Danila Nikitin

ACHIEVING PRIVACY AND ISO 27001 STANDARD

Bachelor's thesis
Bachelor of Engineering

Information Technology

2023

South-Eastern Finland
University of Applied Sciences

South-Eastern Finland University of Applied Sciences

Degree title	Bachelor of Engineering
Author(s)	Danila Nikitin
Thesis title	Achieving privacy and ISO27001 standard
Commissioned by	HewardMills LTD
Year	2023
Pages	108 pages, 8 appendix 1 pages, 1 appendix 2 page.
Supervisor(s)	Matti Juutilainen

ABSTRACT

Organizations of various sizes face two problems regarding their informational assets. The problem of complying with privacy obligations the role of which is to protect data owner's rights in relation to how it is used and how an organization is communicating with customers. The problem of information security and how security is organized in general both apply more to recently founded companies. Founders lack understanding of what to start with, what measures to implement, and how to prioritize them.

The goal of this thesis was to establish a general understanding of privacy obligations and compliance variants as well as an understanding of how ISO 27001 contributes to security, how to achieve that certification and assess its efficiency and value to recently founded organizations. The main aim was to create an achievement roadmap and assess how the standard contributes to the confidentiality, integrity, and availability of an organization's valuable information and assets as well as how valuable it is for recently founded organizations. Topics covered should have provided enough knowledge to grasp the vector of progress and formed a basis for planning and achievement of those goals.

Since the structure of this thesis was shaped around creating guidance for achieving goals, the research method deviated from recognized methods, it involved researching requirements from official sources and possibilities to comply with them considering organizational matters and business needs. The research methodology for privacy is based on the determination of essential privacy matters for organizations that the author learned during an internship and followed research in European law sources on what they impose and how possibly organizations can comply with them. For the ISO part, the research methodology consists of material gathering from reputable sources but due to the lack of coverage for all topics less academically valuable sources such as implementor's or auditor's blogs and forums were also utilized.

The study resulted in the creation of such guidance in which the privacy part was closely tied to web privacy and included contemporary technological privacy matters. Studies showed that standard compliance did not necessarily increase security due to a lack of minimum-security criteria and had lowered value to recently founded organizations due to high costs, lowered organizational flexibility, and complex growth if implemented poorly.

Keywords: Privacy, ISO 27001, obligation, risk.

CONTENTS

1 INTRODUCTION

The ever-changing modern threat landscape imposes the need for the utilization of organizational approach to counter new and existing threats. In its essence the ISO standard is managing the way in which Information Security Management System (later ISMS) operates which involves a plethora of processes and policies. ISO 27001 was chosen as a subject of study due to its heavy emphasis on the continual improvement concept, unique approach to each business's needs and security infrastructure as well as its widespread utilization. ISO 27001 is beneficial for a company not only because of obvious reasons of information security but also because of the structured approach towards security management that streamlines processes and increases trust in your company from existing and future clients, partners, and regulatory organizations as well as aid in building and strengthening organization's reputation. Privacy, the goal of which is to protect client and employee information from misuse and wrong handling from the legislative point of view, is as well a huge contribution to those goals. Although privacy requirements are obligatory and more perceived as a burden, fines from regulators based on not meeting privacy requirements are counted in millions of euros thus, making another stimulus for implementation.

Due to the specific nature of the research, the structure of this thesis is formed around achieving compliance with requirements and thus presented in the following structure: requirements, possible solutions, author's assessment, other compliance variants, and thoughts. The scope of the privacy part of this thesis is broad to involve most personal data handling issues both internally and externally that recently founded organizations struggle with. The inclusion of fundamental concepts of data protection concepts and principles is essential for understanding the privacy framework. The scope of the ISO 27001 part is balanced in a way to provide enough knowledge of general requirements compliance and a more in-depth analysis of core processes such as risk analysis and risk treatment. Processes not listed in the requirements but vital for the integration into existing management and infrastructure of a company and the alignment to business needs are also included. As achieving the standard means acquiring certification almost every section includes the compliance demonstration council part. Due to

the high number of requirements and possible solutions, the structure of the research is mostly done in a way of listing requirements and providing a solution proposal afterward. Where understanding of a topic is not strictly tied to the list structure a more descriptive approach is utilized. The study utilizes REGULATION (EU) 2016/679 OF THE EUROPEAN PARLIAMENT AND OF THE COUNCIL which later in the text will be referred to as the GDPR. The study also utilizes DIRECTIVE 2002/58/EC OF THE EUROPEAN PARLIAMENT AND OF THE COUNCIL which later will be referred to as the e-Privacy Directive. It is important to note that all GDPR Articles stated in the reference section come from a single document that incorporates all Articles. For ISO part, most of the academic material is gathered from the ISO documentation itself, Nine steps to Success: An ISO 27001 implementation Overview by Alan Calder and Information Security Risk Management for ISO 27001/27002 by Alan Calder and Steve Watkins. The first source provides the requirements of the standard, the second one is utilized for general implementation information gathering as well as business-related processes whilst the third one is used for information gathering specific to core processes of ISMS.

The goal of the privacy part of this thesis is to provide general knowledge on privacy obligations and methods of compliance with them. The goal of the ISO27001 part is to provide knowledge on how that standard contributes to security management, guide through requirements and how to comply with them, assess its effectiveness and implementation value to recently founded organizations, as well as to discuss problems of implementation and the standard itself.

In this thesis, the author will cover how to meet privacy requirements with an example of an imaginary company. Mostly the privacy part will include imaginary company examples as for ISO standard risk assessment and treatment processes a detailed sensitive infrastructure documentation including organizational structure and technological stack is needed which cannot be produced artificially. The imaginary company is registered as Memphis in the

European Union and is producing biomechanical prosthetics. Memphis collects data from its customers including health data, utilizes a cloud service, has a site with cookies, monitors traffic and email service, utilizes BYOD, has a physical facility with CCTV and biometric locks, 1000 employees, a branch in the US, New Zealand and Bulgaria, subcontractors and clients in Europe and US.

2 PRIVACY AND GDPR

Privacy regulations set out how companies should treat personal information. GDPR is a set of European laws structured to harmonize complex ideologies and perceptions surrounding human rights in a sphere of personal data. Any storage, processing, or transfer of personal data within EEA should be in accordance with the GDPR. Although GDPR is considered a gold standard, it should be noted that it acts as a baseline for data protection in European countries, and further obligations are imposed by state laws. When dealing with privacy one should think globally and adapt to each jurisdiction of operation. The emphasis of this part of the thesis is mostly pointed at GDPR with parts of the e-privacy directive and working party recommendations where applicable. It should be noted that to comply with the regulations and obligations provided further, the organization should have substantial resources. A serious attitude from senior management should be pointed towards obligations due to possible further neglect from the rest of the organization to privacy issues. (Appendix 1.)

2.1 Data protection concepts

In this chapter, the main privacy-related concepts from Article 4 will be described to help the reader understand further obligations and requirements.

Personal data - all data anyhow related to an identifiable or unidentifiable natural persons is considered personal data. If enough data can be put together to identify an individual it is considered personal data as well.

Sensitive Personal Data - under GDPR is data regarding racial or ethnic origin, political opinion, religious or philosophical beliefs or trade union membership, genetic data, biometric data, data concerning health, or data concerning a natural

person's sex life or sexual orientation. Sensitive data could pose a significant risk to an individual's fundamental rights and freedoms if it falls into the wrong hands.

Health data - these are all kinds of data about the physical or mental health of a natural person. This can also include photos, particularly ones that reveal a physical condition.

Data Controller- a party that defines the purpose and means of personal data collection and processing.

Data Processor- a third party involved in data processing on behalf of the data controller, obliged to follow the controller's rules. The data controller cannot be a data processor in normal conditions however if the same personal data is processed for a different purpose, then collected data controller can be a data processor.

Joint controllers- If both parties determine processing rules, they are considered joint controllers.

Processing – operation or multiple operations performed on personal data, either manually or automatically such as collection, recording, organization, structuring, storage, adaptation or alteration, retrieval, consultation, use, disclosure by transmission, dissemination or otherwise making available, alignment or combination, restriction, erasure, or destruction

Terminal equipment – any electronic device that allows access to data.

Establishment - 'Establishment implies the effective and real exercise of activity through stable arrangements. The legal form of such arrangements, whether through a branch or a subsidiary with a legal personality, is not the determining factor in that respect' GDPR Recital 22

ROPA – record of processing activities is a document that incorporates activities and associated parameters of those activities that organization is performing in relation to personal data.

Data mapping – documented flow of personal data within an organization that describes what and how data is treated.

DPIA – Data Protection Impact Assessment is a privacy risk assessment mechanism that analyzes how new goods or services affect data subject's

privacy interest and whether it is compliant with regulations. Output of DPIA identifies those risks for further treatment.

Based on those definitions Memphis can determine that health data is being gathered to produce correct prosthetics, but it is also important to note that the fact that other data about person who ordered it has a need for that prosthetic is also a sensitive information. Memphis is a data controller and is responsible for the definition of processing rules and should notify its subcontractors of their responsibilities. Memphis establishment is EU based.

2.1.1 Data protection principles

General principles of data protection which should be followed during collection, processing, or transfer are described in this chapter. All collected personal data including sensitive personal data is subject to data protection principles which include lawfulness, fairness, transparency, purpose limitation, data minimization, accuracy, storage limitation, integrity and confidentiality, and accountability. (European Commission site, no date)

Lawfulness

To process personal data, there should be a legal basis for such action. Prior to processing, the specific purpose for which personal data is collected and further processed should be determined. Those bases are:

1. Freely given consent in a specific, informed, unambiguous manner. It should be done in affirmative action such as pressing a button or ticking a box.
2. Processing needed to fulfill contractual obligations to which the data subject is one of the parties or in cases where prior to entering the contract data subject request should be processed.
3. Processing is needed to fulfill legal obligations to which the controller is a subject.

4. Processing is necessary for public interests for official duties or in the exercise of authorities vested in the controller. Such interests are formulated by National EU or Member State Laws.
5. Processing is needed for the purpose of saving or protecting an individual's life. Only applicable in emergency situations.
6. Processing is a legitimate interest of a company. This is the most opted basis for processing grounds, and it requires a balance of interest assessment. Note that this processing should not undermine the data subject's rights.

In the case of Memphis points number 1 and 6 are applicable where legitimate interest is the most flexible way but in case of a data subject access request you are obliged to provide all records as well as justify your legitimate interests. Other lawful grounds are also applicable but rather in an exceptional manner. If the data subject disagrees with its justification, it is Memphis's duty to prove otherwise. Thus, in this case, freely given consent is the best option.

Fairness

Fairness sets out honest behavior in relation to data subjects. Besides the general requirement not to mislead or deceive a data subject, this principle requires data processors to consider the effects of processing on individuals involved and to stop processing in case of adverse effects to them. Data subjects should be aware of their data's processing, which should not exceed the reasonable expectations of data owners.

Memphis can comply with those requirements by performing an internal privacy audit to ensure fairness of processing, providing privacy notice, and performing a privacy impact assessment to ensure no adverse effects to data subjects are present.

Transparency

Transparency is a principle the purpose of which is to govern and enforce fairness by imposing organizations to make their processes clear, open, and

honest. This principle manifests itself in the requirement of simple and plain language utilization during the notification of data subjects in an accessible manner. The privacy notice should include details about controllers such as contact details and purpose of the processing as well as rights of data subjects and possibly contact of regulators.

Memphis can comply with this requirement by including privacy notice in the early stages of service provision like registration, by means of including privacy notice into the contract and/or oral notification.

Purpose limitation

Purpose limitation is a principle that enforces controllers to collect and process data only for legitimate, specified, and explicit purposes. Any collection or processing out of the scope of those criteria is unacceptable. In order to be governable that principle obligates the data controller to identify the purpose, document it and inform the data subject of the purpose before collection or processing starts. Data can be used for other purposes if it is within or relates to original purposes.

Memphis can include purpose limitation checks in periodically conducted internal audits. It is recommended to make a standalone purpose policy that would set out rules of collection.

Data minimization

Data minimization serves the purpose of governing criteria of data collection. Only data relevant and necessary to the purpose of collection should be gathered. Adequacy of collected data in terms of the amount should not exceed boundaries of purpose fulfillment.

Memphis to be compliant should enforce that principle into its data collection processes. This can be enforced by regular internal audits.

Accuracy

The accuracy principle enforces data controllers to put measures to ensure that collected data is correct and not misleading. Information tends to be outdated and it is the controllers' duty to check and keep it updated. If inaccurate data is identified, it should be corrected or if it is not possible inaccurate data should be deleted. Keeping data up to date may face a plethora of challenges, and methods to overcome them should be contemplated and implemented.

Memphis should implement technical or organizational processes to prevent inaccurate, incomplete, and misleading information from being gathered. This might include automatic checks of web pages, comparison of data to other databases, or requirement to provide government-issued documents. Data subjects have a right to correct their data, such requests should be checked by the method above and executed. Recording the source of information change is beneficial as it might provide justification in case of regulatory inspection.

Storage limitation

Storage limitation imposes obligations on data controllers to not keep data for longer periods than necessary for the completion of purposes stated for collection and processing. To comply with that obligation, the controller should determine the retention period, reason it and follow the requirements. When the data retention period ends the data should be destroyed in a manner that ensures deletion, deletion should include all media that contains it. Although there are exceptions stated in Article 5 (1) which states that personal data might be archived because of public interest, historical, scientific research, or statistical purposes.

Memphis might save records of existing clients that might be useful for the maintenance of existing or the production of new goods and services. Although scientific research conditions may apply to the development of new goods, such purposes should also be provided to data subjects. Policy for retention should be created to set universal rules of retention assessment for various information

which need various retention periods. As Memphis is utilizing the cloud it cannot ensure full deletion due to the absence of access to physical drives. This should be discussed with the cloud provider.

Integrity and confidentiality

Appropriate measures should be taken to ensure that personal data is protected against unauthorized or unlawful processing. Data loss, damage, or destruction accidental or deliberate should also be avoided.

Memphis should conduct a risk assessment to determine and address risks associated with access to personal information, tampering, partial or full loss of data. Risk assessment in the scope of ISO 27001 will be described in a 3.4 Planning chapter. Access management also falls into the information security domain, there are several models of access management from which need to know basis is deemed the most secure in that context. Physical, organizational, and technical controls should be used to enforce access management.

Accountability

Accountability ensures that data controllers are responsible and can demonstrate compliance with privacy principles and requirements. This includes:

1. Appropriate policies and processes proving transparency and compliance.
2. Appointed Data Protection Officer (further DPO)
3. Clear contracts are in place with processors.
4. In cases where the processing might result in a high risk to an individual’s interests a DPIA should be conducted.
5. ROPAs should be maintained.
6. Adequate security measures are implemented and demonstrated.
7. Personal data breaches are being reported to DPO and to authorities.
8. Data protection by design and by default approach should be considered.
9. Codes of conduct or certification schemes are followed.

All requirements should be followed by Memphis oy besides requirement number 8 which has a recommendation nature. DPO appointment will be discussed later in chapter 2.6. Criteria to trigger DPIA must be set to not overlook potentially hazardous processes. Adequate security measures are achieved by the implementation of the ISO27001 standard but other standards or certifications that require less effort such as Cyber Essentials might provide enough justification. Breaches, data protection by design and by default, and codes of conduct, as well as associated obligations, will be discussed later. (Appendix 1.)

2.1.2 Data subject rights

When an organization is processing personal data it should respect and execute data subject rights, those eight rights are applied to any data processing or collection that is related to data subjects. (The European Commission what are my rights, no date) Articles 12-23 of GDPR stating data subject rights have a significant impact on an organization's personal data processing including core processes. Data subjects have the following rights in relation to their personal data:

Right of Access
GDPR imposes the necessity to inform data subjects of their personal data processing for purposes of full understanding of processing. Such communication should be concise, transparent, intelligible, and in an easily accessible form, using clear and plain language.

Memphis should be ready to provide data subject with all information that it has concerning that individual or information about processes that relate to their personal data including purpose. This might be achieved by creating an action scheme that would include mechanisms of request and possibly templates that would be automatically filled with all associated data.

Right of Rectification

Data subjects have a right to correct their personal data held by the organization. It is the controller's duty to erase or correct any inaccuracies in personal data based on the data subject's request. Rectification may be done verbally or in writing and a controller should react within a month of receiving the request.

Memphis should be prepared to change information and possibly create a request form on its web page as well as plan storage infrastructure accordingly.

Right to Erasure

Article 17 states that the data subject may request the erasure of personal data if it has fulfilled its original purpose and no new lawful purpose was defined. GDPR promotes strict protection of children's personal data and thus strong emphasis is made on the erasure of children's personal data.

Also, data should be erased if:

1. Lawfulness is based on consent which later was withdrawn.
2. Data is processed unlawfully.
3. Necessary erasure due to compliance with EU or member state laws.

Exceptions to deny erasure requests under Article 17(3) are:

1. Right of freedom of expression and information.
2. Compliance with legal obligations or necessity to perform the task in public interest.
3. Exercise or defend against legal claims.

It should be noted that during erasure all copies should be deleted including ones on backup or any related data on other drives. Memphis should evaluate and respond to such requests.

Right for Restriction of Processing

The right to request the blocking of data processing is stated in Article 12. Article 18 of GDPR states that data subject has a right to restrict the processing of their personal data if:

1. Accuracy of data is being disputed.
2. Processing is unlawful and the request has been sent.
3. Data is no longer needed for the controller, but the data subject exercises data rights or defends legal rights.
4. Erasure request is being contested and a decision on overriding grounds is being produced.

Memphis should evaluate whether data subjects' request have a basis for processing blocking and comply if such is present.

Right for Data Portability

Data subjects have a right to receive their personal data from the data controller in a structured, commonly used, and machine-readable format for transfer to another data controller without any hindrance.

Memphis should plan that in advance and utilize common for a business sphere uniform data storage format and possibly a template for that purpose. This right has a relation to the right of access, and it should be incorporated into the information provision process.

Right to object

Data subjects have a right to object to personal data processing by a controller in case legitimate interest is stated as a basis for data processing. The request might be verbal or written. Proper documenting of requests written or verbal falls under best practice. Unless the data controller can demonstrate compelling legitimate grounds to override the rights, freedoms, and interests of an individual data controller is not permitted to process personal data after a valid objection request.

Memphis should treat each request individually and assess whether legitimate grounds are justified enough to continue processing. On the other hand, if a client is no longer interested in products or services, it is best to comply and not escalate the situation.

Right not to be subject to automated decision-making.
This right has a narrow application since only decisions based exclusively on automatic means that have legal or significant effects on the data subject are affected by this right. The automated decision-making is only allowed if they are:

1. Authorized by law.
2. Are necessary to prepare or fulfill contractual obligations.
3. Explicit consent is provided, and the controller has significant protection measures in place.

Memphis to produce correct prosthetics might use automated means but it does not fall under significant effects besides possible data leak or loss which are countered by the implementation of ISO standard or other security measures. Full automation is also not applicable as during production QA technics and human intervention are inevitable due to individual production. Acquiring consent would be essential in that case.

Data subject requests
Answering the data subject's request is the duty of the data processor. Receiving a request should be acknowledged by a processor and then clarification or confirmation on what was received should be made. GDPR sets a month time frame since receipt of a request is produced as stated in Article12(3). Although that period can be extended by two more months in case of specific situations or complex requests.

The utilization of automatic email functionality by dedicated request address should be used by Memphis to provide acknowledgment or a request form can be filled in on the site which would inform the data subject of acknowledgment. An organization should decide whether it can process a user's request within the first month since the request was received. In case of request processing denial, an organization should notify the data subject of its decision and advise any possibilities to lodge complaints to the local regulator.

2.1.3 Privacy and technologies

A drastic need to regulate data handling arises as new technologies are being developed at a rapid pace. Although most data protection principles stay in place, specific regulations are put in place as new overwhelmingly powerful ways of gathering and processing personal data arise. Misusing such technologies may lead to severe damage to the data subject's interests. In this part regulations for existing technologies will be presented and analyzed but one should take extra caution in utilizing new technologies in their organization from the privacy point of view and contact the regulator if an approach is unclear. Organizations utilizing modern technologies are subject to high complexity even if the organization itself is small. Obligations imposed on these organizations can be frustrating and one should always seek help with such issues as even the extent and applicability of these obligations might be unclear. (Appendix 1.)

Cloud

Cloud computing became very popular during the last decade and its decentralized nature has proven to be worthy from availability, redundancy, and economical points of view but such nature imposes several privacy concerns. Organizations prior to the utilization of the cloud in their business should consider what type of data would be stored in the cloud and what security obligations it should follow. The geographical location of data centers and accordingly their jurisdiction have a significant impact on how data should be treated, this includes the location of primary employees and how transfers are conducted. Further research on how jurisdictions' obligations interact with each other is needed for

each country. Provider's processes for the security of the cloud should be examined with particular attention to how it reports breaches, including timings and documentation. (John C., no date) The relationship between an organization and the cloud provider in terms of who is deemed the controller of data in the cloud and the responsibilities of both parties should be established in a written format. Usually, cloud providers act as data processors but it is in organizations' interest to share responsibility with cloud providers thus making it a joint controller. Ultimately controller bears all responsibility for meeting the requirements of processing. Access to personal data should also be negotiated and documented as cloud providers may access a partition of data in order to execute contractual obligations such as support services. (Appendix 1.)

Memphis should contemplate the usage of the cloud for storing sensitive health data as it imposes severe legal obligations. The author recommends using the cloud for purposes other than production and instead utilize the internal infrastructure. Contract with cloud provider should be contemplated thoroughly and attempt to impose a portion of the obligation conducted. Access to the data by cloud provider should be separately discussed with the aim of lowering the access as much as possible. Whether provided services will breach legal obligations should be established and efforts to mitigate the risk of disclosure requests from foreign authorities done. Utilization of sub-processors from the cloud provider's side should be discussed and agreement of informing of any mistreatment or misuse by sub-processor achieved. In terms of data transfers to data centers outside of the European Economic Area, certain conditions are imposed. It is the controller's duty to safeguard transferred data and be able to demonstrate it. There is a variety of methods which will be discussed in more detail later in chapter 2.7 but applicable to cloud methods of compliance are:

1. Geographical limitation of a cloud.
2. Utilization of successor of Privacy Shield which currently is not working when it will come into effect when dealing with transfers from and to the United States.

3. Data transfer agreements hand-tailored for specific regions
4. Derogation under Article 49
5. Utilization of Process binding corporate rules (BCR)
6. Utilization of conduct codes and certifications

Cookies

Widespread technology for “remembering” users and their data by websites incorporated in the user’s web browser or device. There are two types of cookies grouped by their duration: session cookies which last only during the session period and are deleted after the page is closed and persistent cookies which are stored within the browser cache and have an expiration date. And there are four groups of cookies depending on their purpose: necessary cookies which are essential for the proper work of a website, preference cookies which remember settings like language or region, statistics cookies which are completely anonymized and used only for the improvement of site and business processes, and marketing cookies that are used to determine interests of a user.

When privacy issues arise around cookies usually those are third-party marketing persistent cookies that are collecting personal information for further sale to other organizations. (Cookies, the GDPR, and the e-Privacy Directive, gdpr.eu, no date) Under GDPR recital 30 cookie data in most cases is considered not personally identifiable data unless it links to an individual. Even when it does not link to an individual it does link to a particular device thus it can be linked to an individual. In addition to that it is in the website operator’s interests to link cookie information to name, postal or electronic address. Those dependencies should be analyzed to determine whether personal information is being gathered. Gathering or accessing information already stored on the user’s terminal equipment by cookie utilization is only allowed under consent given in a clear and comprehensive form in accordance with the data protection law. The e-Privacy directive imposes prior informed consent before cookie usage. Cookies prior informed consent means that notice of cookie uses, and purpose is given to a user prior to a cookie being set up on a device.

Users must have a choice to consent or to deny a cookie and must provide an active indication of consent such as a press of a button. Such consent should be stored by an organization. If consent was not given, access to the site should still be granted. Necessary cookies used only for the correct work of a website are an exception. More exceptions to this rule are described in the information provision chapter.

Memphis does have a site that uses cookies thus it is important to provide cookie consent following those requirements alongside privacy notice. The option to manage cookies that would disable the use of non-essential cookies should also be present. Access to the web page should be granted regardless of what cookies were rejected even if the user used tools to reject necessary cookies. The use of cookies should be mentioned in the privacy policy including the possibility not to accept them. What cookies are tracking and whether it is linked to other data thus making it personal data should be carefully examined and such occurrences avoided. It is considered best practice to have a stand-alone cookie-use internal policy and develop legal, technical, and market practices according to this policy. Note that denying cookies should be as easy as accepting them as well as later withdrawing their consent.

Web metadata information gathering.
The IP address is a numerical label assigned to identify a device over the Internet that can be treated as personal data by Internet Service Provider (ISP) since it is possible to link IP addresses to particular users even if the IP address is dynamic. Organizations mostly capture IP addresses to stop denial of service attacks by blocking IP addresses. Other information such as browser type, version, and internet service provider might be tracked as well to analyze trends, administer the website or gather demographic information. The IP address is not considered personal data if an organization does not link it to any other information under GDPR Recital 30.

Memphis does not track any of that information, but if it did, Memphis should have included information about tracking in its privacy policy and provide a purpose for gathering that information.

2.1.4 Data and marketing

Direct marketing is a form of advertising that includes direct contact with potential customers. The directive and the regulation apply to all forms of communication such as mail, email, door-to-door visits, web advertising, and telemarketing. Direct marketing is subject to e-Privacy Directive if it is communicated by electronic networks such as email, fax, phone, and MMS/SMS. The application of privacy principles to direct marketing is one of the most complex themes as not only privacy laws but also consumer rights that vary from country to country are being touched.

To deliver advertisements personal data such as email address, telephone number, or data collected via cookies might be used, collection itself for marketing purposes is already considered direct marketing. Profile creation regarding potential customers and their preferences as well as personalized messages are also considered direct marketing. In addition to that third-party means can be used to deliver advertisements such as instant messengers or social platforms. E-Privacy Directive (42) imposes acquiring consent and informing data subjects obligation which is known as opt-in. Under the directive, the right to object corresponds to cases where prior consent to receive direct marketing was acquired but later was withdrawn, which is known as opt-out. A limited exception to this rule exists as marketing emails are delivered on a denial basis to individuals whose personal data was collected in the context of service or product sales under e-privacy directive Article 13(2). This is known as Soft opt-in. It is important to determine whether Directive’s or Regulation’s rules are applied in a country of operation as it varies. (Direct marketing rules and exceptions under the GDPR, gdpr.register, 2022)

Memphis utilizes direct marketing and to be compliant with requirements prior to marketing should acquire consent to send marketing materials. This might be done in a way of a box-ticking during registration on a site or when a customer is visiting the service for the first time and entering his/her data into the register and the opt-in proposal is asked verbally. In the opt-in proposal means of communication should be stated. Mechanisms to opt-out should be developed such as a hyperlink that unsubscribes your email account from marketing messages or a procedure in customer support which would do the same but for other means of communication.

Location-based marketing.

With the development of the Internet of Things and the widespread popularity of smartphones, location-based marketing became an important tool for marketers to reach their audience. By just passing by a shop, one may receive an invitation for a free sample or a discount. e-Privacy Directive (15) only applies to data revealing the location of terminal equipment and not to the location of a person. It is important to distinguish these aspects as when a data controller wishes to process location information, but that information has no relation to the location of terminal equipment e-privacy rules do not apply meanwhile other privacy regulations are still in power. Types of location data undergoing collection and processing should be informed to users as well as the purpose and retention period in order to get valid consent. Users also should be notified if data is transferred to third parties for additional services.

Memphis is not using location-based marketing, but if it did, it should have received prior informed consent which would include the type of data collected and the purpose of the collection before tying location data to its marketing processes. Overall location-based marketing is most useful for application developers or other internet services as they potentially have access to the location of terminal equipment. In that context, consent might be gathered in the application itself. It should be noted that users should have the option to refuse

tracking of their location and that mobile operating systems will ask for separate consent.

Online Behavioral Advertising (OBA)

Online Behavioral advertising is a web-based form of advertising optimization which uses observation of behavior on the web over time. That approach helps reach relevant audiences and increases the effectiveness of the advertisement. GDPR Article 4 introduces the profiling concept which is described as “any form of automated processing”, where personal data is used to evaluate, analyze, and predict an individual’s performance”. Based on this analysis OBA processed data is considered personal data and is subject to GDPR obligations. Thus, prior informed consent according to GDPR should be acquired. Moreover, IP addresses can be utilized in conjunction with other information to identify an individual, in that case the data set is qualified as personal data. OBA is subject to the e-Privacy Directive with no regard for the data type collected and processed. Under the e-Privacy Directive (25) usage of OBA requires prior consent with clear and comprehensive information provided by the controller. Enforcement of e-Directive depending on the jurisdiction of the country varies as in some cases control over direct marketing including OBA falls in the hands of consumer right regulator rather than the Data Protection Authority. Failure to comply with the Directive or the Regulation may result in fines, administrative sanctions, or civil and criminal liability.

Memphis is not using location-based marketing, but if it did, it should have analyzed under what obligation it falls. As in the previous paragraph, consent should be gathered and close attention to whether personal data is being produced by tying tracked data including data regarding terminal equipment to other data sets.

2.2 GDPR scope

It is important to understand the scope of the GDPR applicability to identify whether processes fall under it. Article 2 and Article 3 of the GDPR form criteria under what conditions the GDPR is applicable.

Material scope
Under Article 2 of GDPR, the regulation applies to the collection and processing of personal data that forms a filing system. It can be achieved either wholly or partially by automated means. Any processes that contribute or result in the creation of database containing personal data are in the scope of the GDPR.

Exceptions to GDPR application include the following:

1. Household and natural person exemption
2. Prevention, detection, and prosecution of criminal penalties.
3. EU institutions
4. E-Privacy Directive
5. E-Commerce Directive

In other words, GDPR is applied to all processing of personal data that will form a database for further unspecified use. Memphis which is collecting data and storing it for further processing should follow GDPR regulations in all instances. If e-Privacy or e-Commerce directives have a legal effect on processing or collection those directives are considered overriding and thus they should be followed. It should be noted that in some jurisdictions member state laws have the most power and one should always check what obligations to follow.

Territorial scope
Under Article 3 territorial scope applies to organizations established in the EU, it is also applicable to extraterritorial and Public International Law. Non-EU organizations controlling or processing European data subjects are also in the

scope of GDPR. In the cases of controllers not based in the EU but where member state laws are applied are subject to International Law.

Memphis is established in the European Union and thus must follow GDPR regulations. In case other branches are registered separately outside of the EU as with Memphis, and they collect or process data of European citizens, GDPR should be followed in relation to those citizens.

Non-EU organizations
GDPR Article 3(2) is applicable to the processing of EU-based subject's personal data by a controller or processor outside of the EU in cases where processing is related to:

1. Provision of goods or service offering with no regard to the fact of payment.
2. Monitoring of behavior in cases where behavior is observed within the EU.

In relation to the first condition, it should be established that the EU language and EU currency are used in offer or service or goods as well as order placing is conducted in the EU language and EU customers are referenced.

Memphis should follow the recommendation stated in the previous paragraph. It is logically more beneficial to address European citizens to European branches of Memphis as GDPR-compliant processes would be utilized by default. The same goes for web pages but one should note that in most jurisdictions it is only legal to conduct sales in local currency. In that situation, it might be worth including a currency converter that would state the amount in Euros while actual withdrawal might be conducted in local currency. Customers should be made aware of that fact.

2.3 ROPA and data mapping

The complexity and volume of personal data collection and processing invoke a need for a systematic approach toward personal data handling management within an organization. Records of Processing Activities, which is also known as ROPA, and data mapping provide a versatile way of doing so.

ROPA

The purpose of ROPA is to demonstrate compliance to authorities upon request by providing a snapshot of the organization's collection and processing practices. This singular document contains processing activities information from all departments of an organization including third-party activities. ROPA facilitates the self-audit process by containing all processing activities which helps to identify processing risks. ROPAs are commonly presented in the form of an Excel document incorporating only necessary information that is being updated only when processing activities change. Under Article 83(4) an organization is subject to fines if it fails to comply with those requirements. The same obligation is applied to processors excluding purpose and description of data and data subject entries. These records should be kept in writing, including electronic form, and be available to the supervisor authority on request. Although this requirement is not mandatory for organizations employing less than 250 people unless a high risk is present to data subjects or if such processing is repetitive. (Osano, no date) Keeping ROPAs actual is one of the top priorities of a company as they provide an overview of personal data processing and help identify privacy risks. (Appendix 1.)

Under Article 30 of GDPR, each controller or controller representative should maintain records of processing activities which would include the following:

- Controller's name and contact details and if applicable joint controller's, DPO's, and representative's details
- Purpose of processing
- Data subject and data categories description

- Transfers to third countries or international organizations including identification of that country or organization. Documented suitable safeguards required for such transfers.
- Data retention periods, or if these are unknown at the moment then predicted data retention periods.
- If applicable general security measures are taken to safeguard the data.

Memphis should take advantage of ROPAs not to just comply with requirements but to use them in internal audits to detect and address privacy-related risks and keep track of compliance with regulations. Memphis should update ROPAs based on the fact of process change and be ready to share that documentation with regulatory bodies on request. Memphis employs more than 250 people and processes sensitive personal data thus it is subject to that obligation.

Data mapping

Data mapping is a process of documenting and understanding how personal data is collected, stored, processed, shared, and discarded. In its essence, it is a combination of data inventory and data flow which provides an overview of personal data lifecycle within an organization. The creation of data mapping includes the following entries:

1. Data source identification
   All sources of personal data collection should be identified including cookies and marketing tools.
2. Personal data categories inventory creation
   All data categories including names, email addresses, and other categories should be identified and documented. It should be separately stated whether the data is sensitive.
3. Data flows definition
   How data is shared and processed within departments of an organization including interfaces of departments, cloud providers communication, and marketing agencies.
4. Addressing cross-border data transfers
   If you transfer data outside of EEA, the country of transfer should be included. Ensure compliance with GDPR requirements of the transfer to third countries.
5. Purpose of processing identification
   The purpose should be documented, and lawfulness compatible with the purpose proved.
6. Data storage

> Data retention is established, documented, represented in policy, and followed accordingly. What security measures are in place to protect it in rest, transfer, and in processing should be documented.

Previously discussed ROPAs can facilitate the creation of road mapping since they contain significant information about processing activities. Data mapping helps to identify privacy risks in motion and address them. If an organization is complex or processes a plethora of data types, it is worth utilizing special tools rather than spreadsheets. (A Comprehensive Guide to Personal Data Mapping, GDPR register, 2023) Keeping ROPA and data maps is essential and one of the first privacy issues an organization should deal with as it provides an invaluable basis for further privacy risk identification (Appendix 1.)

Memphis should take advantage of data mapping as it provides insights into data processing in motion compared to ROPAs and helps to determine privacy risks more efficiently and comprehensively. As Memphis is processing sensitive data utilization of data mapping is highly recommended.

2.4 Lawful processing criteria

Data processing should be carried out in accordance with the criteria described in the data protection principles. The author of the thesis emphasizes that processing should be carried out in a lawful, fair, and transparent manner under Article 5 of the GDPR and have a legal basis under Article 6 of the GDPR which was described earlier.

Sensitive personal data processing
Relation to fundamental rights and freedoms as well as risks of prejudice and discrimination in case of mistreatment requires specific protection to Sensitive Personal Data. GDPR imposes compliance with Articles 6 and 9 for sensitive personal data processing. Processing of sensitive personal data is prohibited by Article 9 in cases that may reveal data subject’s:

1. Ethnic or racial origin
2. Political opinions
3. Philosophical or religious beliefs
4. Trade union membership
5. Sexual orientation
6. Genetic data
7. Biometric data
8. Health data
9. Sex life or sexual orientation

As previously discussed, health data is sensitive data. Biometric data which includes fingerprints is also utilized by Memphis for purposes of identification and authorization at its physical facility.

Exceptions to sensitive data processing prohibition under Article 9(2) are as follows:

1. Explicit consent is given by the data subject.
2. Processing is conducted for social security and employment services.
3. Processing is necessary in vital interests, but the data subject is not capable of giving consent due to physical or legal reasons.
4. Processing is conducted for political, philosophical, religious, or trade union goals.
5. Processing of sensitive personal data made public by the data subject in a manifest manner.
6. Processing necessary for the establishment, exercise, and defense of legal claims or by courts acting in their judicial capacity.
7. Processing is carried out for substantial public reasons with a basis on Union or member state law proportionate to the aim pursued with due respect towards the data subject’s fundamental rights, freedoms, and interests.

8. Processing necessary for preventative or occupational medicine, working capacity assessment, medical diagnosis, provision of health or social care, and treatment. Applicable to services based on Union or member state laws.
9. Processing necessary for public interests in the health sector. This should be done due to the high standards of medical products, services, and devices in relation to quality and safety.

Memphis is collecting and processing sensitive health data which can lead to the disclosure of biometric and health data of individuals. But because it is related to medical treatment activities prohibition does not apply to processing. Produced prosthetics as well as processes succeeding should be of high quality and provide safeguards to the client. It is recommended to inform regulatory authorities of such collection and processing.

2.5 Information provision obligation

Articles 13 and 14 of the GDPR govern provisions of information to data subjects which gives data subjects the right to receive information from data controllers regardless of whether data was acquired directly or from a third party. Data provided to the data subject should be formulated in a concise, transparent, intelligible, and easily accessible form, using clear and plain local or/and English language. In cases where a child is a data subject provisioned data should be written in an easy-to-understand manner. Privacy notices should be reviewed periodically to ensure compliance, audit conduction, and ROPA updates facilitate this process. Senior management and business team involvement directs and provides even more support for achieving effective notice. (Appendix 1.) Direct data provision under Article 13 imposes provision obligation of the following information to the individual if data was gathered directly from them:

1. Controller’s Identity and contact details and if applicable controller’s representative.
2. Controller’s DPO contact details if such is appointed.

3. Purpose and legal basis for processing.
4. Legitimate interest of the controller.
5. Personal data receivers which include processors and subprocessors.
6. Any intentions for data transfers to third countries or international organizations. If such intention exists whether an adequacy decision is produced by European Commission regarding that transfer.

If sources other than data subject are utilized, Article 14 impose more obligations for data controllers in addition to obligations to provide the same information as in the requirements of Article 13(1) and (2) as stated above, to provide categories of personal data gathered, sources from which it was gathered should be referenced. If personal data was gathered from publicly available sources, it should be stated. In cases where the source cannot be identified general information should be provided.

Memphis should include previously listed information in its privacy notice. It is recommended to include working hours in contact details if a telephone number is used for contact. DPO and its obligations to the organization, whether it represents the organization and handles privacy issues should be stated. The legitimate purpose stated in the privacy notice and service/goods agreement should be mentioned. Subprocessors having full or partial access to personal data and processing it on behalf of an organization should be mentioned if such is present. Transfers of data including transfers related to the cloud should be mentioned including the country of transfer and possibly implemented safeguards.

Data subject’s rights provision
Under GDPR Article 13 it is the controller’s duty to explicitly clearly and separately from other information inform data subjects about their rights which include the following:

1. Right to request information processed by the controller.

2. Right to restrict controllers from processing their data in some circumstances.
3. Right to be notified if their data is subject to a breach.
4. Right to object processing if it is conducted on the basis of legitimate interest or used for direct marketing.

Memphis should incorporate those rights into service/goods agreements so that clients are aware of their rights. This will contribute to the transparency principle and demonstrate open and honest treatment of clients.

Additional information provided by the data controller to ensure fair and transparent processing includes:

1. Retention period
2. Right to complain to data protection authority.
3. Right to withdraw consent at any time.
4. Statutory or contractual requirements to provide personal data and consequences of refusal to do so.

Memphis should incorporate that information into the privacy notice and service/goods agreement. It is recommended to provide a basis for a retention period and include contacts from the data protection body. Consequences of refusal to provide personal data are usually a refusal to conduct services.

Fair processing notice requirements
GDPR Article 13 imposes data subjects to be informed of data processing in writing and where appropriate in electronic version. Such notice should be concise, transparent, easily accessible, intelligible, and in clear and plain language. This obligation provides a convenient way of achieving transparency requirements of the GDPR and has other beneficial effects for an organization such as commercial benefits, increased data subject trust, and reduced complaints or dispute risks associated with personal data.

Memphis to ensure fair processing provisions correlating to above stated requirements can utilize just-in-time notice utilization. Those notices are a digest of long 10-15 minutes reading long privacy notices that provide all necessary information in short manageable text in a form of a website pop-up window. Such notice should have a hyperlink to a full version of the notice. Privacy dashboard utilization is another option. This feature is often found in the applications settings tab that informs and manages the utilization of data by an application. Using alternative formats of information communication is not desirable but can be utilized. Mostly provisions are made during the data subject's contact with the data controller but for other situations such as the new purpose of processing an email providing key information with a link to the full text can be utilized.

The new purpose of processing

Under GDPR Article 13(3) whether the data controller intends to process data for purposes not corresponding to purposes stated during data gathering a notice should be provided to the data subject with a statement of new purpose and any other relevant information prior to the processing under new purpose starts. Memphis should notice of new processing purpose in a separate message addressed to contacts gathered during registration or service agreement. It is recommended to include conducted compatibility analysis results related to fair processing obligations in cases where a legal basis other than consent or member state law is relied upon for new purpose processing.

There are exemptions from the provision obligation that might be imposed by member state laws (GDPR exemptions from the obligation to provide information, Data Privacy Manager, 2020):

1. Data subject already has information and data was gathered directly from an individual, this is not relevant to partitions of information that the individual is not aware of. In cases where data was gathered from sources other than individuals, a demonstration of an individual's awareness is necessary.

2. Data is subject to professional secrecy obligations regulated by Union or State Law.
3. In cases where the provision of information is impossible or invokes disproportionate effort to do so. This heavily relates to processing which purpose is archiving in the public interest, scientific or historical research purposes, or statistical purposes.
4. In cases where EU or member state laws are overriding the obligation.

Memphis should keep track of what information is being provided to individuals to not overlook any not provided information. Close attention should be paid to what member state laws are applicable and what laws industry laws regulating exemptions are in effect.

2.6 Security of personal data and reporting on breaches

The lack of proper security measures and protocols can lead to events of the unlawful flow of personal data across borders, data corruption, or loss which would have disastrous effects on the controller's reputation and will lead to fees, administrative or criminal punishment. Data protection and cybersecurity are not synonyms, but they have a lot in common which helps to apply privacy principles to completely different spheres. Appropriate security of personal data achieved by using technical and organizational means preventing unlawful processing, accidental or intentional loss, destruction, or damage is imposed by Article 5 (1(f)) of the GDPR. Controls are called appropriate in case an organization's security measures can deflect complex technological threats such as malware or denial of service attacks and other threats as well as correct and restrain negligent employee behavior or significantly reduce associated risks. Such controls should be determined by a risk assessment that takes into account the nature of personal data for processing. Measures against reasonable, foreseeable threats exploiting business or technological processes and vulnerabilities should be implemented. Requirements for Article 5 include an obligation of technical and organizational measures implementations appropriate to the level of security-

associated risks which is also affected by Article 32. Both the controller and the processor should understand the full extent of their processing operations under Article 30 and be able to demonstrate that their security measures are compliant with Article 24. Records of processing activities that fall under their responsibility including a general description of technical and organizational security should be maintained under Article 30(1).

Security of processing

Article 32 imposes the obligation of keeping personal data secure to which both the data processor and the controller are subjects. It also establishes four domains of security:

- Preventative security- actions taken to reduce the risk of security accidents and ensure confidentiality, integrity, and availability at the moment.
- Incident detection and response – actions taken to detect a breach if availability is compromised and reduce an impact including restoring availability in a timely manner.
- Remedial activities in reaction to risks and incidents – actions taken to restore functionality and security including actions aimed at strengthening security posture by testing and evaluation of controls.
- Data manipulation – pseudo anonymization which can be achieved by replacing information of data at rest that can be tied to an individual with an identifier for later reversal and use. Encryption is applied to data either at rest or at use allows secure storage or processing/transfer.

These requirements are met under ISO27001 compliance described in the second part of the thesis but other certifications and standards requiring less effort to achieve might demonstrate compliance with those requirements. Utilization of appropriate security controls, as well as proper documentation of such security measures, can also demonstrate compliance without the need for certification.

Article 32 confidentiality and employees

Article 32(4) of the GDPR is concerned with employee activities in relation to data under the controller's or processor's authority. Confidentiality in relation to data subject's personal data is expected as under Article 32(4) only actions within the boundaries of instructions are allowed. The controller's position should not be subverted. Risks associated with employee mistreatment of data or infrastructure is known as insider threat and it is the controller's and processor's duty to implement robust security policies informing employees of data handling responsibilities and make consequences of privacy policy violation clear. To reduce the rate and severity of unintentional data misuse, data controllers should provide employees with regular role-based training.

Measures such as network monitoring to detect data intentional or unintentional misuse or mistreatment should be implemented. The right culture profile and behavior in the workforce should be achieved using organizational measures which can be strengthened by the selection of competent, trustworthy, and reliable workers. That behavior, if not caused by deliberate corporate espionage, is mostly triggered by the unfair treatment of employees in an attempt to avenge the employer. Satisfaction screening and utilization of psychologist services might reveal such tendencies which further should be addressed to satisfy employee needs.

Relations between Controller and processor under Article 28

Security principles and measures should be followed all the way down the supply chain to subprocessors. Article 28 imposes obligations which are limiting the usage of processors to only ones that can provide sufficient guarantees of security measures. The relationship between controller and processor should be framed in a legally binding act containing necessary provisions.

Actions taken by Memphis to protect themselves from nonconformity to Article 28 include verification of the processor's compliance to core requirements of privacy. Check whether the processor suffered any high-profile security or privacy-related

incidents which would strengthen the supply chain. Consequently, checking whether the processor was/is subject to investigation due to breaches of data protection laws can be utilized as a part of the previous process. Identification of the processor's clients might provide insights into its reputation and trust from other organizations, security certifications check serves the same purpose. The processor's data protection and security framework revision might reveal privacy flaws that would trigger Memphis to address the processor with that issue. Conducting site inspections might be excessive but it also might be a part of processor risk assessment. Processor's audit documentation assessment might provide valuable insight into how the processor identifies and treats security issues which might play a significant role in the future. Identification of the supply chain and subcontracting processes of a processor and its impact on overall processing is a good practice of following all the way down the supply chain as noncompliance of one joint might result in compromise of the whole chain.

Communication and notification of Personal Data Breaches.

Breach notification is a transparency requirement spotlighting the operational failure of the organization to protect personal data. Benefits of such notice include possible damage and loss mitigation of affected people that can make efforts to protect their interests. The cause of a breach will become available to the public which can prevent similar incidents by reacting to new vulnerabilities by perfecting or creating new controls. Regulators are provided with the necessary data to perform supervisory activities. Under Article 4(12) personal data breach means a breach of security leading to the accidental or unlawful destruction, loss, alteration, or unauthorized disclosure of, or access to, personal data transmitted, stored, or otherwise processed. Requirements for data controllers to notify data protection authorities of data breaches are formulated in Article 33 and the requirement to notify impacted individuals is formulated in Article 34. The breach notification requirement is only triggered if the data controller is aware of a breach. Breach awareness measures are necessary for all organizations and are imposed by Article 5(1)(f). After a breach occurs and the controller becomes aware of it, the controller needs to determine whether the breach meets the

definition of a personal data breach. This should be done in a hasty manner as the controller has only 72 hours to notify individuals of a data breach after becoming aware. As soon as the controller has a reasonable degree of certainty regarding a breach happening in relation to personal data, he becomes legally aware.

Communication of data breach to data subject under Article 34 of GDPR. Controllers are required to communicate a personal data breach to the data subject if such a breach presents a high risk to the rights and freedoms of an individual. A severity threshold is present to identify whether notice should be provided to data subjects. Exceptions under Article 33(3) include:

- Cases where data was rendered unintelligible by use of encryption.
- Cases where the controller has taken steps to prevent high risks from emerging.
- Cases where breach disclosure would require disproportional efforts likely caused by an inability to identify impacted individuals. It is obligatory to announce that the breach has happened to a wide public.

Article 29 of the Working Party in WP250 guidelines outlines a framework for determining whether a breach should be reported. Likelihood and severity of risks should be considered with the controller including:

- Type of a breach.
- Nature sensitivity and volume of personal data affected.
- Ease of data subject’s identification based on affected data.
- Severity of consequences for affected individuals.
- Any special characteristics of affected individuals.
- Any special characteristics of the controller.
- Number of affected individuals.

Memphis should produce an incident response strategy which purpose is to provide employees with clear instructions on how to detect, classify and notify what is needed to be produced by the data controller. Utilization of the European Union Agency for Cybersecurity (ENISA) methodology for assessing breach severity is considered a best practice as it is recognized by authorities. This strategy might include an incident response plan, Incident playbooks tailored for specific roles, incident response team creation including their roles and responsibilities, and possibly Security Operations Center if an organization has resources to maintain it. Policy frameworks, controls, and Processes should be set out, documented, and maintained with extreme caution and attention to detail as it is a reference point for understanding the organization's approach to security and starting point of investigation or inspection by regulators. It should be noted that a significant period of time might pass between the breach happening and the controller becoming aware of it which might include significant changes in the operation of the organization, including its owners. Whoever is governing the organization's operation during becoming aware of a breach is responsible for the breach happening.

2.6.1 Employee data handling

Personal data of employees is being collected by an employer for reasons such as recruitment, salary, benefits, sickness records, monitoring, and appraisals. Also, data collection might be associated with employment laws obligations, and protection of employees. Both employer and employee have rights and responsibilities under the data protection framework for the processing of personal data.

Legal grounds for employee data processing.
An employment contract includes an agreement of employees for the employer to use their personal data, but it should not be mistaken for consent to the processing as it has a relation to the contract. Such an agreement is not valid for data protection law. Grounds for employee data processing under GDPR Recital 155 include:

1. Consent from the employee
2. Employment obligations fulfillment.
3. Legal obligations fulfillment to which employer is subject.
4. Employer's legitimate interest.

Memphis should explicitly ask for consent of personal data processing as it provides the most effortless and comprehensive way to comply with regulation.

Providing notice

Under Articles 12, 13, and 14 organizations need to provide appropriate notice of data usage, purposes of the processing, query contacts, and rights in relation to their data exist regardless of lawful grounds used for processing.

Memphis can deliver notice via an employee handbook or specific notification document provided to new employees and should be accessible on request, for example in booklets or intranet. Such notice should be maintained and in case a new purpose is added employees should be notified. An appropriate level of detail for employees to understand the legal basis of processing, purpose, the legitimate interest of an employer, grounds of processing, where data will be transferred and the retention period of data should be provided in a notice under GDPR.

Personal Records Storage.

From the moment of application, the employer starts to collect various employees' personal data. The retention period of those records should not exceed necessary under the GDPR Article 5 which means the period when the employee is part of an organization is deemed legitimate but as soon as an employee leaves the organization data must be deleted indefinitely. In case an organization might need to store data of employees that left the organization, legitimate grounds to do so should be identified and executed.

Memphis, if it intends to keep the data after an employee leaves, should notify the employee and include it in the working contract. Reasons for keeping that data might come from disproportionate efforts for deletion from documentation in use produced by an employee or in case an employee might re-employ to justify previous employment and ease the onboarding process.

Workplace monitoring and data loss prevention

Background checks of existing and potential staff are a widely used mechanism for preventing access to data of unscrupulous and untrustworthy employees. Monitoring can contribute to this purpose by not possibly stopping malicious deeds but by collecting evidence. Data loss prevention is mainly achieved with technical tools such as software solutions, backups, or network flow monitoring. Company emails may be used by employees for personal communications or on the contrary private communications can be used for organizational purposes. Such acts should be prevented by Internet policy regulating purposes of and means of communication at the workplace. Under Article 29 of the working party, employees should be aware of monitoring or surveillance in the workplace as well as of reasons and purposes. (fieldfisher, no date) Any enforcement procedures should include how and when employees will be notified of policy breaches and given the capability to respond to claims. Intrusive monitoring is considered unlawful and monitoring collecting sensitive personal data is very hard to justify. Covert monitoring or surveillance is unlawful unless prior permission is obtained from regulatory authorities, or an exception is applicable.

Memphis as well as most of the other companies that care about the security of data assets do monitor traffic and emails. Although the purpose of monitoring might be pointed towards prevention of attacks, including social engineering and network worms, employees should be notified anyway, monitoring policy should be produced and distributed. It is recommended that the email monitoring policy should determine the following criteria:

1. Whether work email utilization for personal needs is permitted to the employee.
2. Conditions of access to worker's email client data from the organization.
3. Retention period and justification of messages backup.

Internet traffic monitoring policy should determine the following criteria:

1. Involvement of employee representatives.
2. Whether access to certain sites is blocked should be considered.
3. Whether the amount of time that an employee is spending at the internet is tracked should be considered.
4. Clear purposes and conditions of internet usage.
5. Misuse of the internet should be notified immediately as the organization becomes aware of it.

Caution is needed when an employer detects misuse of the internet as websites may be visited unwillingly by unclear hyperlinks or mistyping, no hasty conclusions should be made. Facts should be presented to the individual with an opportunity for an explanation from the employee's side. In some cases, representatives or work councils can be involved in the investigation.

Bring your own device.

The practice of employees utilizing their own devices for work became a popular way of saving funds on equipment and providing employees with a comfortable and known environment for their work. Work email accounts incorporated in employee's phones, now intended for both personal and professional use alongside other work instruments pose data protection compliance issues as a responsibility to keep clients' personal data safe remains.

Organizations implementing BYOD policies should have:

- Established BYOD policy explaining how employees should use BYOD devices and what are their responsibilities.

- Set out clear rules for the storage of personal data processed on the phone as well as measures taken to ensure security which might include the utilization of company portal application, encryption and self-encrypting drives, usage of separate work instances, and minimal password requirements.
- Ensured safe transfer mechanisms from and to a device to avoid sniffing or data tampering in transit.
- Established policy regarding data stored on devices of employees who are no longer part of the organization. What measures should be taken regarding stolen or lost gadgets. Usually, those measures include the deletion or blocking of all work files on the device.

Some employees when using their devices for work tend to not be satisfied with the monitoring and try to protest this decision even though it has a security-only orientation. Memphis cannot enforce monitoring on the devices of their employees but can incorporate this requirement into the working contract as a potential workaround for this issue. Boundaries of monitoring on employees' devices should be clearly established and conveyed. Such boundaries should not exceed business interests.

2.6.2 Surveillance

With technological advancement more and more data is available for surveillance at organizations' disposal. Surveillance involves observation of an individual or group of individuals in a covered or open manner, conducted in real-time or by access to stored materials. Surveillance activities can be grouped based on the source of surveillance data:

- Video surveillance

The use of video surveillance must be proportionate to its purpose and have a legitimate basis. CCTV should be adequate and not excessive in relation to solving addressed security problems. If an organization wants to secure its facility it is not adequate to place cameras in zones of high privacy expectations such as

toilets and changing rooms. When implementing CCTV, it should be determined whether a position revealing an individual's identity is necessary as well as options to minimize intrusion to monitored individuals under minimal data collection requirements. It should be considered if CCTV footage will be combined with other information for identification purposes as well as the need for disclosure to third parties if needed, requests from authorities such as police should be executed. The retention period of CCTV should not exceed purpose requirements. Access to CCTV recording under usual circumstances should be limited to security employees. Data subjects should be aware of monitoring. This can be achieved with informational signs within a reasonable distance from the monitoring area. Data subjects should have access to footage on request. (5 Step Guide to Check if Your CCTV is GDPR Compliant, Data Privacy Manager, 2021)

Memphis is utilizing CCTV. Cameras should be placed in most security-sensitive areas such as the production line, research and development department, corridors inside the building, and possibly at the entry and exit with signs informing CCTV usage. The usage of CCTV should be mentioned in the privacy notice alongside with purpose of increasing security and details of DPO and equipment storing the footage should have access limited only to security employees. Memphis should prepare to share the footage with authorities such as police on request.

- Biometric data

Personal data relating to the physical, physiological, or behavioral characteristics of an individual which can be used for identification is called biometric data. Fingerprints, voice, handwriting, face, retina, and blood vessel structure of hands are all examples of biometric data. It is important to understand that collection of biometric data can only have identification purposes under Article 9 of GDPR. Although if it is used solely for permitting access to location requirements under Article 9 do not apply. The controller should verify that no additional obligations are imposed by national law before proceeding to the collection.

Memphis is utilizing biometric identification to authorize access to doors thus it is possible to collect such data. This, however, should be included in the privacy notice including the purpose of collection provided. Security measures should be implemented to ensure the safety of stored biometric data.

- Location data

Location data has a lot of implications regarding various services starting from social networks to emergency services. Usually, location data is based on the GPS location of a mobile device but technical solutions such as RFID tags or credit cards are also a source of such data. Under GDPR location data is known as an identifier as it can only be used to identify an individual in conjunction with other data therefore it is considered as personal data only under this condition. Although informed consent and legitimate purpose identified and provided are needed in any case to collect location data. Location data provides a variety of service utilities but also can lead to severe risks of stalking and other malicious activity. Thus, app developers and other controllers should consider the necessity of location utilization due to high risk and conduct a DPIA assessment. In an organizational context companies might use location data to track their fleet of vehicles or devices. But the fact that the location of a device or vehicle is the same as the location of a device handler or driver makes location data personal data. (Meyer D., 2018)

Memphis does not collect any location data, but if it did, employees should have been made aware of it. The purpose of safeguarding the organization’s property should be stated. As location data is tied to terminal equipment or other property and responsibility for that particular property by an individual is documented attention should be exercised not to combine those data sets as it would produce personal data.

2.7 Accountability

The data protection legislation framework has incorporated GDPR requirements of accountability. Accountability in the scope of this thesis's interests means various obligations organizations must execute to show compliance with the data protection framework. Article 5(1) lists six principles of personal data processing that were discussed previously:

1. Lawfulness
2. Purpose limitation
3. Data minimization
4. Accuracy
5. Storage limitation
6. Integrity and Confidentiality

In addition to those principles Article, 5(2) introduces the obligation of the controller to demonstrate compliance with those six principles. This can be achieved through various elements such as the Approved Certification mechanism described in Article 25 which brings up the following factors safety of which should be addressed by the implementation of technical and organizational measures:

- Scope of the processing
- Nature of the processing
- Context of the processing
- Purpose of the processing and risks for rights of data subjects
- State of Art
- Cost of processing implementation

Article 24(1) furthers accountability requirements by imposing demonstration obligations for those aspects. Technological measures for those requirements include:

- Minimization of processed data.
- Pseudonymization

Memphis in pursuit of accountability demonstration should consider the following areas:

1. Internal policies

   Basic principles of data processing and handling are outlined by internal data protection policies. The policy should not only reflect principles described in Article 5(1) but also include information about subjects of policy and related processing activities, commitment to the organization's position regarding data processing, including collection and processing purpose as well as legitimate business purpose. Internal policies should reflect the scope, policy statement, responsibilities of employees, responsibilities of management, incident reporting, and policy compliance. Policies should also include non-compliance consequences associated with local employment laws and employment termination.

   Employee responsibilities
   In addition to the responsibilities stated in the Employee data handling chapter employers should take all reasonable actions to prevent unauthorized access or loss of personal data. Employees should understand the steps of international data transfer as well as the proper process of personal data destruction.

   Management responsibilities
   Policy regarding management responsibilities should include the following details:

   - It is senior management's responsibility to assess business risks associated with the processing of personal data.

- Senior management should work on the development of procedures and controls for the identification and appropriate treatment of risks.
- Senior management should clearly allocate responsibilities to employees in order to determine risk-based technical physical and administrative security measures for personal data protection and establishment of procedures and requirements for international data transfers.

2. Training

Training programs about data protection obligations should be created by the controller. This requirement is regulated by Article 39 which imposes DPO to monitor compliance with GDPR including Article 47 which requires appropriate data protection training for employees with access to personal data. Those programs should be flexible in regard to various positions within the company. Documentation and observation of training program implementation is considered as a part of accountability demonstration. Reminders of data protection obligations to employees help organizations to stay accountable.

Memphis should produce such training by themselves or seek help from DPO. Training is crucial for proper data handling and breach reporting, and it should not be overlooked. Memphis should collect evidence of training creation and/or conduction to be able to demonstrate accountability.

3. Incident reporting

It is required for all employees to immediately report all incidents of data loss, corruption, unauthorized access, communication, disclosure, or inappropriate use. Steps describing employee activities in case of an incident should be reflected in the policy or operational documentation. All significant breaches should be reported to the supervisory authority within 72 hours starting from the moment of becoming aware of an incident. The involvement of employees from various departments in incident response teams is recommended to avoid bias as well as members and roles of the internal

investigation team and breach reporting team should be reflected in the policy.

4. Data Processing Impact Assessment (DPIA)

During the planning and development of new products and services organizations should consider data protection-related issues which might arise with these new products. DPIAs help to identify such issues so companies can minimize or completely prevent privacy issues. Incorporation of these methodologies into project management and risk management schemes is considered best practice. Organizations considering the necessity to conduct DPIA should ask the following questions regarding new products or services:

- Does processing involve any high risks?

  Situations of high risks include systematic and extensive profiling that generates legal efforts or has an effect on data subjects or processing involves special categories of personal data on a large scale. Also, CCTV or other video surveillance of public spaces on a large scale is considered high risk. More detailed information about risky processing is provided by Article 29 of the Working Party. (iaap, no date) DPIA would be considered necessary if at least two criteria from the list of the Working Party are met.

- What if processing involves high risk and assessment is required?

  It is recommended to seek DPO help with DPIA conduction. DPIA conduction is subject to the obligation of Article 35(7) which states that at least one of the following criteria should be documented in DPIA.

  - Systematic description of developed processing including the purpose and legitimate interest of the organization.
  - Proportionality and necessity assessment regarding the purpose of processing.

- Rights and freedoms risks of data subjects associated with processing should be assessed.
- Security and safeguard measures implemented to ensure the protection of personal data.

It should be determined in each case whether it is necessary to seek the opinion of affected individuals on the stated purpose under Article 35(9)

- What if the processing is still high risk after measures are taken?
  If implemented measures are not reducing risks, then consultation with the data protection authority is required before continuing the development of goods or services.

  Memphis is collecting and processing sensitive health data thus DPIA should be implemented in all processes which involve health data to determine and address privacy risks. The help of external DPO should be utilized for unambiguous and globalistic help as Memphis has branches in various jurisdictions.

5. Data Protection Officer (DPO)

   DPOs are organizations specializing in assisting other organizations in the protection of personal data in general or specific fields. DPOs are monitoring the organization's compliance with GDPR and company data protection policies including internal data protection activities management, employee training as well conducting internal audits. Advise on DPIA-related issues and monitoring of performance. DPOs ensure that the organization is cooperating with supervisory authorities. Acts as a point of contact for processing and other issues to supervisory authorities. The compliance framework that an organization creates is best to be oversighted by an independent DPO as services provided can save millions of euros on fines if something was overlooked by an internal team. The role of DPO can be assigned to an employee within an organization or to a third-party organization. (Appendix

1.) DPO designation obligation is imposed by Article 37. It is not mandatory for every company to appoint a DPO unless stated otherwise by a member state law or if the criteria for appointment are met which include:

- Processing is carried out by the public authority.
- Regular and systematic monitoring of individuals on a large scale is considered a core activity of a company.
- Special categories of personal data are processed by the company and considered a core activity.

Memphis should assign DPO for reasons stated in the DPIA obligation part, to comply with the state laws if they impose DPO assignment, and to seek help with treating sensitive data as well as other privacy issues.

2.8 Data transfers

Data transfer requirements are not defined in the GDPR; however, it is established that transit is not just data transportation to another country, it is eventual processing that completes and qualifies it as the transfer.

One of the stated GDPR objectives is to allow the free flow of personal data between member states on agreed terms of personal data protection. In many cases, personal data should be transferred to third countries for processing. Under Article 46 of the GDPR transfers outside of EEA may only take place under the conditions of:

1. Ensured adequate level of personal data protection as determined by the European commission.
2. In case of lack of that protection, the controller or processor executing the transfer should provide adequate safeguards for data subject rights protection.

3. In the absence of safeguards stated in part 1 or part 2 transfer should fit within one of the derogations for specific situations covered by GDPR.

The same conditions apply to international organization transfers.

Providing adequate safeguards.
Adequate safeguards under Article 46 include: binding corporate rules, legally binding and enforceable instruments between public authorities, standard data protection clauses adopted by the EU Commission or supervisory authority, approved code of conduct, and approved certification mechanisms. Under supervisory authority oversight organizations might use contractual clauses for data transfers.

Transfers on the basis of an adequacy decision.
Preapproved by the Commission under the Directive, this mechanism is most frequently used to validate international data transfers. The European Commission recognized Andorra, Argentina, Canada, Faroe Islands, Guernsey, the Isle of Man, Israel, Japan, Jersey, New Zealand, Switzerland, Uruguay, and the United Kingdom as countries providing adequate protection. (Adequacy decisions, no date) Memphis does have a branch in New Zealand and transfers fit into this category.

Data transfers using Binding Corporate Rules (BCRs).
International data transfer in accordance with EU laws is possible for multinational organizations or within corporate groups available for both controllers and processors. Requirements for BCR transfers under Article 47 include:

1. Internal and external legally binding nature
2. Structure and contacts of the corporate group and each member included.
3. Means of noticing data subject of BCR details.
4. Complaint procedures.

5. Appropriate data protection training for employees with permanent or regular access to personal data

Approval criteria for these requirements are further clarified in WP 256 for controller BCRs and WP 257 for processor BCRs and later will be the subject of inspection by supervisory authorities. Memphis has a branch in Bulgaria and transfers conducted to that country after seeking help from DPO should follow the requirements stated above.

Derogations

If an adequate level of safeguards is not met international transfer may still be possible on condition of fitting with one of the derogations under Article 49. Such derogations are applicable in specific situations covered in GDPR which include:

1. Explicit consent to the proposed transfer after notice which includes information regarding risks associated with transfer due to the absence of adequacy decision by the European Commission and appropriate safeguards.
2. Necessity to execute contractual obligations between the data subject and the controller. Implementation of pre-contractual activities by the data subject's request is also applicable.
3. Transfer in public interests.
4. Establishment, exercise, or defense of legal claims

In addition to the situations stated above, derogations include vital interest in cases of an individual needing medical attention requiring health records abroad and public registers. Information acquired from public registers is subject to international transfer on condition of the recipient's compliance with any restrictions concerning transferred data. It should be noted that only parts of registers are allowed to be transferred, not the whole register. Conditions imposed by the register's creator should be honored by the importer and recipients. (Guidelines 2/2018 on derogations of Article 49 under Regulation 2016/679, 2018)

Memphis might use BCRs for transfers to potential processors. Data transfers are very sensitive and might invoke serious legal consequences thus it is recommended to seek help from DPO.

Not repetitive transfers

Not repetitive transfers act as a last resort option under derogations if any other case is not applicable. As the name implies, such transfers are not meant for regular use due to the exceptional nature of such transfers.

Criteria for not repetitive transfers under Recital 113 of GDPR are:

1. Transfers do not repeat.
2. Only a limited number of data subjects is concerned.
3. Is necessary for completing the controller's legitimate interests which do not override the data subject's interests and rights.
4. Circumstances concerning transfer are assessed and data protection safeguards are implemented based on the assessment.
5. Data protection authority and data subject are informed of the transfer including the provision of purpose notice to the data subject.

If Memphis faces the necessity to transfer data to third countries and no other variant is applicable, repetitive transfers might work once. Safeguards should be implemented and the data protection authority informed and consulted with, data subjects to whom data is being sent are informed as well as help from DPO is utilized.

Transfer Impact Assessment

International transfers outside of EEA with a basis of Contractual Clauses (SCCs) and Binding Corporate Rules (BCRs) require an assessment of the recipient country's adequacy of personal data protection. Clause 14 specifies assessment in the form of Transfer Impact Assessment. TIA conduction under European Data Protection Board's methodology includes (White B., 2022):

1. Know your transfers – transfers should be mapped and recorded, including known future transfers. The nature of data identification means establishing data of authority's interest and destination of data.
2. Transfer tools under Article 46 – Adequacy identification, Article 46 tools identification (SCC, BCR, code of conduct, Certification mechanism, ad hoc clauses), Derogations identifications if applicable.
3. Effectiveness assessment – Utilization of publicly available legislation of a third country to determine effectiveness level.
4. Supplementary measures adoption- implemented if the third step showed a lack of effectiveness. Organizational or contractual measures taken to close the gap.
5. Probability and severity of individual harm assessment – assessment of data subject's rights mechanisms availability.
6. Procedural step – Implementation of tools determined in steps 3 and 4. Do not conduct transfer if there is a lack of such activities.
7. Regular re-evaluation – monitoring of the data protection landscape in the third country to ensure the effectiveness of tools.

Transfer impact assessment is a sensitive and complicated privacy mechanism, Memphis should consult with DPO and data protection authority on its conduction. Related documentation should be produced and stored to have evidence of conduction in case data protection authorities will audit transfers. Re-evaluations should be conducted periodically to ensure compliance and effectiveness as well as to reflect changes in both jurisdictions.

Codes of conduct and certification mechanisms

Codes of conduct and certification mechanisms acting as adequacy mechanisms are a novelty to GDPR. Guidelines on codes of conduct and monitoring bodies for clarification of procedures and rules as well as certification bodies under Article 43 are provided by EU Data Protection Board. BCRs are an example of codes of conduct that help to demonstrate high standards of privacy. (Appendix 1.)

Transfers to the United States

A “Privacy Shield” developed by the US Department of Commerce and the European Commission serves as a self-regulatory framework allowing organizations to satisfy strict EU data protection laws and thus allowing transatlantic data transfers. Privacy shield stands on 7 principles such as:

1. Notice - Individuals must be informed of their personal data collection and processing. Contacts of the organization should be stated for inquiries and complaints.
2. Choice - Individuals should have the option to opt-out.
3. Accountability for the onward transfer - Only organizations following adequate data protection principles may further receive personal data.
4. Security - Reasonable efforts are in place to prevent data loss.
5. Data integrity and purpose limitation – relevant and reliable data for collection purposes.
6. Access – Individuals should have the ability to access their personal data, correct and delete it.
7. Recourses, enforcement, and liability- Effective means for enforcement of those principles should be in place.

Although privacy shield is invalidated at the moment due inability to protect the personal data of EEA subjects from US Governments surveillance laws it is important to understand the backbone of Privacy Shield as new legislation known as the Trans-Atlantic Data Privacy Framework is being developed having mostly the same principles. (Trans-Atlantic Data Privacy Framework, 2022)

Memphis should prepare for new legislation but at the moment BCR is the most appropriate variant for transfer. As with other transfers it is recommended to seek help from DPO and consult with the data protection authority.

3 ISO27001 STANDARD

ISO27001 is a world-know information security standard created by the International Organization for Standardization (ISO). This standard governs Information Security Management System's planning, implementation, operation, monitoring, and improvement. ISO 27001 is intended for organizations of all types and sizes. In comparison to other security standards, ISO27001 provides a flexible and risk-based approach that gives an organization and any third-party satisfactory expectations of security management. Besides that, ISO27001 provides a plethora of other benefits including new contract perspectives, possibilities to stand out of the crowd and enter new more security-sensitive spheres and provide sufficient proof of implemented security measures to regulatory authorities. Organizations should consider the necessity of ISO27001-compliant ISMS implementation as mostly it is implemented by business necessity such as contracts bidding or legal obligations such as ones imposed by public sector frameworks. (Appendix 1.) It is important to understand ISMS implementation at the early stages of implementation because of the interconnectivity of processes. As certification is the main goal, collecting documentation for the demonstration of compliance is vital. The collected documentation should be presented to the certification body as evidence. It should be noted that ISO is not responsible for certification, third party with accreditation should perform certification audits. Refer to Figure 5 in Appendix 2 which demonstrates the key implementation and operation processes as well as the documentation required for certification for orientation during the implementation process.

3.1 ISMS

ISMS is a set of technological and processual policies and procedures intended for the systematic management of security within an organization which is mainly focused on the security of sensitive information and business continuity. ISMS is a security framework used for the identification, assessment, and management of information security risks to address the Confidentiality Integrity, and Availability

(CIA triad) of an organization. ISMS is ensuring that security measures are up to date with the present vulnerability and threat landscape with regard to infrastructure used by an organization in a fine-tuned manner. After implementation, ISO 27001-compliant ISMS ensures achievement of information security objectives and continual improvement by consequently assessing risk, creating, and implementing a risk treatment plan to lower the risk, and monitoring of ISMS metrics to evaluate the effectiveness of the risk treatment plan and create a basis for the next risk assessment. All those core processes are further audited to ensure their compliance and effectiveness which may possibly lead to corrective actions to fix or improve those processes as illustrated in Figure 1.

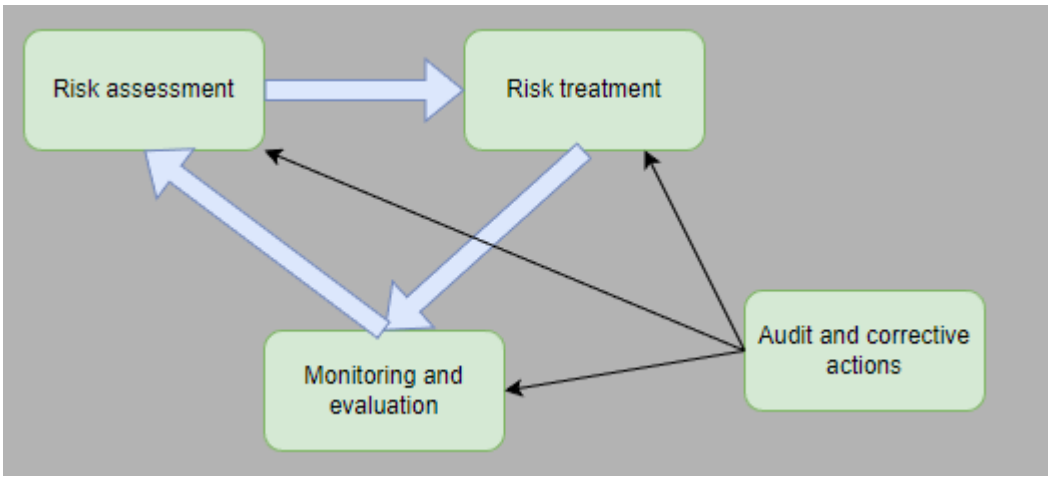

Figure 1. How core processes operate, audited, and improved.

This approach guarantees that the controls implemented within the ISMS framework are relevant to contemporary and possibly to new threats and provides correction possibilities in case any of the core processes are ineffective.

3.2 Organization context

Under ISO27001 requirements organizations should determine internal and external issues relevant to the purpose of the organization and that affect the achievement of intended outcomes of ISMS. Internal issues are factors under the control of the organization and external are one's organization has no control over. Internal issues include organizational structure, business drivers,

processes, resources, and contractual relationships. External factors are generated by the environment in which an organization operates such as market and technology trends, values, and their perception by external interested parties, laws and regulations, political and economic environment. (Leal R., 2022)

All those issues produce a plethora of factors that define how an organization operates and it is extremely important to identify those issues and adapt your ISMS accordingly otherwise a so-called “Concrete lifejacket syndrome” might happen, a situation where ISMS is effective in the plan but fits business and environment so poorly it provides more disadvantages and costs than benefit. Another issue that is typically a part of the previous problem is “ISO in name only”, it happens when an organization formally follows all requirements but does not integrate ISO-compliant processes in its business-as-usual operation. One of the possible sources of that issue is that employees trying to execute their responsibilities but poorly fitted ISMS forces them to bypass ISO-compliant processes. Security by point of view of an employee applies boundaries and obstacles, rules too strict may inflict previous problem. Often departments with rules too strict would address that issue and it is crucial not to overlook such problems as it will form noncompliant “shadow departments” and review security measures and approaches in general. (Appendix 1.)

Under ISO 27001 requirements, interested parties and their needs and expectations including legal and regulatory should be determined. Interested parties or stakeholders can be identified using stakeholder analysis and might include the executive board, shareholders, insurance companies, customers, and regulators. Stakeholder’s requirements concerning ISMS could be asked directly or derived from the nature of a stakeholder but most often it is directly linked to how effectively ISMS protects itself and sensitive data from cyber-attacks, regulatory and legal breaches, how the organization stores and processes information. (The Ultimate Certification Guide To ISO 27001:2022 Clause 4.2 Understanding The Needs And Expectations Of Interested Parties, Hightable, no date)

Under ISO 27001 requirements organizations should determine the scope of ISMS including aspects of organizational context issues, requirements of interested parties, interfaces and dependencies between internal and external processes. What parts of organization ISMS should be implemented is defined by the scope of implementation that organizations wish to implement, it can address only a department or a whole organization. Decisions on scope should be produced by senior management as they possess a broad perspective of the organization's processes and structure. During scope definition, it is recommended for senior management to take into account the experience of ISMS implementation of staff and consider the worthiness of starting implementation with one business unit as it might provide invaluable experience for further implementation or over-complicate the process due to interconnectivity or other reasons. A cautious risk/reward review should be conducted. (Appendix 1.) Dependencies and access points of processes inside the organization should also be contemplated for smooth ISMS integration purposes.

A scope statement should answer the following questions:

- What is the nature of a business? What does the company produce or what services does it provide that need protection?
- What data or services require protection?
- What are processes or means of processing associated with that data that might be targeted?
- Are there any exceptions for the scope within the organization?

This statement should be formulated in a couple of sentences with clear and precise wording. All exceptions should be considered as they would fall out of standard context and thus be deemed unsafe. (Compleye, no date)

3.3 Leadership

Leadership requirements are intended to enforce the management support of ISMS improvement and operation and are subject to close inspection by certification audit. To determine the security leadership team overviewing ISMS implementation a management review team consisting of senior representatives from each department should be created.

Under ISO27001 those requirements are:

a. Ensuring the information security policy and the information security objectives are established and are compatible with the strategic direction of the organization.

   General Security policy and security policies corresponding to business needs and risks should be formulated by senior management. These policies should reflect risks determined in risk assessment and correspond to documents created during organizational context contemplation. It is extremely important to treat ISMS implementation as a business project thus the management team responsible for high-level planning should not include IT security employees.

b. Ensuring the integration of the information security management system requirements into the organization's processes.

   Documentation of processes including documentation mark-up and version control should be created. It is important to incorporate at least one backup plan in case some process will not work or would go not as planned. For example, If any update fails the previous version should be loaded from a backup server, if a worm is not quarantined and continues to spread then a network branch should be isolated. Those aspects should be reflected in an appropriate security policy. (ISO27001 Clause 5.1 Certification Guide | Leadership And Commitment, HighTable, no date)

c. Ensuring that the resources needed for the information security management system are available.

Available, well-allocated, and engaged resources have a crucial role in successful ISMS implementation and certification. Resourcing includes not only funds needed for the purchase of software/hardware needed for controls but also competencies to implement those controls. A specialist's help can significantly reduce the costs of implementation as many mistakes are avoided thus less time is wasted. If a contractor is not an option, then investing in your existing staff might be needed. Certifications of auditor or implementor will greatly increase implementation productivity and will bring confidence in the security team. (Calder A., 2017) An accountability matrix aligning appropriate competencies to security controls stated in Annex A should be created to document the responsibility and allocate competency resources across the ISMS. In case a third party is implementing changes to ISMS responsibility still should be assigned internally. (ISO27001 Clause 5.1 Certification Guide | Leadership And Commitment, HighTable, no date)

d. Communicating the importance of effective information security management and of conforming to the information security management system requirements.

Communication should be established among all levels and appropriate media and thus making it easy to demonstrate to the certification body. Incorporating effective information management responsibilities into contracts is one of the approaches to comply with those requirements. Personal responsibility for the proper functioning of a part of ISMS should be communicated to individuals for stimulation purposes. Implementing Information Security Awareness and Training policy which would incorporate details about training such as training tools or quizzes will be extremely beneficial for compliance demonstration. It should be noted that training frequency should also be included. Different departments and teams have different impacts on security and company assets thus some teams might need more training than others, but it is recommended to conduct at least

one basic security awareness and data protection training annually for everyone. A communication plan should be created describing the topic, sender, receiver, content, and approach to communications for a year. This documentation should greatly benefit compliance demonstration. (ISO27001 Clause 5.1 Certification Guide | Leadership And Commitment, HighTable, no date)

e. Ensuring that the information security management system achieves its intended outcome(s).

   Objectives settled out by senior management are subject to review by the Management Review Team which can ensure objectives achievement by supporting the implementation of security management processes. Report requests and review on implementation, monitoring, and evaluation is also considered solid demonstration of that requirement. Reports may include ISMS performance measurements, audit reports, and management feedback. Setting performance goals for teams/key competencies within the ISMS team may also contribute to the demonstration of this requirement. (ISO27001 Clause 5.1 Certification Guide | Leadership And Commitment, HighTable, no date)

f. Directing and supporting people to contribute to the effectiveness of the information security management system.

   Feedback from management on the effectiveness of the ISMS implementation should be correlated to the organization’s strategic development plan, and based on that prioritized implementation activities should be identified. A properly populated and up-to-date Competency matrix, Information security Awareness Policy, and Communications plan will provide a sufficient demonstration of contribution support. (ISO27001 Clause 5.1 Certification Guide | Leadership And Commitment, HighTable, no date)

g. Promoting continual improvement.

Continual improvement budgeting planning should be considered during management feedback as well as setting objectives for further development. Policy deviations as well as incidents and unexpected events will inevitably happen after ISO certification. All those situations should be addressed and managed as annual certification will closely inspect this aspect as continual improvement is one of the main principles of ISO certification. (Calder A., 2017) The continual improvement policy states how your organization will handle all those events meanwhile Corrective Action log will collect all instances of continual improvement thus providing a demonstration of compliance with this requirement. A communications plan may also aid in this requirement as the annual plan provides a review point for promotion activities. (ISO27001 Clause 5.1 Certification Guide | Leadership And Commitment, HighTable, no date)

h. Supporting other relevant management roles to demonstrate their leadership as it applies to their areas of responsibility.

Top management should provide support to medium-level management leading ISMS implementation within their responsibility area. In cases of an organization that improves ISMS being a part of a bigger organization often leads to leadership improvement due to increased communication with the bigger organization. Leaders of bigger organizations would provide support to management within the scope of the ISMS. This may be in the form of resource allocation aligned with ISMS needs. (ISO27001 Clause 5.1 Certification Guide | Leadership And Commitment, HighTable, no date)

The competence matrix created by the senior management in the Management Review Team sets out a correlation of competencies and security needs thus providing encouragement, support, and structure to medium management. The communications plan also includes management communications to other employees thus those two documents provide a sufficient demonstration of compliance. Failure to comply with this requirement will trigger skepticism regarding certification worthiness and will lead to a more in-depth inspection.

Leadership commitment can be demonstrated not only by providing documentation on ISMS management decisions but also by actively participating in processes involving certification bodies such as participation in annual external audits. (ISO27001 Clause 5.1 Certification Guide | Leadership And Commitment, HighTable, no date) Senior management and executives are focused on business processes, and most don't pose security knowledge in case ISMS implementation is mandatory, they see it as a burden to just comply with and move on thus undermining the importance of ISMS and their input into it. Implementors seeking the attention of leadership on ISMS should start "talking business language" by providing information on how it would benefit business not security. Arguments might include not only compliance but also marketing, cost-cutting, simplification, and optimization of business processes. (Kosutic D., 2017)

Security policy

Security policy is a high-level documented statement of strategic importance for ISMS. Security requirements of an organization are incorporated into security policy in a brief high-level and general manner as a more in-depth description of processes is provided in separate policies which would be described in this chapter later or in operations documentation. Those policies should be aligned with general security policy Information.

Requirements under ISO27001 to top management establishing security policy are:

a) is appropriate to the purpose of the organization.

   Security policy is specific to the ISMS scope of your organization but can exceed those limits. The security policy should reflect organizational issues, culture, and strategy.

b) includes information security objectives or provides the framework for setting information security objectives.

Setting objectives includes how those objectives are proposed, approved, and reviewed. Objectives criteria should include details about how to measure those objectives and other relevant information.

c) includes a commitment to satisfy applicable requirements related to information security.
d) includes a commitment to continual improvement of the information security management system.

The last two requirements can be fulfilled by including a management commitment statement in the policy. That will provide sufficient demonstration of compliance during audit.

The information security policy should also:

e) be available as documented information.
f) be communicated within the organization.

Security policy alongside other policies can be stored on the intranet and guided to during the onboarding process.

g) be available to interested parties, as appropriate.

Those parties usually include customers, suppliers, and certification bodies. Implementation of policy ownership is considered best practice as it will impose the responsibility of keeping policy up to date and proper distribution.

Security policy is a general security statement but when it comes to describing processes it has little applied worthiness thus more specialized policies should be introduced. It is recommended to separate the security policy from other policies rather than combing all documents together. This approach will ease keeping documents up-to-date and separate responsibilities of maintenance among employees. (ISO 27001 Implementation Guideline Clause 5.2 Policy, info-savvy, no date)

Organizational Roles, responsibilities, and authorities

Under ISO27001 5.3 clause top management should determine responsibilities and authorities for information security roles associated with ISMS requirements and communicate them to employees. Roles reporting to top management regarding ISMS implementation evaluation and improvement should also be identified. It is recommended to periodically review how roles and associated responsibilities with authority align with ISO requirements and reflect the competency matrix. It should be noted that top management is not required to set all information security roles related to ISMS in an organization as this authority can be delegated to major roles. It is important to include people from key parts of an organization to conduct an understanding of whose interests those people should look out for. Seniority and competency should vary across the matrix according to complexity of assignment. As already stated, the competency matrix discussed before with the communications plan should provide a sufficient demonstration of compliance. The top management should consider adding these activities to the competency matrix:

- Coordination of Implementation, improvement, maintenance, monitoring, and reporting of ISMS.
- Risk assessment and treatment counselling.
- Security processes and system design.
- Controls standard setting and operation.
- Security incident management.
- ISMS review and audit.

(ISO 27001 Clause 5.3 and Clause 7.1 Resources and Roles & Responsibility, info-savvy, no date)

Necessary roles are not identified in the standard but for ISMS implementation to be efficient it is recommended for senior management to contemplate the following positions:

Information security manager

It is recommended to appoint an information security manager to create an ISMS team. This approach is faster and simpler compared to board team creation. It is not only creating a strategic and day-to-day responsible role but also this role can execute duties for both ensuring ISMS reaches standard requirements and reporting of ISMS performance to top management. (Calder A., 2017)

The lead risk assessor

In relation to who should lead, and coordinate risk assessment two aspects should be considered. Standard imposes that risk and control reviews should be conducted periodically reflecting changes in vulnerability and threat landscape. The effect on business from various environments should also be assessed. The second aspect is derived from the necessity to assign qualified specialists with sufficient experience. During the audit qualifications of key individuals will be questioned and adequate documental proof should be demonstrated. Certifications or proven previous experience with ISO 27001 are examples of qualification compliance demonstration. (Calder A. Watkins S., 2019)

Specialist in information security advice and training.

Detailed, timely, and accurate advisory considering both business and IT aspects of the ISO 27001 implementation project would be needed throughout the whole process. Threats, control implementation, and other security aspects would require a specialist with comprehensive knowledge of the organization.

Therefore, two options to fill this position exist:

1. The first one is to appoint existing IT employees and ensure adequate training.
2. Hire an information security manager with adequate technical training.

Recruitment of people with such high competency should be a priority in large organizations. Most likely this person would lack information security management standards and additional specific training would be needed by

International Board for IT Governance Qualifications Accredited Training Organization. (Calder A., 2017)

IT security practitioners

IT security practitioners include networking specialists, administrators, security analysts, and others relevant to security IT employees are responsible for control implementation. That group should have appropriate certifications including security and technical training. (e.g., CISSP, CCSP, CCNA,) IT security practitioners are responsible for keeping infrastructure protected against new threats by contributing to risk assessment processes and updating it from a security point of view if the infrastructure is expanding or changing. (Calder A. Watkins S., 2019)

Functional competencies

Leaders of IT units, HR head, risk assessment and management experts including risk owners, physical security personnel, finance and audit teams are all examples of functioning specialists. Regarding the ISMS improvement, it is crucial that those specialists should be involved from the early stages of implementation of ISO standard since they have the most realistic opinion on ISMS implementation progress and associated flaws. The business nature of a project should be clearly communicated to every functional specialist. (Calder A., 2017)

3.4 Planning

Actions to address risks and opportunities.

Under ISO27001 during the planning stage, implementors should consider context of organization, needs and expectations of interested parties as well as all other requirements stated in clause 4.1 and 4.2 of ISO 27001. Based on those requirements risks and opportunities should be determined and addressed to:

- Ensure the information security management system can achieve its intended outcomes.
- Prevent or reduce undesired effects.
- Achieve continual improvement.

Under ISO 27001 requirements organization should consider actions to address determined risks and opportunities and how to integrate solutions into the ISMS structure. Organization should also evaluate the effectiveness of those measures.

Planning is the most effort-demanding part of achieving ISO standard-compliant ISMS. Risks and opportunities in relation to the scope and needs and expectations of interested parties can be divided into two groups. Risks and opportunities in relation to ISMS achieving its objectives as a whole and in relation to confidentiality, integrity, and availability. The first group of risks is risks concerning ISMS itself including its processes, they should be identified and treated by complying with ISO 27001 requirements with utilization of scope within the expectations of interested parties. Opportunities of this group include the added value of ISMS implementation and controls identified by ISMS operation. The second group is associated with loss or inefficiency of confidentiality, integrity, and availability. Undesired effects that come from these risks are treated by the operation of ISMS namely risk assessment and risk treatment. Continual improvement should be achieved by repeatedly performing risk assessments, treating those risks, and then by monitoring of treatment effectiveness. But before the start of any of those processes, it is vital to plan how they will operate including all supplementary processes such as support or documentation procedures. Risks associated with the ISMS itself should be addressed to senior management to ensure that solutions are relevant to the scope and business structure in general. Organizations can comply with those requirements by documenting risk management processes. (ISO 27001 Clause 6.1 Actions to address risks and opportunities, no date)

Information security risk assessment

Under ISO 27001 an organization should define and then operate a risk assessment process that will define risk criteria, namely risk acceptance criteria that the organization is willing to accept and criteria of risk assessment itself. Consistent, valid, and comparable results of a risk assessment conducted with the same scope with no regard to other factors such as who has conducted assessments are required. Risk assessment should identify risks in relation to loss of confidentiality, integrity, and availability within the scope of ISMS and assign owners for those risks. Risk assessment under ISO 27001 requirements should simulate events of CIA affecting risk materialization and evaluate consequences. A realistic likelihood of such events taking place should also be identified and risk level determined. For purposes of further treatment identified and analyzed risks should be prioritized based on the comparison with risk acceptance criteria.

The whole risk assessment process including the definition should be documented and presented to the certification body during the audit. Risk assessment in terms of business is an evaluation of business harm from business failures with relation to calculated likelihood.

The complexity of risk assessment directly depends on the complexity of an organization and the quantity and complexity of associated risks. ISO 27000 defines risk, risk analysis, risk assessment, and other risk-related terms which are recommended to integrate into ISMS for consistency and proper documentation. Risk assessment under those requirements should produce consistent valid and comparable results if it is conducted again. It is important to mention that the ISO standard also requires an organization to assess the risks of the management system itself including the risk of failing to achieve intended ISMS outcomes. (Calder A. Watkins S., 2019)

Methodology for risk assessment.
The methodology is needed for assurance that all risks have been identified in the process and documented. Common ways of communication and acting on the results of risk assessment are also a part of a well-defined methodology. As ISO 27001 already has a set of requirements for risk assessment procedures it is important to choose among those that incorporate them, those that are not primarily technology-focused, and ones that include criteria for risk assessment and acceptance criteria.

Although steps for risk assessment are mandatory it is possible to adapt an approach to it that fits the organization the best. Risk assessment can revolve around organizational assets or possible scenarios. A scenario-based approach identifies risks by simulating events and predicting their consequences and estimating the likelihood and severity of those events to determine risk level. The asset-based approach on the other hand assesses risks related directly to assets such as hardware, software, data, and employees. (Calder A. Watkins S., 2019) Which basis to choose is a business decision and for each object of assessment, the fitting basis should be utilized. The scenario-based approach is effective for wider and more high-level implementation and can cover multiple departments. Asset-based is way more precise and manageable for the local system level. (Appendix 1.)

Mainly two risk assessment methodologies are recognized to be suitable for ISO27001 but not limited to include:

1. ISO 27005 Information security risk management standard from the same ISO family is well-aligned with requirements.
2. BS7799-3 is a set of guidelines for information security risk management that identifies the context of the organization from which risks occur.
   “Organizations have objectives, and in exploiting the opportunities that they create or seize to meet those objectives, they can encounter risks that need to be managed for the objectives to be fully realized. Some of those risks are

information security risks”- BS 7799-3, Clause 4. BS7799-3 in relation to what it is based on deviates and instead of just an asset-based approach utilizes the asset-threat-vulnerability model which takes into account the value of information-associated assets (and the value of information asset itself as well). It is important to mention that a blend of those approaches can be utilized. The scenario-based approach is more convenient for a high-level perspective while the asset-threat-vulnerability-based approach is more detailed. Both approaches are suitable for the standard but strategic implementation including relative benefits and drawbacks should be reviewed to determine the most suitable solution. (Calder A. Watkins S., 2019)

Risk itself should be calculated; its general formula is:

$$Risk = Likelihood\ x\ Impact$$

Where likelihood can be interpreted as a probability of vulnerability exploitation by a threat and impact is a total cost of an asset being exploited. The methodology should transfer variables in this equation into valuables and there are two approaches to that.

Qualitative and quantitative risk assessments.

The main difference between qualitative and quantitative assessments is that the quantitative analysis is based on mathematical data and the qualitative is based on non-mathematical data. The qualitative approach has a significant advantage of risk prioritization and identification of areas requiring immediate improvement but lacks in providing quantifiable impact outcomes which makes accurate cost-benefit calculations for controls hard to produce. The quantitative approach on the other side does provide accurate data for cost-benefit calculations and for most of the impacts excluding reputational, credibility, and trust impacts which cannot be reflected in numbers. Although for consistency reasons they can be described as “low”, “medium” and “high”. Despite providing numerical values for impacts, the meaning behind those numbers might be unclear. ISO 27005 states that those two methods can be combined in a way that qualitative analysis is

conducted first to determine general risk levels and major risks followed by quantitative analysis in vital areas such as but not only determining major risks. This approach is explained by the fact that quantitative analysis is significantly more fund-demanding and complex than qualitative. (Calder A. Watkins S., 2019)

Quantitative risk assessment

Quantitative risk analysis in its essence multiplies two variables: the probability of an incident and the likely cost of an incident. Probability is presented in a percentage or fraction of times in a year while cost of impact has solely monetary value. The output is called annualized loss expectancy (ALE). The bigger the value the bigger the risk for the company providing a grade scale for prioritization. The problem arises when a calculated risk is being compared to other assets, threats, and vulnerabilities with little to no implementation worth to ISMS. A problem of subjective assessment is also present in this analysis as both variables are mostly based individual's subjective view. This threatens certification achievement as results should be consistent with no regard to whoever conducts it. BS 7799-3 trying to solve this by utilizing exponential functions instead of numerical values. Rather than providing the exact value of impact, it provides a range within which impact cost might fall.

Qualitative risk assessment

Qualitative risk analysis is the most commonly used approach in risk assessment due to the relatively low cost/effort of implementation and the fact that this approach enables implementors to prioritize major risks. It is important to mention that this method is ranking risks in relation to each other, and all relative rankings should be based on common rules. All members of the risk assessment team should keep in mind that the same results are expected from the same environment if another person is to conduct a risk assessment. BS 7799-3 guideline is also specifying that all consequences including legal, regulatory, and statutory should be included in risk assessment. Qualitative risk analysis is based on impact, likelihood, and precision variables where impact and likelihood are presented in the form of a numerical rating. The general formula for qualitative

risk assessment is: $Impact\ x\ likelihood\ x\ preceision = risk$ For impact usually a five-level system is used (1=very low, 2=low, 3=medium, 4=high, and 5=very high) although another system with less or more than 5 levels can be used. Values for each level of impact should be set for the consistency of an assessment. It is recommended to assess any risk by at least 4 different parameters to give detail and context to an assessment. Those parameters might include monetary impact, reputational impact, business continuity impact, and legal impact. After the impact for every parameter is determined, the overall impact rating should be determined, which is simply the greatest value of all parameter levels. By utilizing the greatest value instead of an average or median implementors exclude the scenario for example when impact levels are 5, 1,1,1 and an event which is in advance is known to be very impactful is given an overall rating of 2 or 1. The likelihood is a probability that an event or in our case an exploitation will take place. It is crucial to set conditions to measure likelihood as a variety of factors influence the outcome. Likelihood assessment without human intervention aspect implies that no one will try to stop security incidents from happening which in most cases is known in advance to be not true. For that reason, likelihood consists of two parts such as probability of occurrence and intervention difficulty which is described as unwanted event prevention difficulty if intervention is present. This variable indicates if it is possible to respond and how difficult it is. The final likelihood rating is the lowest of those two ratings due to how those variables work in conjunction. If it is easy to prevent unwanted events, then the difficulty rating is low and even if the probability is high the ease of evasion minimizes the likelihood of occurrence. Vice versa if intervention difficulty is high and probability is low, likelihood is low due to low chances of that event happening. (Graves R.,2000) To better explain and visualize how the final likelihood rating is derived from probability and intervention difficulty to top management, tables such as illustrated in Figure 2 might be used by organization.

	Probability	intervention difficulty	Final likelihood rating
Earthquacke	1	5	1
Short power outage	3	2	2
Zero day vulnerability	2	4	2

Figure 2. Likelihood rating derived from probability and intervention.

Both probability and intervention difficulty are usually represented by 5 levels. It is recommended to give a rating to probability rather than utilizing percentage numerical values as it is hard to provide sustainable numbers especially when there are not many instances to calculate probability from. Although if one is confident in the consistency and accuracy of numerical data it should be used.

Precision is introduced for the purpose of adjusting the risk value by the factor of how much data is available on a particular risk thus representing the confidence in likelihood and impact assessment. Precision rating is presented in 3 levels and the lower the rating the less is known about that risk. Low precision is usually a warning that a risk may be much more serious than it is estimated. The final and more detailed formula for risk assessment is: $(Greatest\ of\ impacts)x(Lowest\ of\ probability\ and\ intervention\ difficulty)x\ preceision\ rating = risk$ A risk matrix should be produced as a result of the assessment consisting of likelihood and impact values. Ultimately impact is more prioritized than likelihood and in order to populate the matrix an equation of $Risk = likelihood + 2\ x\ Impact$ is often used to reflect the importance of impact. After that numerical values are graded in 3 different levels of risk green – less than 8, yellow – less than 11 greater than 8, and red – greater than 12 on which risk prioritization is based on. Figure 3 demonstrates an example of a risk matrix created according to the methodology described without impact multiplication. The risk matrix is a proven method of risk prioritization that is also convenient for presentation to management due to ease of understanding.

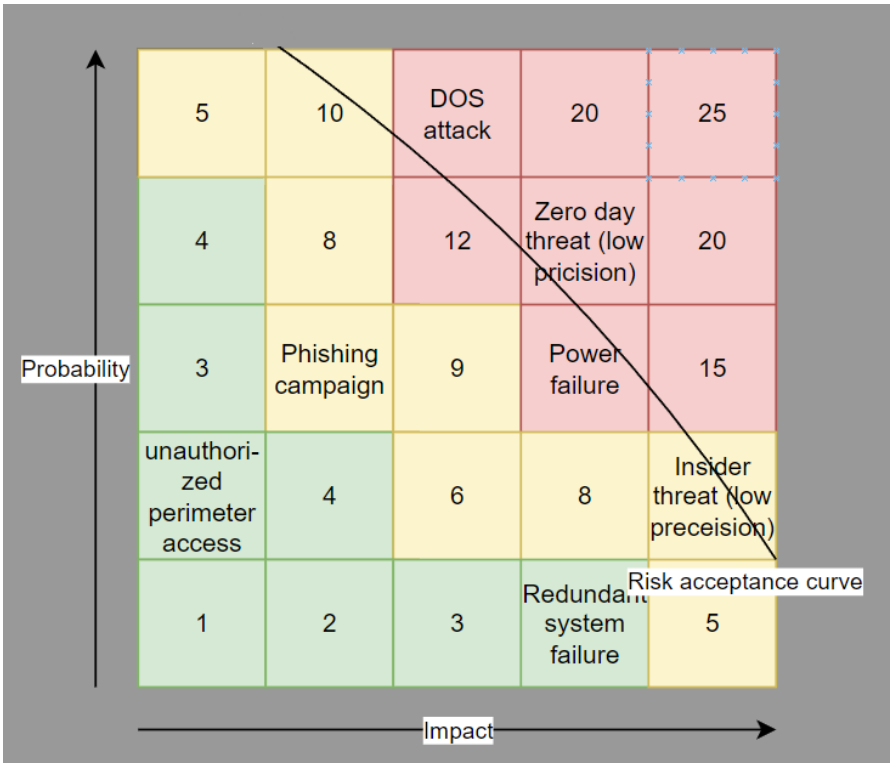

Figure 3. Risk matrix example

BS 7799-3 recommends prioritizing risk acceptance criteria during matrix creation rather than conforming to an arbitrary uniform layout. During grading low precision should also be taken into account without numerical value as a number does not describe the meaning behind it. It might be worth utilizing a more complex system rather than a color one, for example, prioritizing risks based on position in the risk matrix. ISO 27005 recommends conducting a risk assessment on at least two iterations, the first is a high-level general assessment aimed at crucial risk determination and the second one is a detailed assessment of identified risks. (Calder A. Watkins S., 2019)

Risk assessment team

If an organization already has a risk management team, then an in-house lead risk assessor oversees a process. If such a team is absent, then there are two possibilities either hiring an external consultant or training an internal employee to become a lead risk assessor which is preferable due to knowledge of infrastructure change during reassessment. In-house security advisors are the best candidates for the lead assessor role.

Risk assessment tools

Risk assessment automatization is a wanted best practice tool that greatly simplifies the risk assessment at the early stages of the process and is even greater in a longer perspective as review and maintenance processes are more robust. For ISO27001 a vsRisk software can be utilized as it is tailored specifically to this standard. (Calder A. Watkins S., 2019)

Information security risk treatment

Under ISO27001 defined and applied risk treatment is needed for:

- Selection of appropriate risk treatment options, taking account of risk assessment results.
- Determination of all controls necessary to implement chosen security risk treatment options. Controls can be designed or identified from any source.
- Compare determined controls with those in Annex A and verify that no necessary controls are excluded.
- Produce a Statement of Applicability containing controls as well as justification for those controls and exclusion justifications.
- Risk treatment plan should be formulated.
- Risk owner’s approval for security risk treatment plan should be obtained as well as acceptance of residual risks.

There are several risk treatment options:

1. Risk avoidance. Mainly achieved by the decision not to proceed with a solution or process that invokes that risk.
2. Taking additional risks in the pursuit of business opportunities.
3. Risk reduction. The main option for risk treatment that is achieved by reducing the likelihood or minimizing the impact by implementation of controls.
4. Risk transfer. Is achieved by sharing a risk with another party such as an insurance company or sub-contractor.

5. Risk acceptance. Is an informed decision not to do anything about the risk, usually it is chosen for residual risk after the implementation of one or more other risk treatments after risk acceptance criteria are met.

Treatment for each risk should be determined individually and in line with information security objectives. One or more of these options should be selected and implemented to satisfy risk acceptance criteria. Decisions on what controls to use should be based on the results of risk assessment.

Control determination

It is important to note that only necessary controls should be determined and implemented. By necessary ISO 27001 means controls that have more than a negligible effect on risk likelihood or impact and ones that in case of failure/or not being implemented do pose a challenge in business operation or threaten to completely stop it.

There are mainly two approaches for control determination. The first one is the utilization of a control set which is the most used approach, but it does have its downsides. Annex A of ISO 27001 is a control set by itself, but the organization might need controls beyond the scope of Annex A. In that situation utilization of other control sets is not prohibited by the standard and the organization might use control sets from ISO27017 which is a cloud standard or ISO27018 which is a privacy standard or use control sets outside of the ISO family such as NIST CSF. It is possible to aggregate controls from different sets. Implementors can select existent controls or if in the implementor's opinion provided controls are not effective for the organization's risk a custom control can be designed and implemented. When choosing a control from a set it is important that wording provided in a set meets required risk actions. If a control is not accurately described, it is worth defining your own control with all necessary descriptions. The scope of the control set might not cover all risks as if the implementor prioritizes Annex A it might be worth reviewing other sets for privacy, cloud, SCADA, and other sector-specific controls. It should be noted that cybersecurity develops in a rapid manner and controls might be outdated.

Another approach is to come up with control by yourself without the help of a control set by addressing how risk can be reduced. This approach seems nonproductive and contradictive but will generate controls with the most meaning to your organization. This approach does not require the implementor to re-invent control as existent controls may match with identified as well as they may not. This approach is more popular than the first one due to added value of being hand-tailored to meet organizational needs and thus way easier to implement and utilize it day-to-day. It is important to keep in mind the effectiveness of control and thus its cost-effectiveness to business. Services outside of the organization also might need controls and thus it is recommended to discuss controls with suppliers or outsource organizations. (Hall C., 2021)

Annex A comparison

The comparison of identified controls with ones in Annex A is essential to not miss any required control and give a different perspective to review identified controls and maybe find alternatives. Such alternatives might be cheaper and simpler to implement than the identified ones.

Statement of Applicability (SoA)

SoA under ISO 27001 should contain controls that the organization decided to implement as well as justification for inclusion and exclusion. Usually, it is formulated as a table containing all 114 Annex A controls and other identified controls. The first column usually indicates whether the control is implemented and has an effect on the risk, the second is for justification for inclusion or exclusion, and the third column indicates the status of control implementation. There might be a fourth column for details that are outside of the standard scope but might be useful for review such as implementation details or relevant policy. Justification for including the control relies on how and how much control is affecting the risk. Information about risk assessment result for that risk in conjunction with a risk treatment plan and how control reduces risk is sufficient for the certification body. In case control is excluded then a justification might be

that the control is not necessary or applicable due to being outside of ISMS scope. Any other solid reason for not including the control might be used. It is important to have a standalone well-documented and maintained SoA document as it is one of the checkpoints during certification. (Fine T., 2022)

Gap analysis

Although the standard does not include this step into its framework during ISMS implementation, the organization already has security controls in place and it is important to assess those measures for ISO 27001 adequacy and appropriateness. Bottom-up or top-down approaches exist for that process. The bottom-up approach starts with risk assessment results about all utilized security measures which is followed by an assessment of how much they are appropriate from the organization's SoA and the standard's point of view. A top-down approach on the contrary starts with SoA's identified controls and then identified controls are compared with existing ones on how much requirements are met. The top-down approach is faster in identifying major issues in security posture and unnecessary controls. (Calder A. Watkins S., 2019)

Formulating a risk treatment plan

A risk treatment plan is a formal document that contains all necessary data for addressing risks including risk acceptance criteria, responsibilities, and deadlines for risk-related activities. The risk treatment plan should be formulated within the context of security policy and define the organization's approach to risk treatment. Usually, it is a table with risks sorted by severity from risk assessment with relevant controls from risk treatment and employees responsible for control implementation. Other columns may represent the date of control implementation, information about control operation, and implementation status.

There is no specified structure for risk treatment plan but commonly organizations are using the following structure:

- Risk identified.

- Gap analysis results (if applicable)
  - Controls in place
  - Additional/replacement controls
- The gap between assessed risk and acceptable risk level
- Expected residual risk.
- Selected treatment option(s)
- Controls chosen.
- Resources required for control implementation including responsible employees.
- Status of treatment implementation
- Deadlines for control implementation
- Risk owner(s)

It is recommended to include a continual improvement section defining how the risk treatment plan should be reassessed and improved. Incorporation of general training, awareness, and individual competence required for the operation and improvement of this plan is also recommended. (Calder A. Watkins S., 2019)

Obtaining the risk owner's approval
The risk owner's approval should be based on provided risk treatment plan in a formally documented format for further presentation to the certification body. Approval should be based on the fact whether the risk treatment plan lowers the risk to an acceptable level or if there is a justified concession of elevated risk acceptance. Management approval of risk treatment plan is also recommended to document. Besides creating a standalone approval document incorporating approval into the risk treatment plan is also an option. (Calder A. Watkins S., 2019)

Information security objectives and plan to achieve them.
Properly set and maintained information security objectives help to achieve an organization's strategic goals and its security policy requirements. Those objectives are viewed in the scope of achieving confidentiality, integrity, and

availability goals. Specification and evaluation of controls and processes are also affected by security objectives. Usually, security objectives include ISMS improvement plans, risk treatment plans, and plans necessary for achieving or continuing effective operation. It should be noted that ISO requirements concerning objectives are applied to all and any security objectives set including possible objectives in security policy or a framework for setting objectives. During the review of security objectives, results of risk assessment and risk treatment should be taken into account to make sure that objectives are appropriate. (Calder A., 2017)

Security objectives are subject to documentation and under ISO 27001 requirements objectives should be:

- Established at all relevant functions and levels.
- Consistent with information security policy.
- Be measurable (If possible).
- Take into account applicable security requirements and results of risk assessment and treatment.
- Be communicated.
- Be updated as appropriate.

Security objectives to be measurable and achievable under ISO 27001 requirements should specify:

- Numerical values with limits.
- Security performance measurement targets.
- ISMS effectiveness measurement targets.
- Compliance with ISO 27001.
- Risk criteria requirement.
- Necessity to achieve an objective

Under ISO 27001 to achieve these objectives' organization should determine:

- Activities needed.
- Resources for those activities including competencies.
- Responsibilities for implementation.
- Deadlines for completion.
- Result assessment methodologies.

Criteria for appropriate objective setting

Objectives should be pointed towards the more effective and secure operation of an organization as well as being business oriented and corresponding to the expectations of interested parties. Meaningful objectives oriented at providing added value to the organization that are possible to measure is the goal. It is recommended to think from the client's perspective and analyze what security concerns they might have after inspecting the organization's ISMS or what aspects are especially important to them or, what is more important to the business, the costs of a breach. Risks with greatest impact should always be addressed first.(Appendix 1.) For Memphis company that was an example in privacy part those concerns might be elevated expectations about the security of their health data. Thus, Memphis's objectives might be ensuring that the whole process of delivering, storing and processing is secure. (Information Security Objectives & Planning to Achieve Them – ISO 27001 Requirement 6.2, isms.online, no date)

How to make objectives measurable

Making the previous objective measurable means segregating it into three domains: security of gathering information, and security of data at rest and during processing. Thus, risks associated with web security such as connection protocol security and overall penetration possibility of a site should be contemplated and given lower risk acceptance criteria which is numerical measurable value. The same applies to other domains. The source of data to measure the progress of the objective is a risk assessment report. Or if clients of Memphis are all around the globe it is in its interests to make service available as much time as possible.

Thus, an objective of service uptime of 99% or 100% of the time can be set. In this case, the measurement of progress can be assessed by the uptime logs of a website server.

Objectives responsibility
Communication of these objectives to relevant roles is essential for their achievement but what is more important is who is responsible for it in general. It is recommended to form a board for that specific purpose consisting of senior management and identify one person among them that would own the objectives. (Information Security Objectives & Planning to Achieve Them – ISO 27001 Requirement 6.2, isms.online, no date)

3.5 Support

Resources

The ISO standard imposes general requirements of determination and provision of resources needed for the establishment, implementation, maintenance, and continual improvement of ISMS. It is not possible to effectively implement an ISO 27001-compliant ISMS without proper investment in training, tools, controls, and competencies. Tools that are specialized for ISMS improvement would reduce error, time, and cost. Documentation templates and risk assessment software are the two most valuable investments for ISMS implementation. (Calder A., 2017)
To better understand the structure and interconnections of support operations refer to figure 4. Figure 4 divides support into resources and communication domains that incorporate all sub-processes that facilitate ISMS implementation and operation.

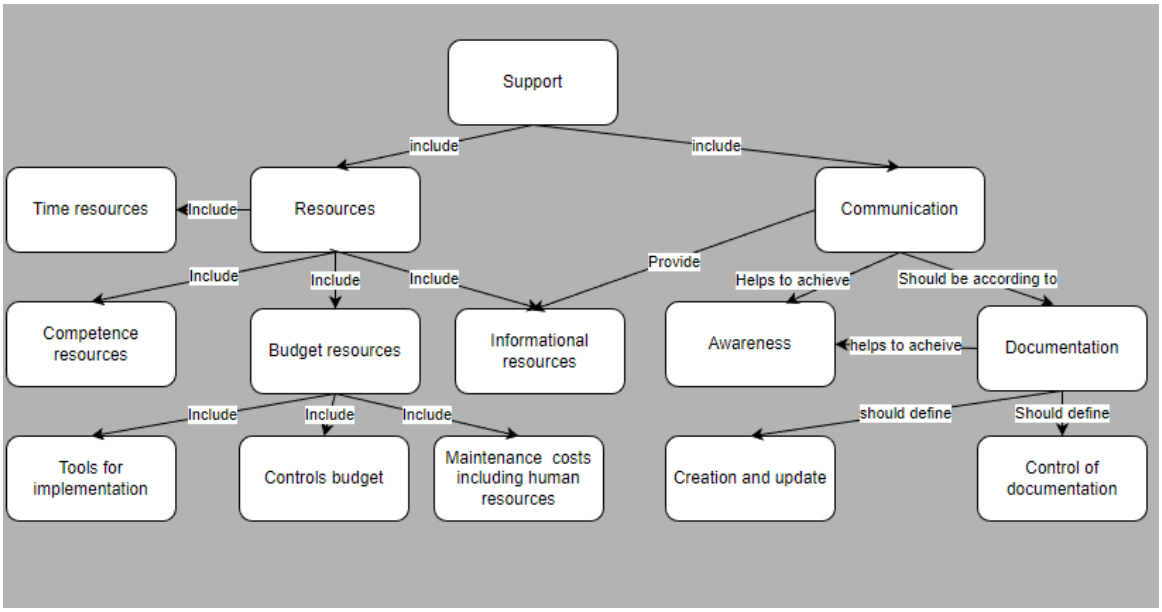

Figure 4. Structure and dependencies of ISMS support

Within the certification process for ISO standards if something is not documented then it does not exist thus it is crucial to document the following categories of resources:

- Human resources operating and implementing the ISMS
- Time resources intended for process execution and system stabilization after change for system operation assessment
- Financial resources for implementation of ISMS including controls and competencies.
- Informational resources for decision-making and improvement
- Infrastructure resources including materials technologies and tools

Resources should be aligned with ISMS implementation and improvement requirements and be adapted to the needs. To fulfill ISO requirements regarding the identification of needed resources a wide range of employees from various departments would need to contribute. Gap analysis conducted during the initial risk treatment plan provides data on existing controls and infrastructure and its

applicability thus making a good point for resource identification for ISMS integration.

Competence

Adequate competence level is one of the vital aspects as the degree of accuracy during the risk assessment, and control identification determines how successful, fast, and cost-effective ISMS implementation and improvement will be conducted.

Under ISO 27001 organization should:

- Determine the necessary competence of employees related to ISMS implementation.
- Ensure the competence of existing employees meets the requirements determined in the previous step. This is to be done on the basis of education training and gained experience assessment.
- If an employee lacks the required experience actions to address this issue are to be taken if applicable. Those actions include mentoring and training as well as reassignment of existing and hiring of new employees.
- Keep appropriate documented evidence of employee competence

The determination of necessary competence is directly linked to the roles and tasks of employees. Previous experience in ISMS implementation and related official training is a must for leading roles. It is desired but not mandatory for functional roles. To determine whether employees meet sufficient competence level and determine appropriate solutions in case they don’t it is worth assessing existing and acquired competence after training on how much they deviate. In cases where on-demand, not frequent competence is needed but there is none in-house it is possible to involve consultancy services or contractors. The ideal scenario is to train your own employees as frequent help with contracts is costly, but the organization should take into account that retaining these trained employees is crucial and thus according raise in pay should be provided. (Appendix 1.) The competence of a new hire can be assessed only after some

period of work and thus it is important to harden interview processes to ensure competence. If employees lack particular skills or are not familiar with ISO 27001 it is recommended to utilize official training programs according to their roles. The previously discussed competency matrix is the recommended document to demonstrate compliance with most of those requirements, keeping it updated and reviewed is crucial.

Time resource management

It is hard to estimate the time needed to achieve security objectives, but gap analysis output might provide some possible boundaries. Initial time planning would be very high-level, but it will be becoming more and more precise along the ISMS implementation process. It is important to logically divide the timeline with milestones, it will set smaller, more measurable thus more achievable steps. A standard management solution such as a Gannt chart will be effective. Mistakes and obstacles to any degree are unavoidable and they should also be considered during timeframe setting, but keeping to original deadlines is a best practice.

Awareness

Employees who access, maintain, or somehow else contact with valuable information and security assets should be aware of ISMS implementation and its relevant parts as well as be motivated to contribute to its development and improvement.

Under ISO 27001 persons doing work under the organization’s control should be aware of:

- The information security policy
- Their contribution to the implementation and improvement of ISMS as well as the advantages of ISMS development.
- Consequences of ISMS not conforming with requirements.

To demonstrate compliance with those requirements communication plan should include how when and where security policy has been provided to employees as

well as documented training sessions that communicate the advantages of well-maintained ISMS and disadvantages of poorly maintained ISMS. It is recommended to create a separate page on the intranet dedicated to security and ISMS which would contain all necessary documentation. It is also beneficial to ensure that every employee related to ISMS implementation or improvement reads through ISO 27001 requirements to better grasp their task.

Communication

Efficient and comprehensive communications as with any other project are vital for success. ISMS implementation and improvement requires communication between internal interested parties on almost all stages and levels as well as with external parties. With social engineering being the easiest and most effective approach for breaching all employees should be trained on how to recognize and act with phishing attempts. Phishing is just one instance of human-related risks, general security training would be needed. Acceptable use agreement outlining how employees should behave in various situations should be integrated. A clear desk policy, proper USB device handling, personal information handling, such procedures should be defined and communicated to all employees. (Calder A., 2017)

Under ISO 27001 requirements organization shall determine the need for internal and external communications related to ISMS including the following aspects:

- Themes of communications

There is a plethora of information types that would need to be communicated between departments and externally for vital ISMS processes as well as organizational requirements, those communications include:

- Risk management inputs, plans, results
- Planned or achieved security objectives
- Security incidents and obligations for reporting to authorities
- Responsibilities, roles, authorities

- Identification of ISMS processes needed communication between roles and teams
- Feedback collection mechanism from employees
- Training

- Communication contents

Identified themes are mostly repetitive or easy to predict and require specific information to be communicated. To ease the communication processes for repetitive processes and save time during incidents it is recommended to pre-determine the contents of communications and possibly create templates or automatic ISMS measurement reports. It should be determined what information is needed for processes and what type of information it is and tailor the output of the previous process to match the requirements.

- Time for communication

Timings of communication may be proactive, reactive, or planned. Proactive communications are usually information requests for ISMS improvement, audit, or corrective processes from other departments. Reactive communications are mostly dictated by the need to react to an incident or unforeseen obstacle. Planned communications are self-explanatory, it is important to set adequate frequency of planned communications to ensure timely delivery of decisions. Communications related to risk assessment, risk treatment, and monitoring should be planned and correlated to the timings of those processes. As training should be re-conducted from time to time it should also be included in planned communications. Traditional training methods have several flaws and they do not produce presentable evidence thus it is recommended to use e-learning. (Calder A., 2017)

- Receivers of communication requests

To whom information should be communicated and in what cases those people should be contacted.

- Who should communicate

Providing authority for external or internal communications is extremely important for overall organizational operation as well as for incident management.

- Communication processes

Means of communication should be established determining what channels to use in various situations. The main goal of this aspect is to ensure confidentiality, integrity, and availability across communication channels. For example, during standard operation Teams, internal mail servers, or other standard corporate software can be used. But in case of a breach where it is known that a malicious actor has access to internal channels it is worth switching to out-of-band communications not to provide any intel on countermeasures.

For a communication plan to be complete and accurate, it is recommended to identify all possible points of communication in processes and logically link them with each other for consistency of processes. As already stated, communications should be classified and documented. The ISO certification body requires data only concerning ISMS. The creation of an annual communication plan is recommended as it will demonstrate compliance with those requirements and provide one point for communications management.

Documented information

Properly documented and updated security objectives, policies, controls, and processes are beneficial not only for ISO certification but also for general organizational operation, especially during reviews and audits.

Under ISO 27001 requirements ISMS should include:

- Documented information required by ISO 27001
- Documented information necessary for ISMS operation determined by the organization

It should be noted that the extent of necessary documentation varies depending on the size and complexity of an organization as well as on the competencies of employees within the organization. Additional documentation necessary for the operation of ISMS needs to be identified, it is recommended to review previous chapters and determine crucial points of ISMS implementation reflecting your unique organization. Those points may be context establishment results, roles, authorities, responsibilities, various reports, determined needed and owned resources, awareness, communications documentation, policies, and procedure descriptions. As it is previously mentioned documentation is one of the main if not the main compliance demonstration mechanisms that the certification body will utilize.

Creating and updating

Documentation should meet organizations' standards for document format and review to accelerate processes that require access to that documentation. Under ISO 27001 requirements, organizations should ensure appropriate identification and description of documentation as well as the format and appropriate media. The organization's documentation standards can be reflected in the documentation policy which further can be provided to demonstrate compliance. Identification of a document can include a specific ID for fast search in a database and other managemental activities, the date for keeping track of review periods, the author to keep responsibility documented and to have written contact information for consultation. Review and approval parameters such as review period and roles responsible for review should also be established and reflected in the documentation policy. Review approval criteria should be clearly defined to check whether reviewed information is correct, fit-for-purpose, adequate form, and detailed/general enough for the intended audience. Appropriate media should be determined with due regard to safety and accessibility parameters. Duplication of data across multiple documents is not desired, utilization of references is recommended instead. Responsibilities for documentation creation

and updates should be assigned. (ISO 27001 Clause 7.5 Documented information Implementation Guideline, info-savvy, no date)

Control of documented information

Information intended for ISMS use and standard certification should be controlled under ISO 27001 requirements to ensure:

- availability and efficiency wherever and whenever
- Adequate level of technical security

Availability of documentation to authorized employees can be achieved by the creation of an e-library on the intranet. Classification of data should be conducted to facilitate only authorized access. Proper controls should be implemented to ensure the security of documentation including improper use and documentation tampering. The whole lifecycle of documentation should be addressed under ISO 27001 which includes:

- Distribution, access, retrieval, and utilization.
- Storage and preservation, including preservation of legibility.
- Version control.
- Retention and disposition.

It should be noted that documentation of external origin determined to be necessary for ISMS planning and implementation by an organization should be considered appropriate and controlled by previously described requirements. Access in the context of the standard means not only access management but also permission management. Proper distribution may be achieved by utilization of documentation groups which will group users based on their role and need in specific documents. Distribution should fulfill security requirements associated with the handling of classified information. An acceptable retention period should be established to ensure accuracy and validity during utilization. Legibility may be achieved via the utilization of only digital variants across the company or the use

of formats readable for software and making sure that paper variants are not corrupted if it is not possible. After the documentation's retention period is over, organization should determine what to do with the information. Archiving for later retrospective analysis or backup is one approach, but documentation disposal is also possible if no other use is identified or it is legally binding to do so. Disposal should meet the security criteria and securely destroy the information, possibly including the media it was stored on. (ISO 27001 Clause 7.5 Documented information Implementation Guideline, info-savvy, no date)

3.6 Operational planning and control

Under ISO27001 requirements organization should:

- Plan, implement, and control processes needed to meet standard requirements determined in chapter 6.2 "Actions to address risks and opportunities" including general requirements, risk assessment and treatment as well as security objectives. Objectives determined in chapter 6.4 "Information security objectives and planning to achieve them" should be planned and implemented.

The lifecycle of a process includes planning, implementation, control of possible change, and eventual termination. During control, processes are reviewed to determine whether they are effective and fulfill the needs of interested parties. Confidence about effectiveness can be gained by inputting documentation gained during monitoring into the evaluation process discussed in the next chapter. A properly determined documentation set and template for this purpose as well as for other processes is considered best practice. It is recommended to integrate objectives projects into the business-as-usual paradigm and utilize the project initiation document. (Calder A., 2017)

- Documentation for those projects should be stored until the process has been fully completed and the process was carried out as intended.

Having documented guidance for the process that an organization is implementing or controlling is imperative.

- Planned changes should be controlled and consequences of unplanned changes should be assessed, and mitigation of adverse effects identified.

If Changes are not planned, they should be treated as either an incident that has its own risks or as an urgent fix. Unplanned changes should be reflected in risk assessment. (ISO 27001 Clause 8.1, Clause 8.2, Clause 8.3 Operational planning & control, info-savvy, no date) Control of changes include the following:

- Assignment of resources, tasks, responsibilities, and deadlines.
- Monitoring and verifying that changes are implemented according to plan.
- Produce and keep documentation of how changes were executed as proof of planned implementation.

The organization's actions regarding unplanned changes include the following:

- Consequences should be reviewed, and adverse effects detected if such exist at the moment and possible effects should be predicted.
- Mitigation actions should be identified and executed.
- Documentation regarding unplanned changes and mitigation actions to be produced and retained.

- Outsourced processes should be determined and controlled.

Control of outsourced processes includes:

- Identification of all outsourced services.
- Interface for contact with outsourcing organizations should be established.

- Information security aspects in light of provided services should be discussed and mutually agreed processes established.
- Monitoring of services to ensure that they are operating correctly, and associated risks are meeting risk acceptance criteria.
- Perform changes if necessary.

Information security risk assessment

Under ISO27001 requirements, organizations should perform risk assessment repeatedly in determined time intervals or after impactful changes in accordance with the risk assessment planning. Documentation of the results of risk assessment must be produced and retained.

For risk re-assessment, the same methodology should be used for the initial risk assessment unless it was agreed upon to change the risk assessment paradigm. Each iteration risk assessment should be more detailed than the previous iteration to comply with continuous improvement requirements. A broad risk assessment which would include all possible risks must be conducted at least once a year. Time intervals should be adequate in a way that they give enough time for monitoring and evaluation processes to produce sufficient output and not too long not to overlook critical risks which might arise after changes. Trigger criteria and mechanisms for unscheduled risk assessments should be defined such as breaches or newly found vulnerabilities affecting security posture. Documentation produced by risk assessment is crucial for risk treatment and certification and handy for performance evaluation, an organization should keep documentation detailed and updated. (Calder A., 2017)

Information security risk treatment

Under ISO 27001 requirements risk treatment plan should be implemented and all produced documentation should be retained. After an organization has completed a risk assessment, risk treatment should follow with due regard to the results of the risk assessment results. Another trigger reason for re-conducting risk treatment is a failure of the previous treatment process or part of it.

Documentation of the treatment process and results should be retained as evidence of compliance.

3.7 Performance evaluation

Monitoring, measurement, analysis, and evaluation

Under ISO 27001 requirements organizations should consider the following aspects during planning how to monitor and evaluate ISMS:

- What needs to be monitored and measured, including controls and processes.

Monitoring of metrics needed for security objectives is crucial. Monitoring of controls effectiveness that treats major risks or risks that are greatly reduced by those controls is critical for ISMS. Most subjects for monitoring can be identified using the scope documents, documentation produced during risk and opportunities planning, objectives documentation, internal audit methodology, and management review reports. The usage of diagrams, risk assessment results, and other tools is desirable. Cost-effectiveness of controls and processes is also highly desired as ISO 27001 is firstly a business project thus it is beneficial to monitor implementation and related budget usage. Vulnerability patching and management are considered not of great importance on a large scale, but they are crucial for processes ‘maintenance’ and control effectiveness. Incident handling and remediation speed should also be monitored as well as the effectiveness of overlooked controls such as physical and perimeter security. It should be noted that it is not possible to measure everything. (Calder A., 2017)

- Methods of monitoring, measurement, analysis, and evaluation and as applicable, methods of ensuring validity of results. Methods should produce comparable and reproducible results to be considered valid.

  Methods should be appropriate for controls that they measure and more importantly what aspects they measure. It may be impracticable, cost-ineffective, or impossible to measure specific aspects in traditional or most obvious ways thus other metrics can act for indirect measurements. As

applicable in that context means that methods for validity should also be determined if it is possible and appropriate to do. To receive valid, reproducible, and comparable measurements ISO9001 methodology can be used. A measurement report template should be created.

- Timings of monitoring and measurements.

  Proper intervals as with risk assessment intervals should be adequately set. Enough time should be given for recording ISMS processes or controls in retrospect and not too much to keep results actual.

- Roles and responsibilities associated with monitoring and measuring.

  There are two approaches to the determination of monitoring and measuring team members. The first one applies that continuity and interconnectivity of ISMS vital processes imply utilization of the same team with possible deviations due to different competence. An advantage of this approach is that most of the team members are well informed of the results of the previous process, but it may stand in the way of an unambiguous and objective attitude towards input for the new process. The second approach does not have this downside as most if not all members of each process are different. Obviously, the second approach would require sufficient human and financial resources. A solution to this issue should be determined with due regard to the organization’s nature, size, and complexity.

- Timings of analysis of monitoring and measurement results.

  Large complex organizations produce a lot of information about ISMS operations. It is crucial to prioritize the crucial data such as control that reduces a lot of risk or measurement related to the objective to have enough time for important measurements. If the security team is divided between processes, analysis of monitoring should be conducted as soon as enough data is gathered. If the same team is responsible for risk assessment it might be worth analyzing measurements during risk assessment.

- Roles and responsibilities associated with the analysis of monitoring and measuring results.

  If the security team is not divided by processes, it should be their responsibility. Roles for monitoring and analysis should be appointed, documented in the responsibility matrix, and communicated.

- Appropriate documentation on the process execution and results should be produced and retained as evidence of compliance.

Internal audit

Under ISO 27001 requirements organization should conduct internal audits at planned intervals to ensure:

- Conformity of ISMS to organizations' own ISMS requirements as well as ISO 27001 requirements.
- Implementation and maintenance are conducted effectively.

To comply with those requirements under ISO 27001 procedure organization should:

- plan, establish, implement, and maintain an audit program(s), including the frequency, methods, responsibilities, planning requirements, and reporting. The audit program(s) shall take into consideration the importance of the processes concerned and the results of previous audits.

The frequency of audits should be planned to cover an extent of a whole year and it should be noted that some controls require more frequent audits than others. Risk assessment results will help determine such controls. Usually, it takes a year for an organization to collect enough evidence of proper testing and auditioning practices. If an organization desires to achieve certification in less

than one year of audition and testing, a test of all crucial ISMS aspects plan should be created and executed. (Calder A., 2017)

- Define criteria and scope for each audit

An organization should consider what process or part of ISMS is being tested and what are the boundaries of it. Audit of controls and emergency countermeasures as well as compliance of core processes should be prioritized. Criteria might include the effectiveness of controls and how properly they operate, do emergency countermeasures are updated and function properly, and the redundancy degree in case of failure.

- Select an audit team and conduct audits based on objectivity and impartiality principles.

Auditors would have to avoid auditing areas of their own responsibility to ensure objectivity. For that reason, auditors from various departments/security teams should be gathered for the audit team.

- Ensure audit results are properly communicated to relevant management.
- Produce and retain audit documentation of process and results as evidence of audit program conduction.

Evidence includes audit plans as well as results and process descriptions of conducted audits.

There are four methods to address the audition process:

1. The first approach is a standard internal audit which involves an internal team of experienced and well-trained auditors drawn from various departments going through documented procedures that would require evidence of compliance with all the requirements of the standard. This is a solid long-run variant.
2. The second approach is a so-called paper test which in its essence is an intellectual exercise requiring a team of at least two people with competence in vulnerabilities, controls, and possible threats. Based on technical

competence and experience of auditors this approach assesses controls effectiveness logically.

3. The third one is known as a limited real-life test; it involves recreating a controlled environment of risk control failure or interruption of normal operation to find out how it affects operation and how effective deployed measures are in practice. A proper “backup” plan ensuring a return to the previous operation state should be established as well as precautions not to harm business interests. Penetration testing is one of the most effective methods in this approach as it can test not only the adequacy of control identification but also risk assessment results. Penetration testing will determine not only the effectiveness of present controls but also the lack of them in places that were not identified.
4. The fourth one is a large-scale scenario test mostly used to simulate major information security incidents and test measures or/and business continuation plans. Usually, these tests condense a timespan of several days of real incidents in a shorter period of time during which all ISMS-relevant roles would attempt to conduct required tasks. Significant planning and the certainty that this test would not harm business interests are essential. External help might be needed for objective assessment. (Calder A., 2017)

Management review

Under ISO 27001 requirements organization’s top management should review ISMS at planned intervals to ensure its continuing sustainability, adequacy, and effectiveness including:

- Status of actions from previous management review.
- ISMS-relevant internal and external issue changes.
- Feedback on ISMS security performance including tendencies in:
    - Nonconformities and corrective actions.
    - Results of monitoring and measurement.
    - Audit results.
    - Information security objectives achievement status.
- Interested parties’ feedback.
- Risk assessment results and risk treatment plan status.
- Continual improvement opportunities, decisions, and needed changes related to them.

Management review should focus on the management aspect of ISMS and measurements indicating the status of security objectives achievement. It should also reflect on changes in the operational environment and adequately adjust internal and external processes. Conducting a management review annually is a bare minimum, a quarterly review is considered best practice. The review team should include an information security manager, a senior leadership representative, and members of each department. Responsibilities for each topic should be assigned to guarantee progress. All members of the team and their responsibility should be documented. Minutes of the meeting should be produced, distributed, and retained.

3.8 Improvement

Nonconformity and corrective action

Under ISO 27001 when nonconformity occurs organization should:

- React to the nonconformity and as applicable:
    - Take action to correct it and gain control.
    - Deal with consequences.
- Evaluate the need for cause elimination to prevent further occurrence:
    - Review the nonconformity.
    - Determine the cause.
    - Determine if similar nonconformities exist or have the potential to reoccur.
- Implement any needed, appropriate to effects of nonconformity actions
- Review the effectiveness of taken actions.
- Make changes to ISMS if necessary

An organization should produce and retain documentation as evidence of:

- Nature and subsequent taken actions regarding the nonconformity.
- Results of corrective actions taken.

A corrective action policy or incident management policy is the perfect place to reflect correction procedure aspects and a point of compliance demonstration. Formalizing corrective and continual improvement processes should include assigning responsibility, determination of evaluation criteria, determination of reaction selection criteria, and determination of effectiveness criteria. Documentation on the operation of corrective measures should be collected and presented as evidence.

Continual improvement

Under ISO 27001 an organization should continually improve the sustainability, adequacy, and effectiveness of ISMS. By repetitively conducting risk assessment risk treatment and monitoring organization achieves a continual improvement of security controls. Monitoring and measuring, internal audit, and management review are sources of nonconformities that corrective action brings to compliance and achieves a continual improvement of the ISMS as a whole. The ISO standard allows the implementation of any continual improvement approaches including ITIL and COBIT schemes. The most commonly implemented approach is the Plan-Do-Check-Act approach or PDCA model. A thorough understanding of the approach by management is crucial before implementation starts. Besides the approach, a root cause analysis (RCA) should be determined to identify or possibly predict identical issues in the ISMS. RCA greatly increases the effectiveness of all corrective actions. A primitive but effective RCA technique is the “5 whys”. This technique is an intellectual exercise that requires consequently asking why five times in relation to the cause of a problem and answering it by yourself. Each iteration creates a basis for the next “why” is being determined in an answer to the previous question which should lead to the logical cause of the issue. (Calder A., 2017) (Appendix 1.)

3.9 Certification

Before the certification process begins organization should if not fully integrate ISMS into its structure, then at least significant progress towards it should be accomplished and if any other management framework is utilized, they should be merged as much as possible. In order to receive ISO certification, the organization should select what certification body will conduct an audit and there are several aspects that affect selection. Pricing, terms, and conditions, as well as alignment of the working culture of both organizations, should be assessed and agreed upon. The approach to certification audit of the certification body should also be evaluated. As each ISMS corresponds to the unique business nature of each organization each ISMS is consequently different. Thus, certification audits should not just compare requirements to ISMS but include ISMS nature into the audit scope.

As soon as the certification body has been selected it is recommended to actively demonstrate compliance and leave a good first impression. This can be achieved by providing complete documentation at the initial visit which purpose is to determine whether your ISMS is ready for an audit in the first place. Ideally, this documentation should include key process evidence with emphasis on internal audit and testing reports. Those documents should invoke confidence in the auditor in relation to the organization’s ISMS. Be ready to send additional documentation on request in a timely manner or better provide access to all of them at once by creating an intranet guest account from which all relevant information can be retrieved.

Employees should be instructed to be open and honest to auditors and not hesitate to bring up areas of non-compliance as it will demonstrate the transparency of an organization and willingness to correct information security issues as well as helps to determine weaknesses to work on. Auditors are experienced professionals, and they know that there is no system without flaws, if an organization acts as if its ISMS is perfect, it will trigger auditors to thoughtfully

hunt for imperfections. Employees that are likely to accompany auditors during the audit and potentially be interviewed should be instructed to actively explain how the system operates and how it relates to a business nature. This will provide evidence of competence and focus on the ISMS improvement of employees. Although it should be mentioned that the explanation should precisely answer the questions of auditors and not mention any themes not related to the question as it may lead to an audit of ISMS areas that do not need external audit.

Management involvement is vital as it not only demonstrates compliance with management requirements but also significantly increases confidence in ISMS's correct implementation and operation. It is recommended to explain how to best demonstrate commitment to senior management and inform them what questions would probably be asked.

No certification goes without arguments and employees should be prepared for discussion in a calm, informed and respectful fashion. Misunderstandings of ISMS implementation or misinterpretation of the standard are common points of argument. Auditors will provide a list of non-compliance that should be addressed with nonconformity and corrective actions defined by ISMS to become compliant.

After all aspects of the ISMS are deemed compliant by the auditors a certification will be issued corresponding to the SoA version utilized during the audit. Any major changes to SoA are undesirable due to certification being closely tied to its version. Proper display of certification to interested parties should be implemented including the SoA version. Surveillance visits taking place in approximately half a year should be taken into account and appropriate preparations should be on their way, which includes documentation level maintenance. (Calder A., 2017)

4 CONLUSION

Privacy and ISO27001 standards are complex and require a specific approach to achieving compliance. The research resulted in the following conclusions:

4.1 Privacy

Provided privacy obligations and measures to satisfy them are mostly needed in organizations that have been recently created and in which various privacy matters are not dealt with. The topics described were chosen broadly to include most of the possible internal and external privacy issues as well as fundamental data protection principles that are applied to any personal data process. Although the description of obligations and measures provided should be sufficient to plan a privacy achievement project and determine some aspects, a case-by-case inspection and decision-making and deeper research to fit into specific jurisdiction requirements are needed. As in most countries of EEA appointment of a DPO either internally or externally is mandatory, the author recommends doing so in the early stages of privacy integration to better implement the activities stated above. Topics and their relevancy are based on internal and client meetings as well as Certified Information Privacy Professional / Europe (CIPP/E) training that the author of this thesis attended during the internship. Data protection in relation to contemporary technologies is explained as methods of achieving compliance with due regard to business nature and needs and a strong emphasis on web privacy. The research includes a breach guide that informs readers about the organization’s actions during and after the breach to minimize potential harm and be compliant with obligations. At the planning stage it was intended that security obligations would be fulfilled by ISO 27001 standard but in practice ISO certification does not guarantee compliance with security obligations but does contribute to that matter. In case an organization would not choose ISO standard, it is possible to achieve Cyber Essentials certification. It provides guarantees that an organization is protected against basic hacking techniques. The research method used for this part has flaws and potentially some topics were overlooked. Further study, if deemed needed should focus on particular countries and jurisdictions and be periodically reviewed to keep actual.

4.2 ISO 27001

General steps for ISO 27001 certification conducted according to the guidance described in this thesis should be clear. In practice, deeper research implemented in relation to unique business needs, technology stack, and infrastructure would be needed. The problem with the ISO 27001 standard in relation to the achievement of confidentiality, integrity, and availability is that in its essence it is a management standard, and its implementation is a business project. ISO 27001 relies on risk assessment heavily but does not govern how risks should be assessed. The statement that an appropriate risk assessment methodology to be effective should be determined according to the business nature is very speculative and uninformative as criteria defining the effectiveness of risk assessment are also not described in the standard. Risk treatment plan have a similar issue, no methodology as well as no criteria for acceptable risk level is imposed or proposed thus, according to the standard if risk appetite is high, controls determined by ISO compliant process will be insufficient to provide adequate security. Thus, being certified to ISO standard does not necessarily mean that your organization is secure. Of course, all those issues arise only in conditions of poor implementation, and effective ISMS streamlines the processes. The lack of baseline security criteria can be explained by the ability of an implementation to various sectors and organization sizes with their own specific needs. (Appendix 1.) The high competence of employees responsible for risk assessment, risk treatment, and internal audit as well as management commitment to information security in conjunction with individual responsibilities for information security processes should be sufficient to ensure proper security within the framework. Another problem of ISO 27001 which is not related to security but has a serious effect on operation is a heavy dependency on documentation. Although it does have the advantage of retrospective analysis and traceability the amount of documentation including how detailed it should be to carry value to the processes is too high and demands sufficient resources to be produced and maintained. Automation and template usage lowers those costs but not significantly. And finally keeping your organization compliant is hard and

requires continuous effort and funding as after first certification at periods of approximately half a year surveillance visits will be conducted, and afterward full recertification will be necessary. All those processes in a coup with the previous issue restrain companies in their growth or reorientation due to the link of certification to the SoA version. Nether the less ISO 27001 is still a valuable organizational asset, understanding its structure, achievement steps, flaws, and ways to remediate their effect should formulate objective decision on whether an organization needs it. Regarding this thesis, the author does acknowledge that utilization of actual data of standard implementation would provide more in-depth knowledge and justification, but it should be noted that it is near impossible to find a job that is declaring ongoing ISO 27001 implementation openly and is willing to hire an intern on a position that demands high competency. The methodology used for research has its flaws, as stated in the introduction non-academic sources have also been used and some of them besides providing relevant and accurate information have been over exaggerating the importance and effectiveness of the solutions presented. When working with those sources, the author justified provided information by addressing implementors' blogs and forums. Further study to be more accurate and fit for purpose should consider more operational aspects of implementation, basis for implementation necessity should include approximate calculations of implementation based on organizational information and specify criteria which would help to choose the best fitting and effective methodology in cases where prior to implementation no methodology is adopted.

REFERENCES

A Comprehensive Guide to Personal Data Mapping. 2023. GDRPregister. Web page. Available at: https://www.gdprregister.eu/gdpr/guide-to-personal-data-mapping/ [Accessed 20 April 2023].

Adequacy decisions. n.d. The European Commission site. Web page. Available at: https://commission.europa.eu/law/law-topic/data-protection/international-dimension-data-protection/adequacy-decisions_en [Accessed 1 March 2023].

Binding Corporate Rules (BCR). n.d. European commission site. Web page Available at: https://commission.europa.eu/law/law-topic/data-protection/international-dimension-data-protection/binding-corporate-rules-bcr_en [Accessed 5 March 2023].

Calder, A. 2017 Nine Steps to Success: North American edition - An ISO 27001 Implementation Overview. Ely: IT Governance publishing. E-book. Available at: https://learning.oreilly.com/library/view/nine-steps-to/9781849289511/ [Accessed 10 March 2023].

Calder, A. & Watkins S. 2019. Information Security Risk Management for ISO 27001/ISO 27002, third edition. Ely: IT Governance publishing. E-book. Available at: https://learning.oreilly.com/library/view/information-security-risk/9781787781382/ [Accessed 18 March 2023].

Cookies, the GDPR, and the ePrivacy Directive. n.d. GDPR.EU. Web page. Available at: https://gdpr.eu/cookies/ [Accessed 15 February 2023].

Direct marketing rules and exceptions under the GDPR. 2022. GDPR register. Available at: https://www.gdprregister.eu/gdpr/direct-marketing-rules-and-exceptions/ [Accessed 30 April 2023].

DIRECTIVE 2002/58/EC OF THE EUROPEAN PARLIAMENT AND OF THE COUNCIL.

Employee Monitoring - the Article 29 Working Party refreshes its opinion. 2017. Fieldfisher. Web page. Available at: https://www.fieldfisher.com/en/services/privacy-security-and-information/privacy-security-and-information-law-blog/employee-monitoring-the-article-29-working-party-refreshes-its-opinion [Accessed 29 April 2023].

Fine, T. 2022. ISO 27001: How to Write a Statement of Applicability. Web page. Available at: https://drata.com/blog/iso-27001-statement-of-applicability [Accessed 14 March 2023].

GDPR exemptions from the obligation to provide information. 2020. Data Privacy Manager. Available at: https://dataprivacymanager.net/gdpr-exemptions-from-the-obligation-to-provide-information-to-the-individual-data-subject/ [Accessed 29 April 2023].

Graves, R. 2000. Qualitative risk assessment. Web page. Available at: https://www.pmi.org/learning/library/qualitative-risk-assessment-cheaper-faster-3188 [Accessed 23 March 2023].

Guidelines 2/2018 on derogations of Article 49 under Regulation 2016/679. 2018. PDF document. Available at: https://edpb.europa.eu/sites/default/files/files/file1/edpb_guidelines_2_2018_derogations_en.pdf?source=post_page---------- [Accessed 26 April 2023].

Hall, C. 2021. With ISO27001 how you should choose the controls needed to manage the risks. Web page. Available at: https://www.linkedin.com/pulse/iso27001-how-you-should-choose-controls-needed-manage-chris-hall/ [Accessed 25 March 2023].

How to do Requirement (of ISO 27001:2013? n.d. isms.online. Web page. Available at: https://www.isms.online/iso-27001/6-2-establishing-measurable-information-security-objectives/ [Accessed 18 March 2023].

How to Write an ISO 27001 Scope Statement. n.d. Compleye. Web page. Available at:https://compleye.io/articles/iso-27001-scope-statement/?gclid=Cj0KCQiAo-yfBhD_ARIsANr56g7mF-T6g2T2pyTHYgbf3zLzO2Isyq_CJsNWSWTvD3enX4Kg1zDld-IaApC2EALw_wcB [Accessed 10 March 2023].

The European Commission. 2016. REGULATION (EU) 2016/679 OF THE EUROPEAN PARLIAMENT AND OF THE COUNCIL. The European Commission regulation. Available at: https://eur-lex.europa.eu/legal-content/EN/TXT/HTML/?uri=CELEX:32016R0679&from=EN#d1e1374-1-1 [Accessed 9 February 2023].

ISO/IEC 27001 Information technology — Security techniques — Information security management systems — Requirements. International organization for standardization. Not publicly available. [Accessed 27 February 2023].

ISO 27001 Context Of Organisation Beginner's Guide, n.d., Hightable. Web page. Available at: https://hightable.io/context-of-organisation/ [Accessed 10 March 2023].

ISO 27001:2022 Clause 4.2 Understanding The Needs And Expectations Of Interested Parties. n.d. Web page. Available at: https://hightable.io/iso-27001-

clause-4-2-understanding-the-needs-and-expectations-of-interested-parties/#h-what-does-the-standard-say-about-iso-27001-2022-clause-4-2 [Accessed 10 March 2023].

ISO27001 Clause 5.1 Certification Guide | Leadership And Commitment. n.d. Hightable. Web page. Available at: https://hightable.io/iso-27001-clause-5-1-leadership-and-commitment/ [Accessed 15 March 2023].

Panhalkar T., ISO 27001 Implementation Guideline Clause 5.2 Policy. n.d. Infosavvy. Web page. Available at: https://info-savvy.com/iso-27001-implementation-guideline-clause-5-2-policy/ [Accessed 15 March 2023].

Panhalkar T., ISO 27001 Clause 6.1 Actions to address risks and opportunities. n.d. Infosavvy. Web page. Available at: https://info-savvy.com/iso-27001-clause-6-1-actions-to-address-risks-and-opportunities/ [Accessed 17 March 2023].

Panhalkar T., ISO 27001 Clause 5.3 and Clause 7.1 Resources and Roles & Responsibility. n.d. Infosavvy. Web page. Available at: https://info-savvy.com/iso-27001-clause-5-3-and-clause-7-1-resources-and-roles-responsibility/ [Accessed 20 March 2023].

Panhalkar T. ISO 27001 Clause 7.5 Documented information Implementation Guideline. n.d. Infosavvy. Web page. Available at: https://info-savvy.com/iso-27001-clause-7-5-documented-information-implementation-guideline/ [Accessed 22 March 2023].

Panhalkar T., ISO 27001 Clause 8.1, Clause 8.2, Clause 8.3 Operational planning & control n.d. Infosavvy. Web page. Available at: https://info-savvy.com/iso-27001-implementation-guideline-clause-5-1/ [Accessed 23 March 2023].

John, C. n.d. Understand the intersection between data privacy laws and cloud computing. Thomson Reuters. Web page. Available at: https://legal.thomsonreuters.com/en/insights/articles/understanding-data-privacy-and-cloud-computing [Accessed 28 April 2023].

Koustic, D. 2017. Preparations for the ISO Implementation Project: A Plain English Guide. Zagreb: Advisera Expert Solutions Ltd. E-book. Available at: https://ru.scribd.com/read/367608240/Preparations-for-the-ISO-Implementation-Project-A-Plain-English-Guide-A-Step-by-Step-Handbook-for-ISO-Practitioners-in-Small-Businesses# [Accessed 20 April 2023].

Koustic, D. 2022. What is the ISO 27001 Information Security Policy, and how can you write it yourself? Advisera. Web page. Available at: https://advisera.com/27001academy/blog/2016/05/30/what-should-you-write-

in-your-information-security-policy-according-to-iso-27001/ [Accessed 25 March 2023].

Leal, R. 2022. How to define context of the organization according to ISO 27001. Web page. Available at: https://advisera.com/27001academy/knowledgebase/how-to-define-context-of-the-organization-according-to-iso-27001/ [Accessed 10 March 2023].

Leadership and Commitment for ISO 27001 Requirement 5.1. n.d. isms.online. Web page. Available at: https://www.isms.online/iso-27001/leadership-commitment/ [Accessed 15 March 2023].

Meyer, D. 2018. What the GDPR will mean for companies tracking location. Web page. Available at: https://iapp.org/news/a/what-the-gdpr-will-mean-for-companies-tracking-location/ [Accessed 26 February 2023].

Müge Fazlioglu. What's new in the WP29 guidelines on DPIAs? 2017. Iapp. Web page. Available at: https://iapp.org/news/a/whats-new-in-the-wp29-guidelines-on-dpias/ [Accessed 27 April 2023].

Recital 30 Online identifiers for profiling and identification. n.d. gdpr.eu. Web page. Available at: https://gdpr.eu/recital-30-online-identifiers-for-profiling-and-identification/ [Accessed 15 February 2023].

DIRECTIVE (EU) 2019/1937 OF THE EUROPEAN PARLIAMENT AND OF THE COUNCIL on the protection of persons who report breaches of Union law.

Recital 155 Processing in the employment context. n.d. gdpr.eu. Web page. Available at: https://gdpr.eu/Recital-155-Processing-in-the-employment-context/ [Accessed 22 February 2023].

REGULATION (EU) 2016/679 OF THE EUROPEAN PARLIAMENT AND OF THE COUNCIL

5 Step Guide to Check if Your CCTV is GDPR Compliant. 2021. Data Privacy Manager. Web page. Available at: https://dataprivacymanager.net/five-step-guide-to-gdpr-compliant-cctv-video-surveillance/ [Accessed 14 April 2023].

Trans-Atlantic Data Privacy Framework. 2022. The European Commission. PDF document. Available at: https://ec.europa.eu/commission/presscorner/api/files/attachment/872132/Trans-Atlantic%20Data%20Privacy%20Framework.pdf.pdf [Accessed 5 March 2023].

Recital 113 Transfers Qualified as Not Repetitive and that Only Concern a Limited Number of Data Subjects. n.d. Intersoft consulting. Web page. Available at: https://gdpr-info.eu/recitals/no-113/ [Accessed 29 April 2023].

What are my rights? n.d. European Commission. Web page. Available at: https://commission.europa.eu/law/law-topic/data-protection/reform/rights-citizens/my-rights/what-are-my-rights_en [Accessed 21 January 2023].

What data can we process and under which conditions? n.d. European commission. Web page. Available at: https://commission.europa.eu/law/law-topic/data-protection/reform/rules-business-and-organisations/principles-gdpr/overview-principles/what-data-can-we-process-and-under-which-conditions_en [Accessed 20 January 2023].

What is a RoPA? GDPR requirements for record of processing activities. 2022. Osano. Web page. Available at: https://www.osano.com/articles/what-is-a-ropa-gdpr-requirements-for-record-of-processing-activities [Accessed 15 March 2023].

White, B. 2022. Transfer Impact Assessments (TIAs). Web page. Available at: https://harperjames.co.uk/article/transfer-impact-assessments-tias/#section-4 [Accessed 4 March 2023].

WP 250 ARTICLE 29 DATA PROTECTION WORKING PARTY. 2018. PDF document. Available at: https://ec.europa.eu/newsroom/article29/redirection/document/49827 [Accessed 27 April 2023].

WP256 ARTICLE 29 DATA PROTECTION WORKING PARTY. 2017. PDF document. Available at: https://ec.europa.eu/newsroom/just/document.cfm?doc_id=48798 [Accessed 23 April 2023].

WP257 ARTICLE 29 DATA PROTECTION WORKING PARTY. 2017. PDF document. Available at: https://ec.europa.eu/newsroom/just/document.cfm?doc_id=48799 [Accessed 23 April 2023].

Appendix 1/1

SURVEY QUESTIONS /ANSWERS ADDRESSED TO SECURITY EXPERT AND CEO OF COMISSIONER ORGANIZATION

Questions about ISO 27001 implementation answered by Steve Durbin, cybersecurity expert.

Question	**Answer**
What is the most frequent pitfall that organizations encounter when they integrate ISO compliant ISMS?	There's three I see all the time: *"Concrete lifejacket syndrome"* – you build a great looking ISMS, but it fits the business so badly it's pulling you down instead of lifting you up. *"ISO in name only (IINO)"* – your ISMS looks great on paper, you've ticked all the boxes, but the business doesn't actually follow the processes, they just pay lip service to it. This is commonly part of the previous one, with the business noncompliance being a strategy staff adopt in order to meet management demands and still get their job done. You tend to only find out when there is a major security breach. *"Department of no"* – one business unit is leading on implementation, and they follow the rules (usually ICT). Everyone else dealing with them finds they can't get things done because the rules are too strict, so they get a "no" to anything they ask. You then get "shadow" departments forming and the whole thing is undermined. Commonly, the department responds to the shadows being set up by trying to get stricter business rules, which leads to board-level arguments, and silos forming. All of these tend to stem from not understanding the organization properly – there's a reason the ISO27001 standard starts with "Context of the organization".

Appendix 1/2

Question	Answer
Do you recommend narrowing the scope of ISMS integration to core production processes for starting organizations?	Yes – because you're much more likely to fail if you try to take too big a bite, especially when starting out due to inexperience. Commonly, I'd recommend dealing with a single business unit to start out, learn from that before expanding. However, the organizational complexity of doing a small part and no other can be challenging, so the risk/reward balance needs to be looked at very carefully.
If an organization faces competency issues, would you recommend utilizing external consultancies, hiring new competencies or training existing employees?	If you don't get the organizational capability to deliver, you will just keep paying consultants forever. This is where the public sector in the UK is, because it won't pay properly for expertise. Not complaining, they are my main customers for this reason! The best way is to train your own people, but you need to be able to pay to retain them. If you can't pay to retain them, you also won't be able to hire competent people. Because an ISMS needs to be a living document, if you don't have the internal understanding maintaining the ISMS will be challenging, or costly due to needing regular consultant engagement.
Can you define under what circumstances an organization objectively needs to implement ISO 27001?	The only time it's objectively needed is if the business needs it to bid for contracts and the like, or it's mandated by law; for example, public sector frameworks commonly require ISO27001 and ISO9001 to be in place before you can even bid for them. There are also some regulations that require you to have a certification for risk, but these commonly specify their own. For example, PCI-DSS if you compare it with ISO27001 is hauntingly familiar…

Appendix 1/3

Question	Answer
Would you agree that ISO27001 compliance slows down organizations growth and does not necessarily mean that organization is secure? Does lack of baseline CIA security in the standard is compensated by certification body risk appetite assessment?	No to the first part – but I would state that badly implemented ISO27001 can have these effects (see q1 response). Good implementations actually streamline processes because they provide clarity and simplicity. The first ISMS I implemented, for example, we simplified the staff security policy to a single page – because we were using behavioral controls not legalistic ones. Think of it as the foundation for a building – a good foundation can allow you to build higher and better with ease, a bad one means you're trying to compensate for the previous neglect (q.v. the Tower of Pisa). There's no "baseline CIA security in the standard" for a reason – because any baseline wouldn't necessarily fit the business. Take CyberEssentials as a standard, for example – that mandates that all software is supported and regularly patched. If you're in the Nuclear industry, you're not allowed to patch without major security assessment, and in fact they are still using software and machines from the 1970s because upgrading is impractical. Similarly for medical devices – updating them can void their certification. If you ever have an MRI scan, have a look at the screen on the device as you're going in. I'll put money on it being Windows NT 4.0 or Windows XP!

Appendix 1/4

Question	Answer
What risk assessment methodology would you recommend in context of the standard?	It's purely a business choice again. ISO27001 section 6 discusses what you need for the assessment. I'd not recommend having a separate risk assessment methodology from the one used by the whole business, as it's confusing. Most people find a simple risk matrix is the easiest way to explain to the target audience, executives… As you're talking systems here, a system-based risk method is also best for the wider organization discussion, but component-based at the local system level.
What information security objectives should the company plan first? What criteria for measurement might be used to assess progress to objective?	The ones that are likely to cost them… Seriously, you should always start with the biggest risks to the business if you can – so look at potential financial and reputational impacts and start with the highest cost and risk ones. The only exception is if you're building small to learn – in which case you'd possibly be limited to what's in your initial scope.
Are there any frameworks that can facilitate ISMS implementation? What are they?	COBIT or ITIL provide very good basics for implementing an ISMS. I've not really encountered any others in the wild. However, these are subject to the same limitations and issues as ISO27001 itself, and can themselves be too proscriptive

Appendix 1/5

Questions about privacy answered by Dyann Heward-Mills, CEO

Question	**Answer**
What are the most frequently encountered privacy issues for recently founded organizations?	Lack of awareness of obligations. Limited resources to deal with requirements. High complexity even when business is small scale or limited geographical application. E.g. an amateur app developer or local ecommerce business can have the same level of risk of a large multinational depending on processing activity.
What privacy issues organizations should address in the first place?	Know your data processing: Keeping ROPAS and Data Maps. Setting the tone at the top. If Exec/C-suite do not take obligations seriously this attitude will percolate throughout the business. Establish an independent and robust compliance framework including oversight from a DPO or Senior Responsible Person.
Does compliance with GDPR mean compliance with most privacy laws of the world?	Generally GDPR is considered the gold standard in data protection. However, it is important to understand that, from an EU perspective, the GDPR is the floor not ceiling and some EU jurisdictions may set higher standards. In a similar vein, other regions and non-EU jurisdictions are building their own frameworks and laws some of which may set higher standards than the GDPR. Important to think globally and act locally when it comes to privacy laws.

Appendix 1/6

Question	Answer
What is the recommended way to comply with lawfulness requirements? Is freely given consent can justify lawfulness in any case? Are there any exceptions?	It is important to consider all lawful basis for processing data. At times consent may not be the most appropriate ground especially when there is an imbalance of power between the parties. In scenarios where consumer choice is paramount and the only basis for data processing e.g. marketing freely given consent is typically the only lawful ground and must be evidenced
If an organization is using cloud to store or process sensitive personal data are there any additional requirements imposed? Do cloud providers have access to that sensitive information?	Generally cloud providers would be processing data on behalf of organisations so would not be controllers of the data. The Controller has ultimate responsibility to ensure requirements are met and would typically seek to impose these standards on the cloud provider via a written contract. The balance of power however can at times remain with the Processer albeit the obligation and responsibility remains with the Controller. This can cause conflict and significant exposures/liabilities in the event of a data breach or other privacy infringement. Often cloud providers have access to sensitive information if they perform support services to customers processing sensitive data and depending on how their technology is configured. See EDPB audit and recommendations on use of cloud providers by public authorities. Often the expectations on public authorities will over time extend to private organizations also.

Appendix 1/7

Question	Answer
What mechanisms do companies implement to provide privacy notices and are there any recommendations to do that effectively?	Companies need to conduct regular audits, compile and update ROPAs and have appropriate review cycles to provide privacy notices. They need a high level of engagement and participation from business teams and functions for an efficacious and effective notice process.
How to demonstrate security of data to regulators? What certifications might be used for those purposes?	See ISO requirements. Also consider privacy by design steps and close interaction between the security and privacy function as opposed to operating in silos.
In what cases codes of conduct and certification mechanisms are useful?	Codes of conducts such a Binding Corporate Rules can be useful in demonstrating high standards but can, without ongoing checks and balances, flatter to deceive

Appendix 2/1

ISO 27001 IMPLEMENTATION ROADMAP.

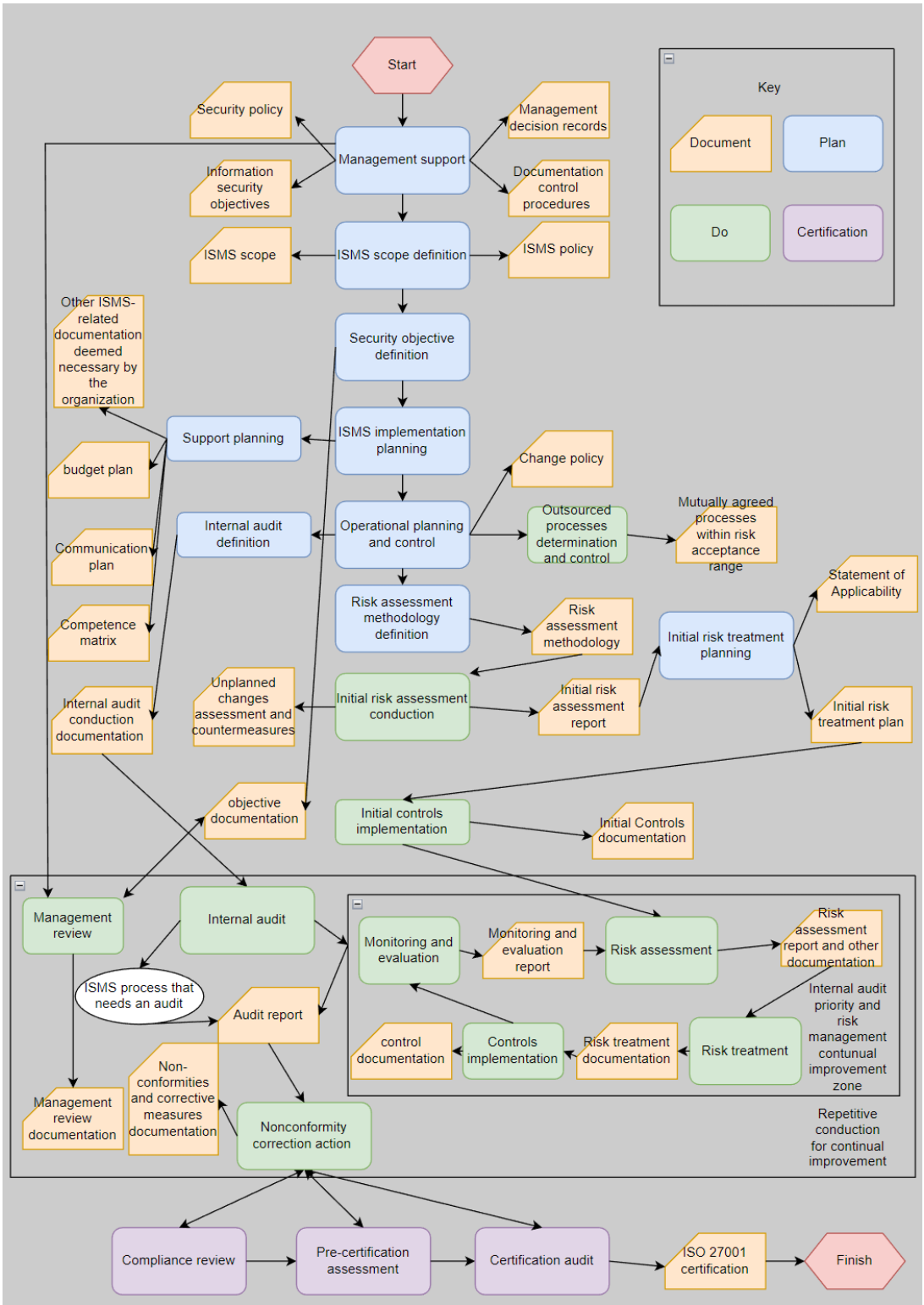

Figure 5. Scheme of ISO27001 compliant ISMS implementation