IMS Insurance & Mobility Solutions

Technical & Operational Measures (TOM)

Reducing Risk & Enabling the Future

9th February 2022

TABLE OF CONTENTS

TECHNICAL & ORGANISATIONAL MEASURES

This document describes the technical and organisational measures (TOM) implemented by IMS ("the Group") to meet legal and contractual requirements when processing personal data.

The measures described herein serve the purpose.

- to encrypt or pseudonymise personal data where necessary
- to ensure the confidentiality, integrity, availability (CIA) and resilience of products and services in connection with the processing of personal data
- to restore the availability of and access to personal data in the event of a physical or technical incident in a defined time frame
- to regularly review, assess and evaluate the effectiveness of all technical and organisational measures to ensure the security of processing data

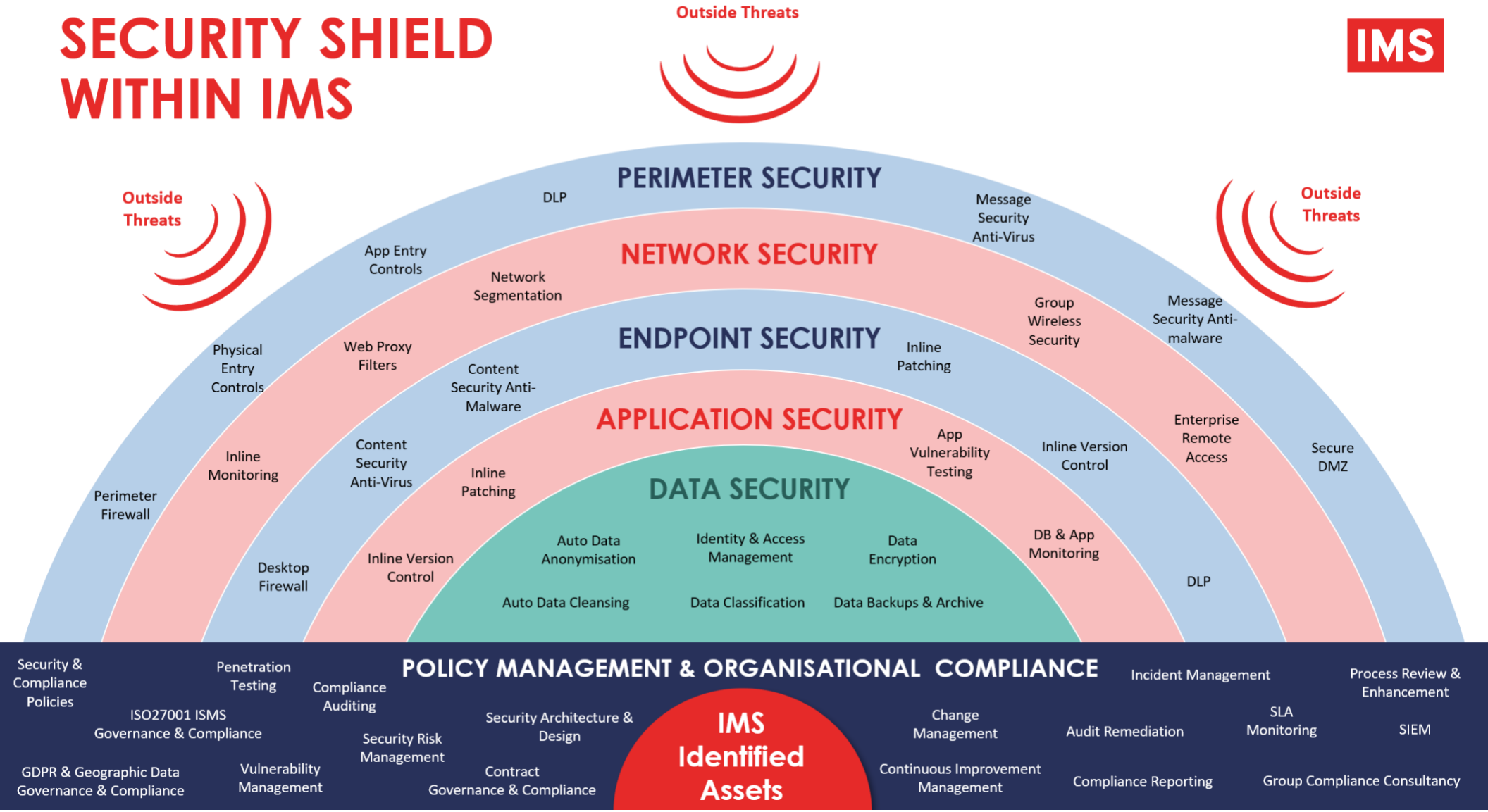
The following measures apply to all data processing activities under the Group's control, or where the Group is a data processor on behalf of another data controller.

In situations where the Group is the data controller and another organisation is the data processor on behalf of the Group, the Group aims at ensuring that the technical and organisational measures implemented by the processor equal, at minimum, the security level indicated by the following measures.

Please note: In federated service delivery scenarios, one or more data controllers and one or more data processors may be entrusted with or involved in processing personal data.

TOM MODELLING

When enduring the protection of Group and Client data it would be irresponsible to rely on just one single security method. Therefore, the Group has adopted the 'defence in depth' or security onion model to build a shield of defensive layers that support each other. If one fails, the next layer is in place to defend the data set, and so on. This approach is considered a modern standard for securing data's CIA. Figure 1 depicts the Group's layered approach to security:



TECHNICAL MEASURES

A range of technical measures have been designed and deployed throughout the Group. These are defined as the measures and controls afforded to systems and any technological aspect of the Group, such as devices, networks, software, and hardware. Protecting such aspects is crucial for the security of personal data and is the best line of defence against data breaches.

Technical Measures for Perimeter Security

Perimeter Firewall

IMS processes data in and between UK/EEA and Canada using on premises, data center (DC) and cloud platforms. This forms the IT environment which hosts all products and services taken by IMS clients. Across the environment, IMS has deployed and maintained a range of firewall appliances and applications which monitor all outbound and inbound traffic. Using defined protection policies and alerts, the Group can closely monitor the traffic.

Physical/App Entry Controls

Physical access to IMS offices is protected by physical controls such as key locked and/or fob access-controlled entry and exit points. Internal rooms and facilities are also similarly protected.

Employee access is controlled with a third-party door access control application. Fob/ID cards are configured and issued to facilitate access to the offices and restricted spaces within the communal areas. Visitor access is also controlled with a third-party application that maintains a visitor's log.

DC Access is managed as part of a third-party. However, due diligence is conducted on the third-party to ensure physical access controls are in place.

This approach is audited and improved in line with ISO27001 ISMS controls (Annex A) A.11.1 and A11.2 and is in line with the contract agreement between IMS and the third-party.

Data Loss Prevention (DLP)

DLP is in place within the Groups network. Several third-party applications detect, protect, and respond to inbound and outbound data traffic. Monitoring is effective within the application to allow for auto alerts to unexpected traffic, meaning the support team respond to exceptions only. The applications also have a range of protect and respond capabilities that remove the suspected data from leaving the Group's network via a range of routes.

Encryption is also applied to all IMS data that is in transit and at rest. Encryption is applied where possible using native tools.

This approach is audited and improved in line with ISO27001 ISMS controls (Annex A) A.13.1.2, A.13.1.3

Message Security Anti-Virus & Anti-Malware

Messaging services that pass through the perimeter are monitored for potential viruses and malware. Several third-party applications are in place to detect, protect and respond to malicious actors. The applications can alert, quarantine, and remove potential threats at the perimeter without human interaction. However, the support staff can view and respond to the alerts for further investigation.

This approach is audited and improved in line with ISO27001 ISMS controls (Annex A) A.12.2.

Secure Demilitarized Zone

A Demilitarized Zone (DMZ) network is in place which adds to the perimeter layer of security to the Group's internal local-area network from untrusted traffic. Within this DMZ is a subnetwork that sits between the public internet and private networks. This DMZ allows the Group to access untrusted networks, such as the internet while ensuring its private network or Local Area Network (LAN) remains secure. Servers and resources that reside in the DMZ are isolated and given limited access to the LAN to ensure they can be accessed via the internet, but the internal LAN cannot. As a result, a DMZ approach makes it more difficult for a hacker to gain direct access to an organization's data and internal servers via the internet.

Technical Measures for Network Security

Monitoring

Network monitoring software is in place across the environment. IMS has installed a range of tools that are configured to monitor for potential security risks and performance issues. Various operational support teams within the business are alerted to exceptions by the monitoring tools. These exceptions are investigated, and remediation is carried out where required. Reports are also utilised from the tools to support the business's decisions regarding issue trends and preventative action planning.

This approach is audited and improved in line with ISO27001 ISMS clause 9.1, 10.2

Web Filtering

Inbound and outbound internet traffic is monitored and restricted to all IMS assets that can access a web browser. Typical sites are blocked such as pornography, gambling or any that can be harmful to the business or its employees. Website allow/disallow policies are reviewed and updated when appropriate by approved support staff.

Network Segmentation

The Architecture team within IMS have designed a segmented network that is maintained by the IT Infrastructure team. The network is segmented at a virtual local area network (VLAN) and by type. IMS operate a range of products and services that are hosted from different cloud hosting solutions and Data Centre traditional hardware. These environments are segregated to manage live, production, test, user acceptance testing (UAT) data, etc.

This approach is audited and improved in line with ISO27001 ISMS controls (Annex A) A.13.1.3

Wireless Security

Included within the environment is the ability to connect to the IMS network via a wireless connection. In each of the IMS locations, wireless connection is approved for approved devices only. Both the asset and the user must hold approved accounts to access IMS hosted products and services that are hosted from the corporate network.

Additional access is provided to visitors (guest network), this is segregated and allows access to the internet only. Access to the guest network is password protected and by request only. Passwords to the guest network are changed periodically to control access.

Enterprise Access Control

IMS have an agile working model to support the employees from working remotely from the office. As part of the security controls managing remote access a Virtual Private Network (VPN) has been deployed to all end-user devices (EUD) used to process client data. The VPN connection is only issued to those employees who require access to applications that reside behind the business network. VPN user accounts are user-specific, and password controlled. Multi-factor authentication is used to access enterprise applications where appropriate.

Technical Measures for Endpoint Security

Firewall

All EUD's used to process client data have a local firewall configured and enabled. The EUD is using the native firewall for additional layered protection against malicious activity. The firewall is maintained and monitored by a range of IMS support staff.

Content Anti-Virus & Anti-Malware

A market leading Anti-Virus (AV) and Anti-Malware application is installed onto all IMS assets (where appropriate). The application is managed centrally by IMS support staff. Using this central management tool, client definition updates, client health, and additional scanning are overseen. Reports are also used to support preventative action planning.

This approach is audited and improved in line with ISO27001 ISMS controls (Annex A) A.12.3.1

Patching & Operating System Version Control

Patching of assets issued by the business is managed through supporting applications. Patches and new versions of operating systems are issued promptly to ensure risks are kept to a minimum. Specific patches and versions that could negatively affect the network, products and services are tested by the support teams before deployment. Other patches are considered safe and are deployed with little or no human intervention. For critical identified products and services, patches and new versions deployed to the host are always supported by a qualified member of the support team.

This approach is audited and improved in line with ISO27001 ISMS controls (Annex A) A.6.2.1 A.12.5.1 A.12.6.1

Data Loss Prevention (DLP)

Access to Mass Storage Devices (MSDs) is restricted using a third-party tool. Access to MSDs is denied by default, written approval must be received and approved with justification before access is granted to a user and the device.

Encryption is also applied to all IMS owned EUD's where data is processed, encryption is applied and monitored using native tooling where possible.

An applied clear desk and screen policy is also in place that includes additional appropriate security controls for EUD's.

This approach is audited and improved in line with ISO27001 ISMS controls (Annex A) A.8.3.1, A.11.2.7, A.11.2.9

Technical Measures for Application Security

Patching & Application Version Control

As with operating system controls, applications that are used around the business are monitored using third-party software. Monitoring is in place against patch and version levels. EoL applications are removed/replaced when appropriate, all activities are carried out by qualified IMS employees.

This approach is audited and improved in line with ISO27001 ISMS controls (Annex A) A.6.2.1, A.12.6.1

Application Vulnerability Testing

IMS run a vigorous vulnerability testing program in line with the internal development team ensuring IMS produced products and services are thoroughly penetration and or vulnerability tested before release into live. Remediations of issues are addressed and managed through an established development lifecycle.

This approach is audited and improved in line with ISO27001 ISMS controls (Annex A) A.6.2.1, A.12.6.1, A.12.6.2

Monitoring

EUDs are constantly monitored with a range of applications and established agreed thresholds to ensure the device is in 'good health' such as disk space, CPU, uptimes, operating system & applications versions, central logs and event management, active connected user and historical user details, asset warranty and licensing consumption.

This approach is audited and improved in line with ISO27001 ISMS controls (Annex A) A.12.1.31 A.12.4.1, A.12.6.1, A.14.1.1, A.16.1.1,

Technical Measures for Data Security

Retention

Data retention is a cornerstone control that underpins the wider activity of data management. IMS have a clear and detailed retention policy and supporting activities to ensure data is processed in line with legislation requirements and contractual commitments. Automated processes are in place to manage policyholder data retention requirements. Data used across the wider business is also supported by automated processes where appropriate.

This approach is audited and improved in line with ISO27001 ISMS controls (Annex A) A.12.3.1, A.12.4.2, A13.2.1, A.18.1.3.

Classification

IMS has applied a classification matrix to all structured and unstructured data into 4 categories, Public, Internal Use Only, Private and Confidential, and, Restricted. The matrix is supported by a company-wide policy that includes data handling controls that reflect each classification category.

This approach is audited and improved in line with ISO27001 ISMS controls (Annex A) A.8.1.1, A.8.1.2, A.8.2, A.8.3.1, A.9.1.1, A.11.2.9

Anonymisation

Policyholder data is pseudonymised, anonymised using automated activities. This automation is in line with contract agreements, legislation requirements and business needs. All of which are captured in a Data Retention Policy. All PII data is removed after a timed period from the policy being cancelled.

Access Management

All access to IMS assets and data sets is set as 'denied by default' in the first instance. Access is only provided based on the IMS Role Based Access Control (RBAC) model for all IMS employees. Additional or elevated privilege access is only granted by written and approved request. Access to assets and data sets are audited regularly. Default accounts and passwords are altered, and system accounts also fall under access management controls.

This approach is audited and improved in line with ISO27001 ISMS controls (Annex A) A.8.1.2, A.9, A.11.1

Encryption

Client data is encrypted throughout the IMS environment. Encryption is in place using a range of controls, these are applied, when required, to data in transit as well as data at rest.

This approach is audited and improved in line with ISO27001 ISMS controls (Annex A) A.10, A.11.2.7, A.12.3.1

Backups & Continuity

Robust backup and continuity planning is in place to support the requirements of the data and clients. A range of applications is in place to conduct and monitor the data backups and disaster recovery solutions. Supporting policies and processes are maintained to support the business.

This approach is audited and improved in line with ISO27001 ISMS controls (Annex A) A.12.3, A.17

OPERATIONAL MEASURES

A range of organisational measures have been designed and deployed throughout the Group. These measures are overseen by the IMS Compliance team, the team is separated into three disciplines of compliance: legislation, regulation, and contract. The team is responsible for internal policies, organisational process methods, standards, controls, and audits used to deliver data protection, information security, and contract agreements. These activities are essential and work in partnership with the technical measures to ensure the confidentiality, integrity, and availability (CIA) of personal data and commercially sensitive data is maintained.

Operational Measures for Policy Management and Compliance Operations

Geographic Data Protection

At IMS a dedicated full time Data Protection Officer (DPO) forms part of the Compliance team. The DPO ensures the business operates all products and services within the strict requirements of not just GDPR and UKGDPR but all of the applicable geographic data protection legislation.

This approach is audited and improved in line with ISO27001 ISMS controls (Annex A) A.18.1.4

ISO27001 Information Security Management System (ISMS)

Along with the legislation controls, IMS holds accreditation to ISO 27001 ISMS since 2018. The accreditation covers all offered products and services from the business. This regulation element is managed by dedicated and qualified staff within the Compliance team. Ensuring a safe and secure environment is essential to IMS, its clients and its wider supply chain.

Contract Compliance

The contract between IMS and its customers and IMS and its suppliers make up the 3rd framework element managed by the Compliance team. Making good on contact agreements and SLAs is essential in delivering reliable, robust, and fit for purpose products and services to IMS customers. Again, experienced staff are in place within the Compliance team auditing and supporting delivery of the contract agreements and SLAs.

Risk Management

A defined legislation, regulation and contract Risk Management process is in place across IMS. Risks are assessed for initial raw risk scores, risk types, and remediation options, risks are also issued owners and risk categories. The process is maintained and reviewed quarterly with the risk owners and wider business.

This approach is audited and improved in line with ISO27001 ISMS controls (Annex A) A.6.1.5, A.12.6.1, A.15

Vulnerability Management

Appropriate IT issued assets are subjected to vulnerability scanning and remediation activities. These scans and actions are predominantly conducted on a schedule based around vendor release and recommendations of updates, patches, and version controls. However, Ad hoc scanning is conducted in line with development and change to support the business.

This approach is audited and improved in line with ISO27001 ISMS controls (Annex A) A.12.6

Penetration Management

Penetration testing is conducted multiple times throughout a 12-month period at IMS. The testing is conducted using reputable third parties, in line with development and change to support the business. Results are internally reviewed, and remediation is agreed upon based on the risk criteria of the finding.

This approach is audited and improved in line with ISO27001 ISMS controls (Annex A) A.18.2.3

Auditing

Defined internal auditing of data protection and retention, ISO27001 clauses and controls, plus contracts are conducted by the Compliance team as part of the core business as usual (BAU) activities, this also includes the auditing of the IMS supply chain.

The business undergoes and welcomes external auditing. The Compliance team assist and oversee the external auditing of yearly ISO27001 audits by its certification body and a range of IMS customer audits.

This approach is audited and improved in line with ISO27001 ISMS controls (Annex A) A.18

Monitoring

BAU activities are in place within the Compliance team to monitor the ‘health’ of the IMS environment. A range of third-party applications is in a place where application generated reporting is produced. Additional investigation activities are carried out to identify housekeeping activities and remediation to unexpected changes.

This approach is audited and improved in line with ISO27001 ISMS controls (Annex A) A.12.1.3, A.12.4, A.12.6.1, A.13.1.1, A.14.1.1, A.15

Compliance Consultancy

The Compliance team are in place to deliver an internal 'consultancy service' to the business. Members of the Compliance team are involved in all areas of the business and all stages of the customer journey. It is their role to ensure the appropriate controls, policies, processes and wider frameworks of legislation, regulation and contracts are in place and maintained.

Change Management

Change to the IMS environments follow an established, controlled, and documented change control process. All changes are documented and reviewed/approved by selected stakeholders within IMS and when required by customers and third parties. Using this process and the Change Advisory Board (CAB) IMS ensures all changes are necessary, documented, risk assessed, and approved before deployment.

Incident Management

Incident management is in place at IMS. The management is broken into a potential 3 set process that can move from event logging, incident investigation and possible escalation to a breach investigation. All 3 sets are process controlled with defined roles and responsibilities, recorded evidence and opportunities for lessons learnt for preventative actions.

This approach is audited and improved in line with ISO27001 ISMS controls (Annex A) A.16

Continuous Improvement Management

The plan-do-check-act cycle is essential in ensuring IMS actively improves its compliance levels. Improvement is delivered through a range of existing processes and activities such as change management, audit remediation, staff training, and project development. Improvements are applied for corrective action (immediate remediation) and preventative action (long term remediation).

This approach is audited and improved in line with ISO27001 ISMS controls (Annex A) A.18