**Scope public statement**

This ISMS applies to ABC Technologies. ABC Technologies facilitates the acquisition of information, including customer data entry (name, contact information, availability, and recreation). It allows a company to store, control and modify information, plan tasks, annotate notifications as well as several other functions. This is in accordance with the Statement of Applicability.

**ISMS Scope Boundaries**

**Information systems Boundaries**

**Within the ISMS Scope**

* ABC software products: ABC Supreme, ABC Pro, ABC – Although the software is not stored by ABC Technologies the software is owned by them (Product development plan (design, development costs, and source code)).
* Personal and financial data.
* Network devices. Firewalls, switches, hubs, routers, etc.
* Input and transfer stage of customer data during the transfer and treatment process by the third party.
* Networks
* Operating system

PECB (2011)

ABC software products like Customer Relationship Management (CRM) are the key process and are the most valuable to the company. It must be included as this is the product they sell to customers.

The personal information of customers is currently stored in the database with no security. Customer data needs to be protected to ensure ABC Technologies' credibility is maintained as well as customers' trust. Losing customer data will be a breach of The Data Protection Act, which also will lead to a fine. Losing customer data can also have a huge effect on the performance of the company’s software products as data may be sent to the wrong customer thus the service is not adequate.

The company’s financial and accounting data is required to ensure all the activities within the software team can be performed and completed. Financial data also helps the company to see how well each software technology is selling and can help determine the number of resources needed.

Network devices are a crucial part of any company that uses any form of an electronic device in their internal networks. Each network device needs to be configured correctly to ensure all data passing through is secure (only authorised people can view it) and not lost. There is no network diagram therefore it is presumed that ABC Technologies have the following network devices:

* Hub.
* Switch.
* Router.
* Bridge.
* Gateway.
* Modem.
* Repeater.
* Access Point.
* Printer.
* Firewall.
* Computer.
* Server.

The input and transfer stage of customer data during the transfer and treatment process by the third party is a process that ABC Technologies is responsible for as at this stage as the data is controlled by the company. Only ABC Technologies at this point should have access to it until it is sent securely to the third-party databases.

Intranet is used by ABC Technologies to support the ISMS, all policies, procedures, and guidelines must be available in print or electronic version to all authorized persons using an internal network system;  thus allowing all procedures being security/work based to be viewed by any employee of the company.

The networks used within ABC Technologies are not specified to be wired or wireless but will be presumed to be wired as it is more secure. Two internal networks are being used one at the Leeds office and the other at the Bradford office and communication between the offices is possible via server. It is assumed the network is setup as follows:

Employees at the Leeds office use desktop computers. The network is also connected to a central server, which is used to store customer data, customer orders, financial and accounting records, and contracts of partnerships.

Employees at the Bradford office have desktop computers connected through a network. The network is connected to a central file server. This server is used to store all relevant information.

The ABC Technologies employees currently are using the Windows 10 operating system to perform their daily tasks on the computers owned by the company. As this is the only operating system ABC Technologies uses the employees must be competent at using it. Although it is not recommended to use an older version of windows as patches and updates to known vulnerabilities may not have occurred.

**Outside the ISMS Scope**

* Data information assets in control of third-party companies. - Software-as-a-Service (SaaS) environment provided by ABCloud.
* Corporate company website – Was built by an external company and also takes care of relevant updates.
* Physical access control from remote devices via VPN – managed by a leasing company.
* Application – utilities, software management payroll

Anon *(2022)*

AB Cloud provides the Software-as-a-Service (SaaS) environment. This is outside the scope as ABC Technologies is not storing the data assets on their servers.

The Cooperate company website was built by an external company that also takes care of the updates. Although there is a website designer working for ABC Technologies it appears they do not implement any updates.

A leasing company manages the physical access control from remote devices via VPN. ABC Technologies does not own the physical access control software therefore cannot be included in the scope.

Applications like utilities and software management payroll do not need to be included as they are not relevant in protecting crucial assets in the company.

**Organisational boundaries**

**Within the ISMS Scope**

* Internal network end devices
* Access control policy.
* Departments that are relevant to software activity – Software activity team (CRM) and IT team.
* Personal who are involved with the software activity and software infrastructure.

PCB (2011)

Internal network end devices are within the organisational boundaries of ISMS scope because these are key components used by the employees to allow them to communicate and save information on; servers allow employees to communicate (PDF) with each other through end devices like laptops and computers.

An access control policy is a vital part of any organisation with the main idea being to keep data assets confidential. Access control can range from who can enter what part of a building to what files a person can access. ABC Technologies  is allowing cleaners to have the ability to see source code on paper without any presence from the ACB Technologies team. Cleaners could easily take the code and sell it on to competitors or leak the code online which would lead to repercussions to the organisation. For example, loss of revenue.

**Departments that are relevant to software activity.**

Activities relating to the software must be carried out by people in the selected departments as they are the only ones who are allowed to have involvement. This type of access control ensures that everyone working and helping run the software is competent and trusted.

The IT team is involved in the software activity as it is a subdivision of the CRM.

**Personnel who are involved with the software activity.**

Personnel involved with the software activity at ABC Technologies are from the CRM, IT teams, and Sabrina Senat the CEO as they oversee all the firms activities:

CRM

* President - Paul Evans (Leeds),
* Vice-President - Sally McCarty (Bradford),
* Manager Software Development - Sam Gold,
* Support Technician - Billy Davis
* And others

IT Team

* IT Supervisor - William Clay,
* Network Supervisor - Peter Ly,
* Network Technicians - Richard Feringa, Patrick O’Grady,
* Supervisor  IT Support - Fred Jones,
* Support Technicians - Francis Smith, Reese Taylor, Malcom Porter.

**Outside the ISMS Scope**

* Data transfer links
* Standalone applications
* All external contracts (partnerships, contractors, relationships, and contracts) – ABCloud data centers are in the UK, USA, and India.

PECB (2011), Mackie, R. (2016)

Data transfer links would not be included in the scope as they are all outsourced. Examples of this would be the internet and telephones. ABC Technologies do not conduct any business in these areas and therefore would not deploy them. ABC Technologies would only replace outdated or broken devices like a modem or telephones as well as wiring like fiber optic.

Standalone applications are only used by the company and as it is a type of file it would be saved on a database. The company only cares about the contents of the PDF and not the application itself. This can be said for all standalone and software applications the organisation does not own.

All external contracts are not managed by ABC Technologies. As this is the case there is no risk or requirements for ACB Technologies to implement security controls. This applies to the following third parties:

* SoftProd- a database that contains information on ABC’s products, and the companies in charge of maintenance on both sites. In the situation of ABC Technologies SoftProd only provides the service of their database software. The security controls will need to be implemented by SoftProd in this situation as ABC Technologies do not own the software.
* ABCloud- Provides software developed by ABC Technologies is held in a Software-as-a-Service (SaaS) environment
* Corporate website of ABC Technologies that was built by a website  
  development company that also takes responsibility for relevant updates. Although Julia Robinson is a web designer at ABC Technologies, they do not actively maintain the cooperate website.
* Physical access control from remote devices – managed by a leasing company.

It is expected that third-party third parties maintain a trusted ISMS (ISMS.online 2015).

**Physical boundaries**

**Within the ISMS Scope**

* Employees working from within the Leeds and Bradford offices.

The main place of operations for ABC Technologies is the two office locations, Leeds and Bradford. These are the only two office locations in which the organisation can control the assets within the buildings. Physical security is as important as cyber security. The offices need to have appropriate security on doors and could be as simple as having a security guard and having a reception as a first point of security in the building. This may not return determined criminals however having reinforcement and access control where identification is required in certain areas of the office can help.  Sutton, D. and Taylor, A. (2013).

**Outside the ISMS Scope**

* All external contracts (partnerships, contractors, relationships, and contracts).
* Workplaces in buildings owned by third parties that ABC Technology staff work from.
* Hardware employees use outside of the office.

(PECB 2011)

Employees who decided to take hardware outside of the company’s physical boundary are then responsible to ensure the hardware is kept safe and undamaged. As it is outside ABC Technologies' boundary the organisation cannot enforce where the hardware goes but can only enforce software activities. For example, ABC Technologies can implement control access via username and password login to different applications as well as an employee laptop.

ABC Technologies cannot control the environment of employees who work remotely. This results in several factors that the organisation cannot control like access control at the workstation. As the users use VPN it can be hard to distinguish the exact location the employee is logged in making it hard to identify the employee as a username and password are only required. The remote access is also managed by a leasing company resulting in the leasing company having to implement security controls. Another issue could be the employee’s internet connection is too slow or keeps disconnecting slowing down productivity.

All external contracts are not managed by ABC Technologies. As this is the case there is no risk or requirements for ACB Technologies to implement security controls. Physical access control from remote devices is managed by a leasing company.

* Physical access control is managed by a leasing company that uses a VPN to allow a connection.

**Size of scope**

* Company financial accounting data.
* Product development plan (design, development costs, and source code).

BSI Standards *Publication (2013)*

Using a limited scope in these ISMS allows ABC technologies to focus purely on the software activities of the organisation. There is no need to include printing/3D printing business processes of the organisation as ABC Technologies purely want to focus on the software activities because of the performance. This benefits the organisation by pushing the software activity side of the organisation to compete with competitors with similar products in a rapidly increasing market. Having the two listed business processes will help the organisation to solve operation problems like loss of important information and loss of several contracts. In turn, this will help with customer confidence.

The product development plan is the most valuable business process in the organisation as it shows the organisation where there are efficiency flaws. ABC Technologies' software department currently is very inefficient costing the company in the following:

* Loss of important information
* Loss of several contracts
* Loss of confidence of some customers
* slow the growth of the company’s software activity

These issues occurred because of poor management and organisation and operation problems.

Without adequately securely stored and accessible financial data the organisation will struggle to function. Financial data will be needed to allocate funds to certain areas in the organisation as well as account for customer payments.  Certain activities may go over budget and without proper tracking of financials, the organisation can easily overspend, which over time could result in layoffs.

A limited scope is being used for the following reasons:

* Crisp boundaries can be defined
* Easy adoption and buy-in to the change
* Only critical services are focused on
* The organisation gets a faster return on investment as a limited scope can be seen as a quick win.
* Takes a shorter time to implement compared to an expansive scope.

PECB (2016).

The drawbacks of a limited scope are:

* A culture change only happens with people involved the in the scope.
* Only focuses on one area of an organisation and not the whole.
* Senior leadership team does not necessarily have to be involved therefore the scope may not be suitable for the organisation being assessed.

PECB (2016).

It is important to follow the minimum requirements of ISMS by conducting a management review once a year. This can be more frequent if any material changes occur that affect the security of information to the ISMS. Further implementation can be added to other departments in the organisation later (Asosheh, A., Hajinazari, P. and Khodkari, H*. 2013)*. This will result in the scope of the organisation being changed as well as the ISMS.

**Bibliography**

Asosheh, A., Hajinazari, P. and Khodkari, H*. (2013). A practical implementation of ISMS.* [online] IEEE Xplore. doi:10.1109/ECDC.2013.6556730

Bsigroup *(2015). Benefits of using standards | BSI Group*. [online] Available at: <https://www.bsigroup.com/en-GB/standards/benefits-of-using-standards/>

BSI Standards *Publication (2013), Information technology – security techniques – information security management systems.* Accessed via University of Bradford: Canvas 01/11/22, Faculty of Engineering and Informatics (El), University of Bradford, <https://bradford.instructure.com/>

ISMS.online. *(2018). ISO 27001 Requirement 4.3 - Determining The Scope Of The ISMS.* [online] Available at: <https://www.isms.online/iso-27001/determining-scope-information-security-management-system/>

Mackie, R. (2016), To Include or Not to Include – Scoping ISO 27001 and Colocation Service  
Providers.  Available  at:  <https://www.schellman.com/blog/to-include-or-not-to-include->  
scoping-iso-27001-and-colocation-service-providers

PECB *(2016). How to select the best ISO 27001 Scope? Extended vs. Limited.* [online] pecb.com. Available at: <https://pecb.com/past-webinars/how-to-select-the-best-iso-27001-scope-extended-vs-limited> [Accessed 1 Nov. 2022]

Professional Evaluation and Certification Board (PECB), 2011. Initiating ISMS, Understanding the Organisation, Scope.  Available at: <https://bradford.instructure.com/>

Sutton, D. and Taylor, A*. (2013). Information security management principles*. Bcs Learning & Development Lim