OPEN BANKING

Participant Guide: Information security operations

A guide to implementing effective information security controls

Date: January 2018
Version: v1.0
Classification: PUBLIC

Contents

1 Introduction

Open Banking enables enrolled Account Servicing Payment Service Providers (known as ASPSPs) including banks and building societies, to allow their personal and small business customers to share their account data securely with Third Party Providers (known as TPPs). This enables those third parties to provide customers with services related to account information such as product comparison or payment initiation using the account and product information made available to them.

This is achieved by the development, maintenance and publication of standards for Application Programming Interfaces (APIs). APIs are an established technology that use defined methods of communication between various software components; they are used by many well-known online brands to share information for a variety of purposes.

March 2017 saw the introduction of the first Open Banking standards for APIs to support access to defined elements of Open Data, as defined in the CMA Order; specifically information on ATM and Branch locations, and product information for Personal Current Accounts, Business Current Accounts (for SMEs), and SME Unsecured Lending, including Commercial Credit Cards.

As required by the CMA Order, this was followed in July 2017 by the release of further API standards for Read/Write Data. These additional Read/Write API standards enable third party providers, with the end customer’s consent, to request account information such as the transaction history of Personal and Business Current Accounts and/or initiate payments from those accounts.

Following the 2017 Budget announcement, a programme of releases to build on the core requirements of the CMA Order will be implemented throughout 2018 and into 2019.

Implementation of information security controls must be in line with the Open Banking Read/Write API specifications - particularly the Open Banking Security Profile. These specifications detail the underlying information exchanges between Participants and how these are secured, but do not define the way each Participant can operate securely to meet their specific needs. This document should be read in conjunction with other Open Banking 'How To' guides.

This document serves purely as a guide to information security operations and does not constitute legal or regulatory advice. All Participants are responsible for their compliance with the relevant regulations applicable to their service offering and are encouraged to seek external legal advice.

2 Information Security

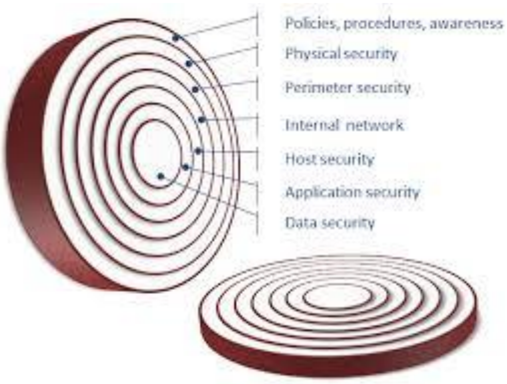
Information Security protects the confidentiality, integrity and availability of information through the application of physical, administrative and technical controls to manage and mitigate risks to acceptable levels. There are many sources of advice about information security and how to implement effective controls that are proportionate to the size and scale of your business and the products or services you provide. To protect the confidentiality, integrity and availability of information and data in the Open Banking Ecosystem, all Participants should ensure that security is given sufficient profile and influence in their organisation. This good practice guide is designed to provide Participants with the Open Banking Implementation Entity view on how this can be achieved. For a good overview, have a look at the BSI website and the IASME website.

The document consists of 4 sections:

- Top Tips
- Information security
- Security operations
- Cybersecurity

Implementation of Information Security controls must be in line with the Open Banking Read/Write API specifications - particularly the Open Banking Security Profile. These specifications detail the underlying information exchanges between Participants and how these are secured, but not the way each Participant can operate securely. This document should be read in conjunction with other Open Banking 'How To' guides and the Open Banking security profile.

An effective approach to information security layers multiple defences to protect the confidentiality, integrity and availability of data and information.



3 Top Tips

3.1 Effectively manage information security

- Use specialist resource and an appropriate controls framework - ISO27001:2013), IASME, CyberEssentials - externally assessed rather than self-assessment
- Complete regular threat assessments and ongoing risk management using experienced staff and robust processes (risk management standards)
- Allocate accountability to a nominated board member to oversee risks
- Implement strong passwords and access management controls
- Review and refine threats and mitigating actions regularly
- Vet all staff - internal threat from malicious or accidental activity is often the biggest risk to an organisation
- Develop a strong security awareness culture within your organisation
- Implement and run a dedicated security operations centre
- Ensure strong IT systems controls - access and role management etc. covering infrastructure, applications through software development lifecycle
- Ensure clear information security requirements are stated in contracts with third party suppliers
- Regularly undertake assurance of third party providers
- Assume you will have a problem - create and test an incident response plan

3.2 Protect against a data breach

- Implement strong password and access controls - and ensure secret credentials remain secret at all times
- Classify data - understand what data you hold, assess the sensitivity and protect according to the threat likelihood and impact
- Manage access to data - use strong authentication to manage access to company systems and role based access for individual data sets. Review access at least quarterly
- Train staff - over and over again. Training should cover risks (particularly phishing and social engineering), web use, proper data handling and data management processes

- Foster a culture of security - prioritise security over functionality - a bit of friction is a good thing

- Eliminate the use of portable storage, install Mobile Device Management software on mobile devices and restrict the ability to download and store data etc.

- Assess new applications, processes or services from a security perspective before introducing them

- Production data used in non-production environment must have production level controls implemented

- Emergency access to production data needs to be made through a secure break-glass process

- Have a clear data retention and destruction policy

3.3 Technical security

- Enforce continuous patching, including documenting and archive dates to all technology and have individual accountability for patching specific software and equipment

- Maintain firewalls, vulnerability scanning, patching, Denial of Service (DoS) and Distributed Denial of Service (DDoS) protection

- Implement regular vulnerability scanning - scan your networks and endpoints for vulnerabilities and weaknesses

- Harden your operating systems - take simple steps such as changing default passwords, delete unnecessary service accounts, remove unused or superfluous software

- Secure provision of experienced external penetration testing services

- Where authentication is handed off or redirected to other sites, ensure credentials cannot be intercepted and avoid the need for disclosure

- Always maintain the ability of the user to verify the authenticity of the site they are entering - i.e. maintain the ability to see the url bar/lock icon

- Manage and implement session timeout values to ensure users cannot leave transactions 'hanging' that could then be intercepted

4 Information Security

4.1 Organisational risk

Successful information security controls are essential to effective management of organisational risk. The risks faced by any organisation are varied, but the most common for Participants are:

- Loss of customer trust and take-up of services
- Information Commissioner's Office (ICO) monetary penalties and censure for data breaches
- Competent Authority (CA) revocation of regulatory status
- Friction in customer experience as additional security checks are imposed on transactions
- Reputational damage

Having a defined approach to information security, underpinned by a strong controls framework will enable Participants to manage and mitigate risks to their businesses and customers more effectively.

4.2 Approach to take

- Identify threats - for Open Banking transactions, data loss or financial loss
- Split into threat vectors, actors and surfaces
- Use a defined methodology to assess threats and define as risks
    - Common Criteria
    - ISO27001:2013
- Assess risk to the organisation
- Likelihood vs. impact
    - Proximity (timing)
    - ISO27005:2011
    - ISO31000:2009

- Identify optimal control mechanisms
    - Mitigate
    - Accept
    - Reduce
- Review regularly - at least annually, but more often in a fast moving, technology based environment such as Open Banking
- Allocate response actions to People, Process, Technology

4.3 People

People are a company's biggest asset, but also their biggest threat. All research indicates that the 'insider threat' (which can be malicious or accidental) poses the biggest risk to an organisation. Robust people controls are therefore essential to managing information securely.

- Strong Vetting
- Strong initial security training
- Continual education & awareness
- Clear accountability

4.4 Policy

- Define key policies - data handling & classification, acceptable use, whistleblowing, vetting of staff, incident management and crisis response, access management (policy, good practice re passwords, MFA etc)
- Governance - Information Security Management Forums, Enterprise Risk Committees
- Policy compliance monitoring and control maturity reviews
- Policy assurance reviews, including third parties
- Data handling guidelines - tie into relevant data protection laws

4.5 Technology

- Security incident & event management solution - Gartner and Forrester Research Ltd have assessed different vendors providing SIEM solutions
- Security operations centre

- Identity and access management policies, processes and technologies
- Industry trusted perimeter security technologies
- Understand your technologies threats and vulnerabilities
- Strong configuration and patch management

Where to go for more information

- Information Commissioners Office
- Financial Conduct Authority
- Get Safe Online
- European Banking Authority
- Gartner SIEM review
- Forrester Research Ltd Security Operations

5 Security Operations

Security operations relates to the security of information systems in a live production environment. All users interact with information assets and have a responsibility to ensure the security of those assets. This also applies to the operational teams that run and maintain the systems, equipment, applications and databases that are so critical to the effective operation of the business and the protection of customer data.

While other parts of this guide cover good practice in terms of security controls that need to be considered during the design and build process, security operations classically include activities such as security monitoring, incident response and management, and situational awareness. The function of security operations is to protect assets, detect threats and respond to issues.

Operating procedures and responsibility for information systems (information assets) should be authorised, documented and maintained. It is crucial that organisations understand the information assets that their business holds, have identified relevant information owners and system owners, and have in place operational security measures to protect systems and data. The National Archives have put together some helpful guidance on understanding the information an organisation holds and how to ensure digital continuity.

All organisations should identify information assets and carry out information security risk assessments from a thematic perspective. Information assets should then be protected through good practice security operations in terms of the following:

- Personnel
- Physical
- Procedural
- Technical

5.1 Personnel Security

As already highlighted ‘people are an organisation’s biggest asset’ but they can also pose a significant insider risk. The National Crime Agency in their 2017 National Strategic Assessment of Serious and Organised Crime report[1] highlights corrupt professionals as a common enabler to eCrime. Cyber criminals continue to exploit vulnerabilities in human behaviour and smaller organisations with less mature security strategies and operational capability are likely to be more vulnerable.

Effective personnel security requires the integration of policies and procedures that seek to mitigate the risk of workers (insiders) exploiting their legitimate access to information assets for unauthorised nefarious purposes. In this context, the Centre for the Protection of National Infrastructure (CPNI)[2] has published good advice on its approach to personnel security that focuses on three main strands of activity:

- The reduction of insider risk:
  - Reduce the risk of recruiting workers who are likely to present a security concern
  - Minimise the likelihood of existing workers becoming a security concern
  - Reduce the risk of insider activity
  - Implement security measures in a way that is proportionate to the risk
- Optimisation of the capability of the organisation’s security team:

[1] http://www.nationalcrimeagency.gov.uk/publications/807-national-strategic-assessment-of-serious-and-organised-crime-2017/file
[2] https://www.cpni.gov.uk/personnel-and-people-security

    - Identify the target security behaviours required from the workforce
    - Develop a security savvy mind-set and culture in the organisation
    - Embed security behaviour change
    - Develop and maintain a professional security posture
- Disruption and mitigation of the external people threat:
    - Deny hostile outsiders the opportunity to gain valuable and exploitable information
    - Detect reconnaissance activities
    - Deter the threat through messaging and physical demonstration of effective security

In the context of personnel security, it is also important to consider the following factors:

- Effective access controls including role based access control
- Separation of duties: operational responsibilities versus administration rights, and who has access to production environments

In agile environments this is known as DevSecOps (Development Security Operations) and the mindset established by DevSecOps fosters an environment that enables business operations to be supplied with tools and processes that help embed good security design and development practices. Appropriate controls, logging and analysis of access to systems and data can highlight areas for concern and further action.

5.2 Physical Security

Physical Security is not just an important facet of information security, it helps safeguard the business and mitigates risks associated with unauthorised access such as theft, vandalism, physical attack, arson etc.

Small organisations are often responsible for their own office security and it is good practice to assess premises to ensure that there is a commensurate level of security to protect both customer data and the critical information assets that are essential to business operations.

Organisations should consider a three-pillar approach to assure they have appropriate physical security measures to ensure a safe and secure working environment for their personnel and that they can adequately protect against a wide range of threats.

- A risk assessment to determine the appropriate physical security requirements
- Mechanisms in place to implement internal and external security controls in a layered fashion that deter or prevent unauthorised access and protect assets, especially those that are critical or sensitive, against forcible or surreptitious attack.
- Appropriate access control to both the day-to-day workplace to reduce the risk of break-in and to restricted environments such as server rooms, network rooms and facilities such as a security operations centre (SOC), which must be kept physically secure.

In addition, simple precautions such as locking filing cabinets and storage areas when not in use can be effective deterrents to theft of documentation, records and physical assets. More advanced protection should also be given to the control and storage of highly sensitive material such as cryptographic material.

Where to go for more information

- Financial Conduct Authority
- Centre for the Protection of National Infrastructure
- ISO/IEC 27001:2013

5.3 Procedural Security

Procedural security is about having good policies in place along with supporting procedures and monitoring. This includes regular auditing and monitoring of procedures and policies. They mitigate identified risks with controls that rely on users following a set of rules or performing certain activities that are not necessarily enforced by technical or physical means.

The implementation of a robust Information security management system aligned to ISO 27001:2013 is an excellent starting place for procedural security. It implements a controls based procedural approach designed to identify and mitigate risks using specific controls that are defined, tested and recorded. These can be audited to ensure the risks and consequent impact of any breach/compromise can be brought within the organisation’s risk appetite.

Implementation of information classification and handling policies enables an organisation to more readily identify information that is sensitive and needs specific protection.

Changes to system environments including the provisioning and de-provisioning of assets, promotion of code, configuration changes and changes to standard operating procedures should be controlled and authorised through an appropriate operational governance mechanism, such as a change advisory board (CAB).

The routine application of security procedures also enables good security practices to become ingrained within the organisation and applied in a consistent way.

Where to go for more information

- National Cyber Security Centre – Risk Management Principles
- Financial Stability Board

6 Technical Security

6.1 Secure Development and Deployment

The NCSC has published guidance to improve and evaluate development practices. It comprises ‘8 Principles of Secure Development & Deployment’ as follows:

- Secure development is everyone’s concern
- Keep your security knowledge sharp
- Produce clean and maintainable code
- Secure your development environment
- Protect your code repository
- Secure the build and deployment pipeline
- Continually test your security
- Plan for security flaws

6.2 Security Measures

Technical security measures also include:

- System monitoring and logging
- Change management

- Intrusion detection, prevention and incident management
- Virus and malicious software defence
- Segregation of duties and environments (including techniques such as role based access control)
- Capacity planning and load testing
- Cryptographic controls
- Rigorous penetration testing

Actively monitoring the threat environment and regular checks on the effectiveness of the organisation's current security controls improves technical security posture. It is also beneficial to review both free and paid for sources of threat information.

The Open Web Application Security Project (OWASP) is an online community that produces freely-available articles, methodologies, documentation, tools, and technologies in the field of web application security. The OWASP Top Ten Application Security Risks identified for 2017 are:

- Injection
- Broken authentication
- Sensitive data exposure
- XML external entities
- Broken access controls
- Security misconfiguration
- Cross-site scripting (XSS)
- Insecure deserialisation
- Components with known vulnerabilities
- Insufficient logging & monitoring

7 Security operations centre

Organisations should also consider the benefit of implementing a security operations centre (SOC) to provide situational awareness on the effectiveness of its technical security defences.

A SOC in the context of information security is a facility where enterprise information systems (web sites, applications, databases, servers, networks, desktops and other endpoints) are monitored, assessed and defended[3].

The key aims of a SOC are:

- 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 to shape and prioritise the development of technologies

An organisation that is considering the benefits of acquiring a SOC from a third party should also consider how to exploit security information and event management. Organisations should also consider the requirement for trained SOC analysts who can use scripts, correlate logs and develop the rulesets needed to maximise the benefits of a SOC.

The NCSC has published a useful SOC buyers guide.

Where to go for more information

- NCSC Advice and Guidance on Operational Security
- US Department of Defense Education Activity
- EBA Guidelines on the security measures for operational and security risks of payments services under Directive (EU) 2015/2366 (PSD2)
- OWASP

8 Cybersecurity

All organisations should take steps to protect their business against online threats. The number of successful high-profile attacks and data breaches are indicative of security

[3] https://en.wikipedia.org/wiki/Information_security_operations_center

weaknesses and the task of delivering effective cybersecurity is made increasingly more difficult as threats evolve.

In the National Crime Agency National Strategic Assessment of Serious and Organised Crime 2017, the NCA Director General, Lynne Owens, stated:

> *'We have seen the rise of off-the-shelf cybercrime products which have resulted in less technically proficient offenders being able to commit large scale, high impact offences. Likewise, the professional enabling of major economic crime and money laundering allows this type of offending to take place at scale'.*

The report goes on to state:

- There are indications that the threat to the UK from cybercrime is increasingly global
- Under-reporting of cybercrime continues to obscure understanding of its true scale and cost
- The most competent cybercrime actors are moving towards targeting businesses and payment systems drawn by the prospect of greater financial rewards
- Cyber criminals still benefit from the exploitation of basic security vulnerabilities and human vulnerabilities through social engineering
- Ransomware attacks are increasingly prevalent
- The ready availability of as-a-service toolkits has further lowered the barrier to entry for committing cybercrime

8.1 Ten steps to Cybersecurity

The UK Government published guidance on 10 Steps to Cybersecurity in which it highlighted why protecting information is a board-level responsibility. The 10 Steps are as follows:

1. *Risk Management Regime:* Embed an appropriate risk management regime across the organisation

2. *Secure Configuration:* Having an approach to identify baseline technology builds and processes for ensuring configuration management can greatly improve the security of systems

3. *Network Security:* The connections from your networks to the internet, and other partner networks, expose systems and technologies to attack

4. *Manage User Privileges:* If users are provided with unnecessary system privileges or data access rights, then the impact of misuse or compromise of that users account will be more severe than it need be

5. *User Education & Awareness:* Users have a critical role to play in their organisation's security and so it's important that security rules and the technology provided enable users to do their job as well as help keep the organisation secure

6. *Incident Management:* All organisations will experience security incidents at some point

7. *Malware Prevention:* Malicious software, or malware is an umbrella term to cover any code or content that could have a malicious, undesirable impact on systems

8. *Monitoring:* System monitoring provides a capability that aims to detect actual or attempted attacks on systems and business services

9. *Removable Media Control:* Removable media provide a common route for the introduction of malware and the accidental or deliberate export of sensitive data

10. *Home and Mobile Working:* Mobile working and remote system access offers great benefits, but exposes new risks that need to be managed

8.2 Cyber Threats

In the NCSC's report 'The cyber threat to UK business 2016/2017 Report', the CEO of the NCSC, (Ciaran Martin) stated:

> *Cyber attacks will continue to evolve, which is why the public and private sectors must continue to work at pace to deliver real-world outcomes and ground-breaking innovation to reduce the threat to critical services and to deter would-be attackers.*

The report goes on to highlight that:

> *Cyber criminals seek to exploit UK organisations and infrastructure for profit. Their technical sophistication varies from small scale cyber-enabled fraud to persistent, advanced and professional organisations. They may directly steal money or monetise their capabilities indirectly through intellectual property theft, through extortion (issuing ransom demands following denial of service or data theft), or through malware*

The current Cyber threat trends are underpinned by three key features:

- technical expertise is not necessary to carry out attacks
- a broadening attack surface leads to more opportunities for attackers
- threat actors are learning from, and using one another’s skills and capabilities

And there is evidence that:

- Cyber extortion has increased with cybercrime becoming more aggressive and confrontational
- Computer misuse offences and cyber-related fraud are a more prominent threat than traditional crime types
- Ransomware remains the most common cyber extortion method
- There has been a rise of ‘botnets’ exploiting security flaws in internet-connected devices
- Easy access to offensive cyber capabilities, such as ransomware or DDoS, has allowed individuals and groups to have an impact disproportionate to their technical skill
- Financial trojans have become more targeted and less visible
- Sophisticated actors don’t need to be sophisticated
- While the mobile threat is low, it is growing. Malicious apps are increasingly requesting elevated permissions. Furthermore, fake apps mimic a brand or organisation to trick users into downloading them and entering credentials which are then stolen
- SMS phishing ‘smishing’ is often now more effective than traditional PC phishing
- Social media has become an attack vector

Patching remains a very powerful tool to counter cyber threats. The most commonly exploited vulnerabilities in 2016/2017 were well known and failing to patch legacy systems leaves organisations unnecessarily vulnerable.

Organisations should also be on their guard for attacks that tamper with, rather than steal or deny access to data. An attack on the integrity of data is particularly dangerous as the victim is not aware the changes have been made. Using an integrity attack can create virtual private network (VPN) backdoors and significantly weaken security.

8.3 Cyber Hygiene

Cyber hygiene is of critical importance as ASPSPs and TPPs deliver new Open Banking account information and payment initiation services.

There are many schemes and certifications that can help organisations improve their Cyber hygiene stance such as:

- *Cyber Essentials:* Cyber Essentials is a simple but effective, government backed scheme that will help you to protect your organisation, whatever its size, against a range of the most common cyber-attacks. Cyber-attacks come in many shapes and sizes, but the majority are very basic in nature, carried out by relatively unskilled individuals. They are the digital equivalent of a thief trying your front door to see if it's unlocked. Our advice is designed to prevent these attacks.

- *IASME:* IASME is an information assurance standard managed by The IASME Consortium that is particularly suitable for Small to Medium Enterprises (SMEs). It was originally developed as an academic-SME partnership and has attracting interest among decision-makers within the UK small business community. IASME controls are aligned with the Cyber Essentials scheme and certification to the IASME standard usually includes certification to Cyber Essentials.

- *ISO 27032:2012:* ISO/IEC 27032:2012 provides guidance for improving the state of cybersecurity, drawing out the unique aspects of that activity and its dependencies on other security domains, in particular:

  - information security;
  - network security;
  - internet security; and
  - critical information infrastructure protection (CIIP)

ISO 27032:2012 covers the baseline security practices for stakeholders in cyberspace. This International Standard provides:

- an overview of cybersecurity;
- an explanation of the relationship between cybersecurity and other types of security;
- a definition of stakeholders and a description of their roles in cybersecurity,
- guidance for addressing common cybersecurity issues; and
- a framework to enable stakeholders to collaborate on resolving cybersecurity issues

8.4 Cyber Information Sharing Partnership

CiSP[4] is a joint industry and government initiative set up to exchange cyber threat information in real time, in a secure, confidential and dynamic environment. This increases situational awareness and reduces the impact of cybercrime on UK business.

There is an Open Banking Node on CiSP designed to enable ASPSPs and TPPs to share cyber and fraud related information either with other Open Banking Participants or on a one-to-one basis with other specific Open Banking Node members.

Participants who wish to become members of the CiSP should sign up through the NCSC web site and, once a CiSP member, request membership of the Open Banking Node.

Where to go for more information

- NCSC '10 Steps to Cyber Security'
- European Commission Digital Single Market Policies - Cybersecurity
- Cyber Essentials
- IASME
- ISO 27032:2012
- CiSP
- FCA Approach to Cyber Security

[4] The NCSC Cyber Information Sharing Partnership (CiSP) https://www.ncsc.gov.uk/cisp

Definition of Terms

Information Security

Information Security is the practice of preventing unauthorized access, use, disclosure, disruption, modification, inspection, recording or destruction of information

2FA/MFA

Two-factor authentication (2FA) and multi-factor authentication (MFA) are methods of computer access control in which the user is granted access only after successfully presenting several separate pieces of evidence – typically something they know, something they have and something they are

Information Security Management Forum

A management group that operates and is responsible for the organisation's Information Security Management System

Enterprise Risk Management

Enterprise Risk Management or 'ERM' in a business includes the methods and processes used by the organisation to manage risks and seize opportunities

Enterprise Risk Management Committee

The ERM Committee is the leadership group responsible for operating the organisation's risk management processes to achieve its business objectives

Virtual Private Network

A Virtual Private Network or 'VPN' is a technology that creates a safe and encrypted connection over a less secure network, such as the internet.

Glossary of Terms

For further information on the terms used within this document please refer to the Glossary on the Open Banking website at www.openbanking.org.uk.

Abbreviation of Terms

Term	Definition
API	Application Programming Interface
ASPSP	Account Servicing Payment Service Provider
CAB	Change Advisory Board
CIIP	Critical Information Inrastructure Protection
CiSP	Cyber Information Sharing Partnership
CMA	Competition Market Authority
CPNI	Centre for the Protection of National Infrastructure
Common Criteria	Common Criteria for Information Technology Security Evaluation
DDoS	Distributed Denial of Service
DevSecOps	Development Security Operations
DoS	Denial of Service
FCA	Financial Conduct Authority
IASME	Information Assurance for Small to Medium Enterprises
ICO	Information Commissioner's Office
MDM	Mobile Device Management
NCA	National Crime Agency
NCSC	National Cyber Security Centre
SIEM	Security Information & Event Management
SME	Small to Medium Enterprise
SMS	Short Message Service - telephony
SOC	Security Operations Centre
TPP	Third Party Provider
VPN	Virtual Private Network