service on IPT.
6. Use of SIP authentication between IPT ATA and IPT Platform, with robust mechanisms in place to prevent disclosure of the associated SIP credentials.

7. Consideration should be given to employing transport layer security between systems utilising up to date protocols and algorithms to prevent man in the middle interception and enable trusted endpoint connections. See section 8.

Consideration should also be given to implementing the following protections, namely:

- On CP Service Portals:
 - Single sign-on between multiple areas of the service portal, so that the user does not have to enter a different password for each area of the service portal,
 - Two factor authentication, for example where user receives a unique PIN code to his mobile number after putting password to login.
 - Bilateral verification, where the user can verify that the portal is a genuine web portal and the Communication Provider should be able to verify the identity of the user logged in.
- On CP Platforms:
 - Configuration of the IPT platform in accordance with CP's security policy, and with IPT platform vendor's recommendations.
 - Network traffic /Signalling/ and Platform monitoring
 - Use of intrusion prevention mechanisms such as Firewalls, SBCs or IDS, and consider judicious use of Intrusion Prevention Systems.

Consideration should also be given to the way internal access of the IPT platform and associated OSS/BSS is managed, such as;

- Implement suitable OSS/BSS configuration and implementation to prevent misuse of key services, for example call diversion, premium numbers misuse etc. As a minimum all usage should be monitored, and targeted preventative methods employed where possible.
- When designing the service, attention should be given to the amount of detail that is provided in terms of physical labelling and potential for connecting un-authorized devices. The same principles apply with the underlying operating system and application to minimise the amount of detail disclosed when the device is accessed.
- Controls should be put around any areas where mitigation still shows a higher residual risk than the business would want to tolerate. It is important that these controls are detailed, and time bound for review with clear accountability.

5.3 Threat Sources and actors

Large organisations will have their own trusted resources for intelligence which is beyond the scope of this document. See Section 9.3 for information and references associated with the fraud aspects. Up to date credible threat intelligence is essential in order to apply mitigation in a timely manner and manage the associated risks.

6 IPT Service Security Dependencies

The delivery of the IPT service has several underlying dependencies and associated criteria. These include

1. Delivery of customer broadband service including DNS.
2. Design and implementation of customer CPE.
3. Requirements for delivering the 999 service

6.1 DNS

Traditionally, deployment and use of DNS has been ubiquitous in the World Wide Web. The evolution of telephony and overall communication network-based services delivery has resulted into incorporation of DNS related technologies in IPT communication services.

Implementations vary largely but use of FQDN (Fully Qualified Domain Name) in SIP registration and telephony sessions require some form of name resolution by the name server at communication provider end. This is achieved either by dynamic exchange of DNS query/response or by static mapping in local host files.

Such variations mandate consideration of securing DNS infrastructure and its associated communication. DNSSEC, briefly described below, is one of many means, to achieve this end goal.

Secure DNS could be considered if there are concerns around the integrity of DNS communication within the IPT solution. Typically, DNS can be susceptible to a range of exploits such as forged DNS updates, unauthorised zone transfer, cache poisoning and man in the middle attacks. Secure DNS can help protect against this to ensure a valid source of DNS response that has not been tampered with in transit and adds a digital signature to DNS responses using a chain of trust to validate responses.

Integrating Secure DNS into an existing solution may be more complex than taking a green field approach but Secure DNS is more complex to implement and operate than traditional DNS deployment and is why it is not widely adopted in industry. See informative reference [i14].

6.2 CPE Testing and Security

CPE testing and security is a key part of the overall security of any All-IPT solution. Consideration must be given to both hardware and software testing to find security issues. This will mean the use of software testing tools and possibly engaging 3rd party penetration testers. If using 3rd party hardware/software then consideration must be given to the vendor providing evidence of such testing.

6.3 All-IP and Emergency calls

The owning CP must meet the current General Conditions of Entitlement which refers to CPs responsibilities with respect to safeguarding customer access to the Emergency Services (at the time of writing specifically Part A3 of Annex 14 (2017)).

7 IP Voice Security Areas/Implementation

For any specific All-IPT implementation there will be a defined architecture. From this there will be several specific areas that will need to be addressed;

1. IPT Platform Security.
2. CPE to IPT network transport design, including CPE authentication and IPT dependencies such as DNS, broadband network etc.
3. CPE Security implementation.
4. Signalling Security, including SIP authentication.
5. Media Security.
6. Security hardening of All-IPT platform Components
7. The ability to assure the implementation against known vulnerabilities and deviation from hardening baselines.

7.1 IPT Platform Security

The aim of security is to reduce exploitable risk to the Platform/Service/Product and mitigate the impacts of any incidents. This is achieved by a circular approach, i.e. identify risk, prevent (by putting in place mitigations, controls or design enhancements), detect security incidents and react in a timely and appropriate manner to security events (ideally pro-actively).

The following security considerations should be made:

- A SIP aware boundary device (such as a Session Border Controller [SBC]) is strongly recommended to provide the following features;
 - Act as a back-to-back user agent (B2BUA)
 - Provide network topology hiding
 - Protect the network and other devices from:
 - Malicious attacks such as a denial-of-service attack (DoS) or distributed DoS
 - Fraud via rogue media streams
 - Malformed packet protection
 - QoS policy of a network and prioritization of flows
 - Control of media flows
- The SBC should be configured to only allow IPT service required protocol signalling from the trusted All-IPT CPE endpoint. All other application ports should be administratively disabled.
- Secure generation, management, distribution and storage of authentication credentials and encryption keys for the All-IPT service. Examples of this include SIP digest authentication methods, implementation of TLS and/or IPsec. These will require security procedures for handling security credentials, such as SIP Passwords, X509 certificates and encryption key pairs on the IPT Platform and on the CPE.
- The IPT platform should be accessible for user plane and control plane traffic by exposing only a limited amount of public facing interfaces whose identities are embedded into the CPE firmware configuration, such that it is not accessible for the end user to read or amend.

7.2 CPE Security Implementation

All-IPT CPE (because of its use in association with multiple services) needs to be securely managed, usually over the customer broadband.

As the IPT service is of a fixed (rather than a Nomadic) VoIP type, care may need to be taken in order to ensure that Home Routers supporting the All-IPT service are connected to a data line allocated to a customer's specific voice identity e.g. a geographic E.164 number. Such protection may be afforded through an authentication server, so ensuring that a hub is indeed connected to an appropriate data (e.g. Broadband) connection.

CPE security will be dependent on the chosen, implemented IPT architecture. However, the following areas should be considered as part of the CPE design.

- Security software Design including
 - Security of log files stored on the CPE.
 - Security of the boot process of the CPE.
- Prevent being able to tap into the service from the copper line/optical line side of the CPE.
- Prevent DOS attack towards the Communication Provider infrastructure (SIP or Media).
- Validation and prevention of spoofing/manipulation of SIP messages.
- Secure Management Channel

7.3 CPE security assessment

The CPE architecture will be implementation dependent, however NICC recommend some areas that would benefit from Penetration testing that should give insight to any security weaknesses;

- Testing against IPT enabled CPE used by the IPT service (This could be ATA or CAT-iq enabled equipment and associated CP supplied home router/hub)

Tests should include-

 - Security of log files stored on the CPE.
 - Security of the boot process of the CPE.
- Testing using non-All-IPT voice enabled CPE and third-party CPE to determine if it is possible to attack the IPT service platforms.
- Testing CAT-iq specific for handset spoofing and/or Man in the Middle attack.
- Un-intended access to any control or protected data from the customer LAN side interfaces
- Any ability to tap into the service from the copper line/optical line side of the CPE.
- Ability to launch a DOS attack towards the Communication Provider infrastructure (SIP or Media).
- Validate if SIP messages can be spoofed or manipulated (E.g. (fake calls/ bye requests/not available response).

Many security issues should be prevented within the integration testing process and mitigated /removed at an early stage of the development life cycle.

7.4 IPT Signalling Security

As discussed in Section 5 of this document there are 3 main threats to service: Fraud, misuse of service and denial of service. In an IPT world all of these threats can be leveraged by monitoring the Signalling path and pulling out user credentials or manipulating the signalling path with false, excessive or malformed requests.

To prevent these kinds of problems it is vital that steps are taken to protect the signalling path when it is passing over networks outside a CPs control. Such steps should be implemented for *all* links in the path to reduce the risk of information being harvested and passed on to threat actors. However, encrypting all links in the path is non-trivial for centralised CPs with large infrastructure, with significant cost for minimal risk mitigation; hence CPs should pass this through their own threat models.

Most App based solutions can implement end to end encryption quite easily. However, infrastructure CPs (ITSPs) cannot as -

- there is no direct IP to IP link for their customers
- CPE is of unknown capability,
- traffic may pass over TDM circuits (at this point in time), especially if one end is still using a circuit switched POTS service,
- there are legal requirements which prevent true end to end encryption

CPs should implement encryption over high-risk links from the customers' CPE (i.e. the home router) into the CP's termination point (i.e. SBC), where there is the potential for an external attack vector.

Implementations should therefore make use of transport network design and device authentication such as:

- Transport security using IPSEC/PKI or TLS.
- CPE authentication (SIP authentication or SIM based technology).

For more details on encryption see section 8.

7.5 IPT Media Security

To cover privacy obligations it is incumbent on CPs to provide some measure of protection to the media stream of an IPT call. This prevents against eavesdropping or media manipulation such as diverting, inserting or replacing the media stream in one or both directions.

Again, this is architecture dependent, but consideration should be made to implement Media security protections (i.e. SRTP) over network links i.e. between customer CPE and the CP's termination point (as discussed in section 7.4). This provides encryption of the media streams preventing the attacks discussed above.

For more details on SRTP encryption see section 8.2.3

8 IP Voice Cryptographic Security

To ensure the confidentiality, integrity and authentication of the information on the communication networks, the appropriate use of asymmetric cryptography (PKI) or symmetric cryptography is recommended. It is likely that a solution may make use of one or other or both types of encryption within it.

For All-IP Telephony, the main areas to be considered for application of cryptography are

- Protection of signalling with a focus between customer device and Telephony Platform.
- Protection of media
- Protection of data
- Protection of management/system access

A risk-based analysis of the chosen architecture (to deliver All-IPT) should be used to determine what security needs to be implemented and in which parts of the solution.

The use of tunnelling methods will also need to be considered. The options for this are covered in section 8.2.

8.1 Cryptographic Methods

There will be a need to consider the use of both "Symmetric" key and "Asymmetric" key solutions. A number of important security architecture decisions will be needed. This will include

1. How is signalling confidentiality, integrity and authentication to be achieved? Does the chosen architecture inherently provide this (e.g. secure transport design) without the need for additional protections?
2. How is device/account authentication to be implemented?
3. How is confidentiality, integrity and authentication of the data in the customer equipment and All-IPT platform maintained?
4. How is confidentiality of the media data to be achieved?
5. What secure protocols/mechanisms are needed to control user/support management on the All-IPT Platforms and systems?

The following subsections provide some important areas for potential consideration and use. It is not intended to be a full and prescriptive definition of the security that needs to be implemented for a chosen All-IPT solution. A full end to end security analysis and design should be undertaken for a CPs chosen All-IP architecture.

It should be noted that the use of encryption techniques by the Communication Providers, such as secure SIP and SRTP, will result in the loss of visibility of the traffic for lawful intercept and diagnostic purposes. To gain visibility either:

- the encryption will need to be removed at the interface where lawful interception is required, and operational diagnostics data are gathered, or

- some mechanism will be needed to decrypt the secure channel.

For further information and research the NCSC provides a knowledge base on Cryptography which may be useful. See normative reference [i17].

8.1.1 Public Key Infrastructure

One option for cryptography is to use Public Key Infrastructure using X.509 (PKIX) in the communication networks for embedding the three security principles (confidentiality, integrity and authentication) into the overall solution architecture.

The PKI is a framework that encompasses hardware, software, people, processes and procedures involved in the security infrastructure deployed within the CP. It could be a logical function running in software or could be a dedicated high-density hardware-based separate multi-tier distributed infrastructure that is responsible for ensuring security for the services offered by the communication provider.

It uses asymmetric cryptographic algorithms (which uses two unique, distinct pairs of keys) to authenticate client-server entities participating in an application layer protocol handshake to establish a secure transport link for the application layer in the TCP/IP protocol suite.

Normal components such as a CA (Certificate Authority) and a CRL (Certificate Revocation List) Database will need to be deployed. A CP will need to engage specific expertise to deploy PKI architecture, taking into account the latest recommendations for encryption and hashing algorithms.

8.1.2 Symmetric Encryption

Another option, used by mobile networks, is to deploy symmetric key pairs (or pre-shared keys), one on the customer device (either by SIM card or E-SIM) and one in the network. There are a number of challenges to be met using this method, not least the security and management of the Master database of keys in the network and the distribution of the keys to the customer device. Again a CP will need to engage specific expertise to deploy the architecture, taking into account the latest recommendations for encryption and hashing algorithms.

8.2 Cryptographic Tunnelling Methods

There are three main ways to transport data securely across a network which may be applicable to All-IPT. These are discussed in the sections below.

8.2.1 Use of IPSec

One option is to use IPSec to encrypt all traffic profiles within the secure tunnel, with or without TLS for individual application layer protocols within the tunnel. However, this depends greatly on the overall solution architecture for the voice and IP network within the CP.

Additional information can be found in 3GPP TS 33.210 and TS 33.310 (See normative references [7][8])

8.2.2 Use of TLS

Another option is to use TLS on a per application basis and the following interface types will be individually secured;

1. O&M interfaces between CPE and ITSP
2. Voice signalling interfaces between CPE and ITSP telephony gateways

At the time of writing this ND, it is assumed that SIP URI would be used for SIP PDU while implementing TLS for securing the transport for SIP based telephony. However, use of the SIP Secure URI scheme could also be an option, though agreement should be made with the peer telephony nodes to ensure interoperability. Consideration should also be given to how the version of TLS should be kept up to date in the network.

Using versions recommended by NCSC is preferred.

8.2.3 Use of SRTP

If TLS is used for securing SIP signalling with the voice platform, then use of secure RTP may also be considered. The encryption keys for securing the RTP are negotiated during SDP offer/answer exchange using the SDES 'crypto' media attribute containing the mandatory crypto suite for authentication, encryption and integrity.

The use of SRTP is optional, however if implemented then it is recommended to secure the SIP signalling using TLS so that the SIP PDU containing the master key, session key and salt value for establishing secure RTP are not in plain text

Additional information can be found in 3GPP TS 33.210 and TS 33.310 (See normative references [7][8])

9 Generic Security Controls

9.1 Access Controls

Access to All-IPT for configuration, operation and maintenance shall

- a. Have processes and procedures to control and allocate access for use.
- b. Allow appropriate roles and capabilities to be clearly defined and managed.
- c. Maintain a documented detail of access list functions deployed.

Where appropriate use shall be made of two factor authentication.

9.2 Good Practice information and guides

The following references are designed by and sourced from the industry supporting the technology and devices in scope of this NICC Standard. They are based on current best knowledge and experience.

The references listed in this section were correct at the time of publication.

For any further information about the documents referred to in this section, please contact the relevant document owner.

Additional guidance can be found in ND1438. See normative reference [6]

9.2.1 Cyber Essentials Scheme

Cyber Essentials is a government Scheme which is supported by industry. It enables organisations of all sizes to be tested against a set of criteria to ensure they have good basic cyber hygiene in place. A description for the Scheme can be found here –

- Cyber Essentials Scheme: overview. See Informative reference [i6]
- Cyber Essentials self- help information. See Informative reference [i7]

9.2.2 NCSC 10 Steps to Cyber Security.

Guidance on how organisations can protect themselves in cyberspace, including the 10 steps to Cyber security can be found at the NCSC website. See Informative reference [i1]

9.2.3 Fraud Mitigation Documentation

The FCS has produced a standard for mitigating fraud. The FCS Fraud Mitigation Standards - See normative reference [n4]

The FCS also produces a Telephone Security Checklist – See normative reference [n5]

The Communications Crime Strategy Group, which sets the strategic crime agenda for the industry members it represents -

See informative reference [i8]

The UK's national fraud and cybercrime reporting centre

See informative reference [i9]

UK Cross-sector fraud sharing organisation

See informative reference [i10]

Association of Certified Fraud Examiners

See informative reference [i11]

9.3 Threat intelligence and Threat actor classification

Threat intelligence is a large and complex area that cannot be well described within the scope of this document and will differ depending on the type of organisation.

Simple definitions can be:

- Evidence-based interpretation of data, collected on or against the identities, goals, motives and targets of malicious actors;
- Information that provide relevant and sufficient understanding for mitigating a harmful event.
- The process of analysing data creating contextualised knowledge to mitigate a threat. A threat is an event potential to cause harm.

The maturity of being able to collect intelligence and build this into a threat model is still relatively immature in many technology areas. However, there are many threat intelligence sharing initiatives, one example being the Cyber Security Information Sharing Partnership (CiSP), a joint industry and government set up to exchange cyber threat information in real time in a secure, confidential and dynamic environment. See informative reference [i15]

The following highlights some basic threat terminology that is associated with IPT communications that can be used to reference out from to gain more detail. A recommended document is the Cyber Threat Intelligence Operations, from a CBEST Intelligence Led Testing. This document provides a comprehensive list of threat intelligence resources, underlining the amount of information available on this subject. See informative reference [i16].

Threat actor classification is important. Hacking is a multibillion-pound industry for cyber criminals for commercial or political gains.

Actors typically fall into one of the following camps:

- External – Cyber Criminal
- External – State Sponsored
- External – Hacktivist
- Internal – Sys Admin, User, Manager, Executive.
- Partner - Third Party

Threat actor attributes can be built up by intelligence over time and give an insight to potential threats to All-IPT as implemented by the owning CP.

These can include: -

- Relationship being Internal/external
- Geographic Operation

- Objective
- Motive
- Intent
- Typical industry target
- Tools and methods of attack
- Asset types typically targeted

Incidents will have at least one and usually more actions instigated by a threat actor. These typically fall into the following categories:

- Social Engineering- people hacking
- Misconfiguration – errors, malfunctions, omissions
- Hacking – unauthorised access
- Misuse – None approved actions
- Malware – Malicious scripts or code

Typical asset types being targeted

- Physical devices and locations
- Technical infrastructure
- Business applications
- Data / information
- People

9.4 Vulnerability Management

Vulnerability management assessment is essential in risk reduction. All devices **should** be subject to review and if vulnerabilities are found they **should** be recorded and prioritised for remediation. Suitable tools **should** be used to probe for vulnerabilities open ports, etc. These tools **should** be run in normal design/test validation or with periodic (including penetration) testing.

In life systems **should** be scanned to ensure compliance and highlight misconfiguration or the insertion of unauthorised code. This **should** be reviewed frequently, and controls put in place to mitigate risk whilst change management requests flow through to remediating the vulnerabilities with patching or new code releases.

Any vulnerabilities that are not able to be addressed in the short term **should** be signed off as a risk by the system/platform owner to ensure accountability for risk in the organisation is managed. This can sometimes be the result of suppliers not having been able to fix the code for technical or commercial reasons.

Note: It is important to validate that suppliers can adequately manage vulnerabilities. These suppliers should deliver security patches and software updates that align with timeframes within the organisation's vulnerability management processes. This can be problematic if not robustly managed.

9.5 Understand IPT assets

Every organisation **should** have an asset register, which is a fundamental enabler to protecting those assets. If assets are not known about, they cannot be monitored and protected.

Typical information recorded about an asset: -

- Asset ID
- Asset Description
- Ownership
- Location
- Categorisation (Low, Medium, High). Impact assessment against Confidentiality, Integrity and Availability (CIA).

Beyond this, there **should** also be a view on what assets are critical. It could be the case that some assets are shared between different platform solutions.

Having a robust inventory will ensure proactive measures are applied to all required assets and incident management will understand the assets they could respond to.

9.6 Business Impacts

The business impacts of cyber threat to All-IPT can be wide ranging from reputational damage through financial regulatory and legal impacts.

For financial impact typical areas of consideration would be: -

- Revenue loss resulting from down time.
- Staff required for post incident analysis.
- Infrastructure damage and the cost to implement new controls.
- Regulatory fines.
- Legal costs.
- Compensation costs.
- Loss of customer base.

Business impacts are typically indicated by threat modelling, this maps out the typical threats, the likelihood and impact based on previous experience or industry indicators.

9.7 Controls and organisational structure

Given the potential impact there is a compelling case for security to be embedded in all product development and design activities right through to deployment and in life operations.

9.7.1 Typical controls

Controls are used to mitigate impact of damaging system and network attacks. These controls are reviewed and tailored over time where their effectiveness can be assessed providing heightened maturity.

Some typical controls are shown below: -

- Hardware asset register.
- Software asset register.
- Hardening policies.
- Malware protection.
- Vulnerability assessments.

- Secure software development.
- Red Team exercises.
- Vendor conformance quality gates.
- Design test and conformance quality gates.
- Incident management.
- Business Continuity plans.
- Data Protection (Privacy by Design).
- User assess management.
- Proactive monitoring tools.
- Perimeter defences.
- Configuration management and validation.
- Data backup and recovery.
- Malware defences.
- Training and awareness.

9.7.2 Security Event Management

Often abbreviated to SIEM or Security Information and Event management. It usually integrates several technologies together to provide a holistic security view of the Platform. Examples of these could be events, alarms or logs generated from equipment as well as validation of correct configuration and live vulnerability scans. The aim of the event management is to provide centralised security event management where the alerting and other inputs are correlated. This allows operational teams to gain a dashboard view often in real time to make informed decisions and take corrective actions when appropriate. This helps to address managing a multitude of different technologies being bolted together that make up a service.

9.7.3 Change Control

The ability to assess the impact of changes and revision control to the platform is paramount. Often changes will need to be tested in a model environment to confirm compliance and maturity. It is also important that changes are fully understood and recorded, particularly when configuration changes are made.

Typical change control areas are: -

- New Hardware.
- New Software.
- New features.
- Capacity upgrades.
- Patching.
- Hardening.
- Reconfiguration.

Making sure that the platform can maintain control of all changes and these are, documented and approved will reduce risk. A change management process allows this to be done formally.

9.7.4 Root Cause Analysis

It is important to look at the cause of an event rather than just the symptoms. In a busy Operational environment this may not always be easy to achieve but it should be the objective rather than a

short-term fix. More often this requires reaching out to other experts be that in the design and development space or the supplier. Organisations are likely to have a test environment where they can attempt to recreate a failure scenario. This can sometimes be time consuming and resource hungry but that needs to be balanced against the potential impact of another failure and the risk associated with that failure.

9.8 Response and Escalation

Security and business departments **should** be able to coordinate efforts and have a Security Response Plan (SRP) providing a methodical approach.

A good resource is NIS guidance collection on the EU directive on the security of Networks and Information Systems (known as the NIS Directive).

Around managing cyber security incidents and oversee the application of the Directive. This includes a National Cyber Security Strategy, a Computer Security Incident Response Team (CSIRT), and a national NIS competent authority, or competent authorities.

See Informative reference [i2].

9.9 Security Operations Centre SOC

The Security Operations Centre (SOC)

Key aims as taken from the NCSC website: -

- To detect and respond to threats, keeping the information held on systems and networks secure
- To increase resilience by learning about the changing threat landscape (both malicious and non-malicious, internal and external)
- To identify and address negligent or criminal behaviours
- To derive business intelligence about user behaviours in order to shape and prioritise the development of technologies.
- Depending on the nature of an organisation the choice is either to resource a SOC internally or reach out to a third party to implement the use as well as improvements to the security capabilities as the Platform evolves.
- There would also be the opportunity to raise defects that could be reviewed tracked and updated and aligned with findings raised within the test phases which could be reviewed periodically.

Change management plays a pivotal role on maintaining the integrity of the live Platform and robustly policing updates and the associated impacts throughout the Platform life.

When products are retired as end of sale, there **should** be contractual agreement between the organisation and the suppliers to ensure that high risk vulnerabilities can still be remediated and at what point this will no longer be possible. This is crucial to ensure that the Platform assurance levels are maintained and allows the Platform owners to plan for new technology to intercept key milestones.

9.10 Privacy

As taken from the Information Commissioners Office (ICO).

Privacy by Design is an approach to projects that promotes privacy and data protection compliance from the start. Unfortunately, these issues are often bolted on as an after-thought or ignored altogether.

Privacy by Design is and by Default is a requirement of the General Data Protection Regulation and for high risk processing the ICO requires that a Privacy Impact Assessment is conducted. In certain circumstances if the data is particularly sensitive or high risk there may be a requirement to go to the Regulator in advance to discuss the purposes for processing. The ICO encourages organisations to ensure that privacy and data protection is a key consideration in the early stages of any project, and the throughout its lifecycle.

Taking a privacy by design approach is an essential tool in minimising privacy risks and building trust. Designing projects, processes, products or systems with privacy in mind at the outset can lead to significant benefits.

More detail on Privacy by Design can be obtained from the Information Commissioners Office. See Informative reference [i4].

In general terms the GDPR requires an organisation to do the following;

- Process personal information fairly and in accordance with applicable laws;
- Tell people (either directly or in our policies or notices) about how we will use their personal information;
- Only collect personal information when we need it for legitimate purposes, or legal reasons;
- Ensure that personal information is adequate, relevant and limited to what is necessary for the purpose for which we collect it;
- Kept accurate and up to date;
- Not keep personal information for longer than we need to;
- Keep personal information secure, and limit the people who can access it;
- Ensure that people know how to access their personal information and exercise their rights in relation to it;
- Ensure that any third parties we share personal information with take appropriate steps to protect it;
- Help our business customers to comply with any legal obligations they have in connection with any personal information that we process on their behalf.

More detail on Privacy by Design can be obtained from the Information Commissioners Office. See Informative reference [i5].

More information on Data protection including detail on conducting Data Protection Impact Assessments can be obtained from the Information Commissioners Office

History

Document history		
Version	Date	Status
1.1.1	27 th June 2019	Initial Version Published
2.1.1	22 nd June 2022	Second publication