Satakunnan ammattikorkeakoulu
Satakunta University of Applied Sciences

NEA KEITAANPÄÄ

Regulations in Identity and Access Management

DEGREE PROGRAMME IN ELECTRICAL AND AUTOMATION ENGINEERING

2022

Author(s) Keitaanpää, Nea	Type of Publication Bachelor's thesis	Date January 2022
	Number of pages 34	Language of publication: English

Title of publication
Regulations in Identity and Access Management

Degree Programme
Electrical and Automation Engineering

Abstract

The need for Identity and Access Management solutions for organizations are growing vastly. The purpose of the thesis is to bring knowledge for organizations on what Identity and Access Management is, which regulations are important when Identity and Access Management is used, basic knowledge on common practices regarding the regulations and how these need to be taken into consideration when implementing the solution.

In the beginning of the thesis, it is explained what Identity and Access Management is and what the benefits of IAM are for organizations. Then deep dive is made on the regulations needed in IAM solutions. Last part of the thesis called 'common practices' investigates the basics of what an organization should know and do regarding the regulations introduced and what the process is from the vendor's perspective when the IAM solution is implemented.

The conclusions for this thesis are that IAM is a crucial part of Information Technology security, and it is a big entirety - which requires many different laws and regulations to be complied with it. The biggest and most important one is the General Data Protection Regulation which needs to be complied in any organization which handles customer data. When starting an IAM solution implementation project, the compliance work starts from the organization buying the solution, then joining forces with a vendor suited the best for this solution.

Keywords
IAM, Identity and Access Management, GDPR, Public Information Management Act, PiTuKri, Katakri

CONTENTS

LIST OF SYMBOLS AND TERMS

AD = Active Directory

AM = Access Management

CCM = Cloud Controls Matrix

CIAM = Customer Identity and Access Management

CRM = Customer Relationship Management

CSA = Cloud Security Alliance

eIDAS = electronic Identification, Authentication, and trust Services

ERP = Enterprise Resource Planning

EU = European Union

GDPR = General Data Protection Regulation

HR = Human Resources

IAM = Identity and Access Management

IdM = Identity Management

IT = Information Technology

Katakri = Information security audit tool for authorities
(Kansallinen turvallisuusauditointikriteeristö)

M&A = Mergers and Acquisitions

MFA = Multi-Factor Authentication

NSA = National Security Agency

PiTuKri = Criteria to Assess the Information Security of Cloud Services
(Pilvipalveluiden turvallisuuden arviointikriteeristö)

SaaS = Software as a Service

SSO = Single Sign-On

1 INTRODUCTION

In recent years, the demand for secure access has increased dramatically. Businesses must accommodate the access needs of a broad set of users across a wide range of applications while maintaining acceptable security. However, even minor misuse of user passwords could result in tremendous security risks. (StealthLabs 2020.)

Without a suitable management system, user information can soon become a complex issue to track, whether it is passwords or email addresses. With so much data to store, analyze, and communicate, many scenarios requiring changes to access rights emerge on a daily basis. Access control solutions that are dependable and versatile are required to meet these objectives across a wide range of on-premises and cloud applications. This is where Identity and Access Management (IAM) comes into action. (StealthLabs 2020.)

As Identity and Access Management is based on user data, there are certain regulations and laws which are needed to use in order to be compliant. This thesis is looking at these regulations and laws from Finland's perspective and as in many IAM solutions, the vendor is working as a Data Processor and the organization buying the solution is a Data Controller, the thesis is done from both perspectives for the scope of the thesis.

This thesis is to give guidance on what Identity and Access Management is - what are some of the most common regulations regarding it - and what does an organization need to take into account when considering the need of an Identity and Access Management solution implementation. It is covering IAM, General Data Protection Regulation (GDPR), different kinds of audit criteria, and an Act on Information Management in Public Administration as well as common practices around the topics.

2 IDENTITY AND ACCESS MANAGEMENT

Identity and Access Management (IAM) systems can be divided into two categories: Identity Management (IdM) and Access Management (AM). IdM is a system for managing user profiles and permissions. Workflows, for example, are used to handle providing and de-provisioning capabilities. The usage of user-profiles for access control is known as AM. It handles things like user authentication, Single Sign-On (SSO) and authorization. (Efecte n.d.)

Identity management is one of the most crucial parts of IT security. As traditional perimeter boundaries loosen and employee turnover rises, controlling who has access to what, when and where is more difficult than before. Single Sign-On, LDAP, MetaDirectories, Virtual Directories, automated provisioning/de-provisioning of user accounts and privileges, and role management are all part of a bigger solution that is becoming more important as threats and regulatory requirements grow. (Isaca n.d.)

Identity and Access Management is the discipline that allows the correct users to have access to the right resources at the right time and for the right reasons. IAM fulfills the need to assure proper resource access in increasingly diverse technology environments while also meeting more demanding compliance requirements. IAM is a critical project for any businesses. IT is becoming more business-oriented, and it necessitates business abilities rather than merely technical knowledge. (Gartner n.d.)

2.1 Customer Identity and Access Management

Customer Identity and Access Management (CIAM) is the process of granting end users access to a company’s digital properties, as well as governing, collecting, analyzing, and securely storing data for those users. CIAM sits at the intersection of security, customer experience and analytics. It is vital to provide a simple, seamless manner for users to onboard and log in for increasing conversions and client loyalty. A solid security policy and compliance with data privacy laws require safeguarding sensitive data from unauthorized intrusion and taking efforts to avoid data breaches.

(Poza 2021.) Figure 1 shows an overview of Customer Identity and Access Management.

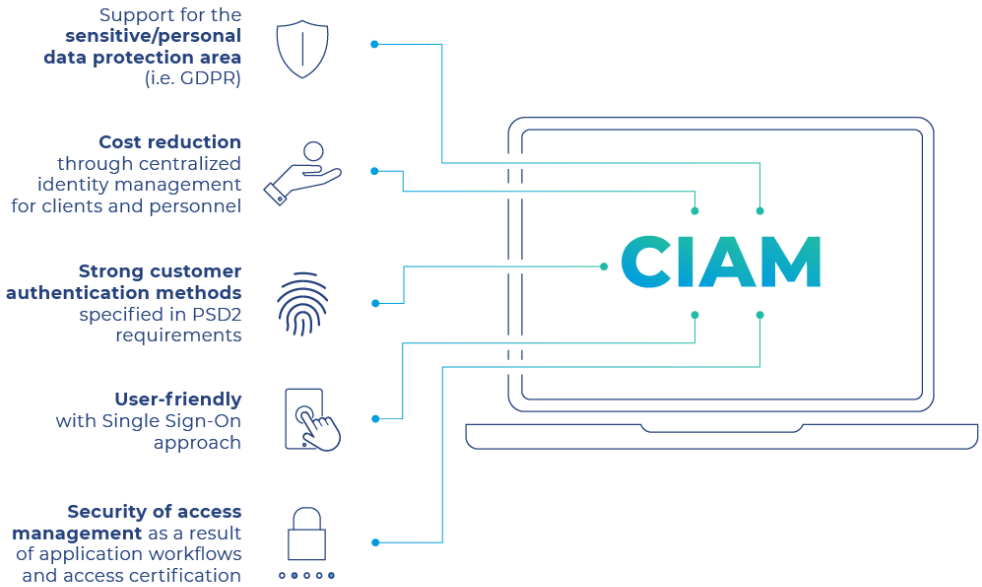

Figure 1. Overview of CIAM (Comarch n.d.).

Traditional Identity and Access Management solutions are frequently compared to Customer Identity and Access Management solutions. Both IAM and CIAM systems include access restrictions, MFA and SSO capabilities to provide strong security and better user experience. While the two solutions are conceptually similar, they are designed for different audiences and serve different functional and operational needs. (Cyberark n.d.)

Employees and contractors use traditional IAM solutions to authenticate and approve access to corporate applications and IT systems. They are built to interact with corporate Human Resources (HR) and IT systems and function with enterprise directory services like Active Directory (AD). (Cyberark n.d.)

CIAM solutions, on the other hand, are designed to authenticate and authorize clients who want to use public-facing applications and services. They are designed to handle millions or even billions of users. They are built to work with a range of sales, marketing, and business analytics platforms and support social login. They are also

subject to severe data privacy and consent requirements, such as the GDPR. (Cyberark n.d.) The comparison between IAM and CIAM is shown in figure 2.

Traditional IAM	Customer IAM
Manage **employee identity** within a corporation.	Manage **customer identity** on digital, customer-facing, multichannel sites (web, mobile, IoT).
Users are **registered by their company**, with key profile data filled in by HR or IT.	Users **register themselves** and generate their own user-specific data.
Authentication against internal **directory services.**	Authentication against **public services** like OpenID and social media, as well as directory services and external credential verification services.
Users are known and captive: employees, contractors, partners. **Identity may be assumed.**	Users are **unknown** (until registration) and may create multiple and fake accounts. **Identity cannot be assumed.**
Workforce users are **more tolerant** of latency and poor performance because they often **do not have an alternative.**	Customers and prospects have **very low tolerance** for poor performance and **have many attractive alternatives.**
Scalable from **10s to 100 000s of users**, one identity each.	Scalable up to **100s of millions of users** with up to billions of consumer identities.
Traditional identity provider (IdP) is **typically one central internal IT system.**	**Many decentralized identity providers:** social login through Facebook, Google, LinkedIn, etc., as well as traditional login.
Many heterogenous IT systems, on a **closed, corporate network.**	Many heterogenous IT systems, on **public networks (Internet)**.
Employee profile data collected for **administrative and operational purposes.**	Customer profile data collected for **highly critical business purposes** (transactions, marketing, personalization, analytics, and business intelligence).
Integration with **HR and ERP systems.**	Integration with **a broad landscape of marketing and sales automation** technology, **analytics systems**, and security and **compliance** solutions.
Management of personal data and user privacy/preferences/consent happens only within a tightly **controlled, homogenous corporate environment.**	Handling of personal data subject to a **broad variety of privacy and data protection regulations** that require enabling users to view, modify, and revoke preference and consent settings.

Figure 2. Differences between IAM and CIAM (Akamai 2019).

2.2 Benefits of IAM

With the implementation of IAM tools, IT administrators can deliver a unique digital identity for each user that includes a set of credentials. Users no longer have to manage dozens of accounts for various company applications or resources, which is a tremendous step forward. End users can access corporate networks with IAM systems regardless of their location, time, or device. Furthermore, the SSO approach allows

users to use their unique identity to access Cloud-Based, Software as a Service (SaaS), Web-Based and Virtual Applications. (StealthLabs 2020.)

IAM solutions prevent several password-related concerns, such as keeping passwords in notes and forgetting user credentials, in addition to making sign-in process quicker. Password management capabilities in IAM products assist security administrators in implementing password best practices such as frequent password updates and strong authentication techniques such as Multi-Factor Authentication (MFA), biometrics, or role-based access. (StealthLabs 2020.)

Businesses can use IAM solutions to implement appropriate security policies across all systems, platforms, applications, and devices. This makes it easy to spot security flaws, revoke access when necessary and eliminate inappropriate access privileges. Employees can access systems based on their individual roles with IAM systems, but privileges cannot be escalated without consent or role change. As a result, the risk of insider security threats is greatly reduced. (StealthLabs 2020.)

The most significant benefit of IAM – aside from increasing security posture – is that it increases the efficiency and effectiveness of security teams. Security administrators can utilize IAM technologies to grant user role access privileges based on the principle of least privilege. Users such as clients, workers, contractors, third-party vendors, and partners can be organized quickly and efficiently with only the appropriate access. Furthermore, IAM systems employ automation, artificial intelligence, and machine learning to assist administrators in automating many important areas of identity management, authentication, and authorization. (StealthLabs 2020.)

Organizations are held accountable for managing access to consumer and employee information under government data requirements such as the GDPR. Data security, privacy, and protection mandates, such as who has access to information and how that access is secured, are all closely tied to IAM in the legislations. As a result, IAM solutions assist businesses in achieving regulatory compliance as well as industry best security practice standards. (StealthLabs 2020.) Additionally, operational expenses can be reduced by taking a strategic approach to managing IAM, which includes

automation and right sizing of your business (Wilhelm n.d.). Figure 3 displays benefits of IAM.

Figure 3. Key benefits of IAM (StealthLabs 2020).

2.2.1 Identity governance

IAM also gives vital insight on how employees and customers have accessed applications such as who logged in – when it happened – and what data they had accessed. This can provide convenience in addition to security. IAM solutions include MFA tools and processes as well as self-service capabilities that allow users to manage their own access information. This is all part of the IAM strategy and policies established by an organization and the platform will include auditing capabilities to verify that internal policies and obligatory regulation such as GDPR are always followed. (Opentext 2018.)

2.2.2 Cloud services

As with many areas of GDPR, there is a lack of clarity about how enterprises should setup cloud services in order to be GDPR compliant. The EU Article 29 (EU-Justice) Working Party's code of practice for cloud computing, comes the closest to being definitive although it is not binding. However, because the provider is now liable for processing, the GDPR changes how enterprises must deal with cloud providers. (Opentext 2018.)

According to research, the typical European company utilizes 608 cloud applications, thus getting cloud compliance right is critical. It is impossible to administer cloud services in a compliant manner without IAM. For example, integrating on-premises workloads with cloud-based workloads necessitates the secure and compliant sharing with the chosen platform of personal information on users, such as personal details, permissions, group memberships and so on. GDPR recommends that cloud services should be underpinned by new contractual partnerships, but IAM will be required to ensure that these arrangements are appropriately enforced. (Opentext 2018.)

3 REGULATIONS IN IAM

3.1 General Data Protection Regulation

General Data Protection Regulation is a regulatory framework that establishes standards for the collecting and processing of personal data of European Union citizens. GDPR came into force in 2016, but it came into effect on 25 May 2018. (Frankenfield 2020.) GDPR is essential as it establishes a single set of rules for all EU organizations to follow and making data transfers between EU countries faster and more transparent. It also gives EU citizens more control over how their personal data is handled. (DeltaNet n.d.)

To comply with GDPR it must be ensured that personal data can only be accessed by authorized individuals for the specific reason for which it was gathered, and for the time period for which it was gathered. The regulation emphasizes data reduction. The amount of information kept on each individual, must be as small as possible. In terms of IAM, one approach to think about data minimization is to provide the least amount of access possible. While access must be limited, the organization cannot limit the authentication and authorization that may be used. Many companies are developing for example centralized SSO capabilities for all of their company assets. This appears to provide both user convenience and organizational security, but if implemented globally, it could be a potential GDPR problem. The risk is that users would get broad access to assets for which they are not authorized to. MFA will be required to ensure that the person is who they say they are and that they have access rights when dealing with personal data, even if this form of generic access is possible where personal and sensitive data is not involved.

3.1.1 Different roles in GDPR

Data Controller

Data Controller is a legal or a natural person, an agency, a governmental authority, or any other organization that alone or in conjunction with others, determines the goals

and means of processing personal data. They play a crucial role in decision-making. They have the final say and control over the reasons and goals for data collecting, as well as the means and methods of data processing. (GDPR EU n.d.)

Data Controllers oversee the most rigorous GDPR compliance. They must actively demonstrate full compliance with all data protection principles, according to Article 24 (EU-law (3)) of the GDPR. They also need to ensure that any processors they engage to process the data are GDPR compliant. They must show justice, lawfulness, and transparency, as well as correctness, data minimization, integrity, and storage as well as complete secrecy of personal data. Data Controllers can define the goals and methods of data processing alone or collectively with another party as Joint Controllers, according to Article 26 (EU-law (4)) of the GDPR. Joint Controllers must decide who will bear primary responsibility among themselves. (GDPR EU n.d.)

Data Processor

Data Processor might be a corporation, a partnership, or an individual. Data Processors will act on behalf of and under the authority of the applicable data controller, even if they make their own operational decisions. Unless required by law, a data processor must only process personal data pursuant to the controller's instructions, according to the Article 29 (EU-law (5)) of the GDPR. (GDPR EU n.d.)

Individual users have the right to claim compensations on both Data Controllers and Data Processors for damages. As the Data Processor always follows the instructions of the Data Controller, the Data Processor needs to inform the Data Controller if the instructions are against the law, or they cannot be followed. Any data breaches will be the responsibility of the Data Processor if they go against the Data Controller's instructions. As a result, Data Controllers and Data Processors must always ensure that they are following GDPR guidelines. (GDPR EU n.d.)

The Data Controller's employees are not considered as Data Processors. An individual acts as an agent of the Data Controller as long as they are acting within the extent of their employment obligations. In other words, the GDPR will consider them to be a part of the controller rather than a third party hired to process the data on the

Controller's behalf. (GDPR EU n.d.) In figure 4, the differences between Data Subject, Data Controller and Data Processor are explained.

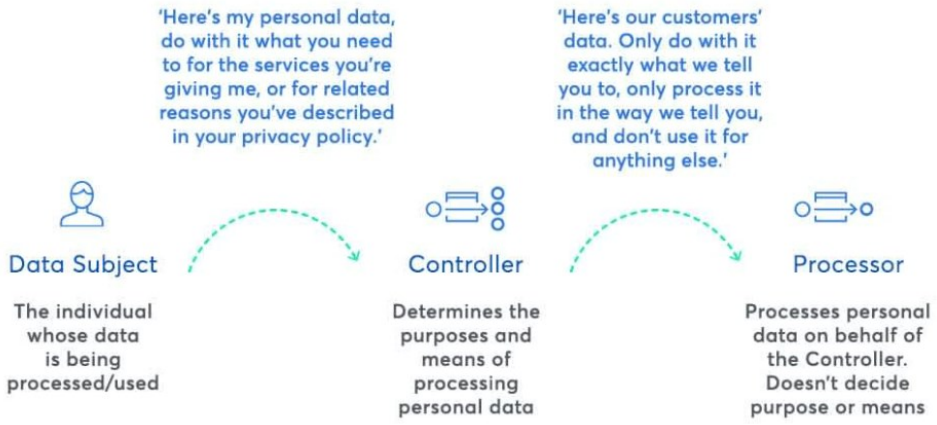

Figure 4. Differences between Data Subject, Data Controller and Data Processor (Badr 2018).

Data Subject

Any individual who can be recognized directly or indirectly, using an identifier such as a name, an ID number, location data or factors related to the person's physical, physiological, genetic, mental, economic, cultural, or social identity is referred to as a data subject. In other words, a data subject is a person whose personal information can be collected. (ATInternet n.d.)

3.1.2 Data processing

Personal data processing

The GDPR establishes strict criteria for the processing of personal data, including the obligation of "protection against unauthorized and unlawful processing". Through MFA and access policies, the only way to achieve this is through a centralized and uniform IAM platform. With this way, it is possible to ensure that only authorized users have access to certain resources. To simplify and strengthen internal access management, it may be worth considering using role-based authentication for

employees. Also, another factor to consider is that the IAM platform will require federated authentication in order to quickly provide and revoke approved access to partners and temporary workers. (Opentext 2018.)

Security of processing

The GDPR's Article 32 (EU-law (1)) outlines the security criteria for processing personal data. This includes the necessity to maintain processing confidentiality and integrity while also being able to swiftly restore access in the event of a compromise. The organization must be able to show that it is capable of doing this - and is doing it. It controls access to business networks and safeguards the data subject's and system user's identities. Furthermore, IAM enables the prompt restoration of systems by assisting in the rapid identification of whose personal data has been compromised by a breach. (Opentext 2018.) Figure 5 shows an addition to securing personal data.

Figure 5. Integrity and confidentiality in GDPR (Netfort n.d.).

3.1.3 Data minimization

The concept of data minimization is one of the most important parts of the GDPR. There should only be stored as much data as it is required for completing a processing task. IAM enables to having centralized control over all employee, customer and partner access and authorization information. It can be used to define not only for how long the access is permitted, but also for how long the data must be stored. This allows for the secure and timely deletion of user account information. IAM will assist on reducing this cybersecurity risk while complying with data minimization standards, as "Ghost accounts" are a large-scale system vulnerability that provides a backdoor for hackers. (Opentext 2018.)

3.1.4 Access to own information

According to Article 15 of the GDPR (EU-law (6)), customers must have access to their own data. This is something that, within in the EU, can be taken for granted these days. If one has many business lines or brands, and additional services have been added over time through mergers or acquisitions, there might be several separate identity domains with redundant user data. In order to comply with GDPR, a system should be created that allows end users to access their identification data regardless of where it is stored within the organization. (Ubisecure n.d.)

Authentication is another component of access. Article 24 (EU-law (3)) of the GDPR states that "appropriate technological and organizational measures" must be implemented to protect personal data, but it does not specify which steps must be taken, such as implementing MFA. Similar approaches are taken by other EU regulations, such as electronic Identification, Authentication, and trust Services (eIDAS) (European Commission). Furthermore, the lack of any specific technology in legislation should not be interpreted as a dismissive factor. Stronger authentication methods, such as MFA, would be a wise commercial and compliance option. If an organization is in the financial business and operates in the EU, the new Payment Services Directive 2 (EU-law (8)) and regulatory technical criteria for strong consumer authentication will compel to use strong authentication. (Ubisecure n.d.)

3.1.5 Right to erasure

The right to erasure also known as "Right to be forgotten", appears in Recitals 65 and 66 and in Article 17 (EU-law (9)) of the GDPR. The Article 17 states "The data subject shall have the right to obtain from the controller the erasure of personal data concerning him or her without undue delay and the controller shall have the obligation to erase personal data without undue delay". "Undue delay" is considered as about a month. The Right to be forgotten is linked to Article 15 (EU-law (6)) – right of access to personal information. An individual can request their data to be removed for any purpose whatsoever. (GDPR EU n.d.)

3.2 Act on Information Management in Public Administration

Act on Information Management in Public Administration (The Public Information Management Act) (906/2019) (Finlex (1)), came into effect on 1 January 2020. The purpose of the law is to ensure for authority's data a uniform, high-quality management, and secure data processing. It is important to implement the principle of transparency even better than before. The aim of the act is to pay more attention to the safe and efficient utilization of data and to promote the interoperability of information systems and data resources. In short, the purpose of the Public Information Management Act is for authorities to process data in a customer-oriented, uniform and information-safe manner in accordance with the principle of transparency. The act also contributes to the development of the digital society. (Seppo 2020.)

The Public Information Management Act sets its own requirements for information management and information security in organizations in public administration. The aim of the act is to promote uniformity of information management in a digitalizing operating environment. The most visible reform of the Information Management Act is the obligation for information management units to produce a clear description of the organization's extended information management. (Haapala n.d.)

The Act sets out clearer minimum requirements for what an organization must describe in the information management model, that defines and describes information management in its operating environment. According to the act, the responsibility for organizing information management clearly lies with the organization's management and in the future the management is responsible for ensuring that the information management unit defines – among other things – the responsibilities related to the implementation of information management. (Haapala n.d.)

The information management unit is a new concept introduced by the Information Management Act, which means an authority whose task is to organize information management in accordance with the act. Inter alia in the municipal sector, this means a municipality, an association of municipalities or an independent legal institution, each of which forms its own information management unit. (Haapala n.d.)

The goal of the information management model is to enable the versatile and smooth utilization of information in various services and processes. For this to be successful, the model must at least ensure that the organization has existing and up-to-date information on business processes, data resources, data sets, information systems and information security measures. (Haapala n.d.)

Many of these descriptions required at the minimum level can already be found in the information management units of organizations and they are worth utilizing when developing a new information management model and the corresponding activities. At the same time, it is useful to assess the consistency, timeliness, and equivalence of the description in the relation to the obligations provided for in the Information Management Act. (Haapala n.d.)

The information management model is not a nonrecurring project, because in the future the information management units will also have maintenance responsibility for the model and the operations in accordance with it. In the future, descriptions according to the information management model will be utilized, for example, when planning updates or implementations of information systems, but above all, the model will help to form an overall picture of the organization's information management. Therefore, it is worth starting from the beginning to build it as a resource for the organization. (Haapala n.d.)

The major benefits of information management are achieved when investing in information management, ensuring the quality of information, and utilizing information throughout the organization. With digitalization the emphasis on information lifecycle management is particularly emphasized, as initial decisions and actions play a crucial role in how information can ultimately be used. (Haapala n.d.)

3.3 Audit criteria

An audit is defined as the assessment of a subject matter against criteria. Criteria define the intended or required state or expectation for the program or procedure. Criteria

provide the stage for analyzing evidence and comprehending the report's findings, conclusions, and recommendations. Relevant, reliable, objective, and intelligible criteria are those that do not result in the omission of significant information, as applicable, within the audit objectives. Professional judgment is required to determine the relative value for each of these attributes to a specific engagement. (Yellowbook-CPE 2019.)

3.3.1 PiTuKri

The security assessment criteria for cloud computing (PiTuKri) are intended to improve the security of confidential information handled in cloud services. The criteria are primarily intended for official use, but it can also be used by other organizations. (National Cyber Security Centre 2019.) PiTuKri is to be used in Finland and has been composed from the Finland's national needs perspective.

PiTuKri aims to enhance the security of confidential information in situations where data is processed in cloud computing services. The criteria are intended to be a tool for cloud security evaluation. The national legislation reform projects have been considered in the drafting so that the criteria support legislation that was renewed at the beginning of 2020 (Finlex (1) & (2)). (National Cyber Security Centre 2020.)

In particular, BSI Cloud Computing Compliance Controls Catalogue (C5), the Cloud Security Alliance's (CSA) Cloud Controls Matrix (CCM) (Cloud Security Alliance), ISO270015 (International Organization for Standardization (1)) and ISO270176 (International Organization for Standardization (2)) standards as well as the Katakri criteria (Ministry of Foreign Affairs of Finland) has been used in the composition. The criteria also aim to support and concretize the introduction of the Ministry of Finance's public administration cloud services guidelines (Ministry of Finance). PiTuKri takes a stand on both the authority's national secrecy and those which has the security classification level IV (Ministry for Foreign Affairs). For data that is of higher protection level, security arrangements are only addressed when in connection with the evaluation of general applicability of cloud computing services. PiTuKri can

also be used to protect the public information of authorities and correspond to the demand of business and industrial life. (National Cyber Security Centre 2020.)

The criteria are meant to be used in the evaluation of cloud security. They can also be utilized to support the independent information security activities of cloud service providers. The criteria were created to support a variety of cloud computing services and use cases. The criteria should be applied in a case-by-case basis in order to be effective. (National Cyber Security Centre 2020.)

In most use cases, the assessment of the security of data handled in cloud services can be divided into sections that are the responsibility of the customer and the cloud service provider. The customer is typically responsible for both the cloud service's customer system and the customer's other processing environments. Figure 6 shows the segmentation of responsibilities for different processing environments. (National Cyber Security Centre 2020.)

In most cases, the criteria's requirements should only be applied to the part that the cloud service provider is responsible for, in some cases to both the service provider and the cloud service customer's parts, and in some cases, just to the part that the customer is responsible for. The security assessor, cloud service provider and cloud service customer all need to have satisfactory qualifications in order to use the criteria appropriately. (National Cyber Security Centre 2020.)

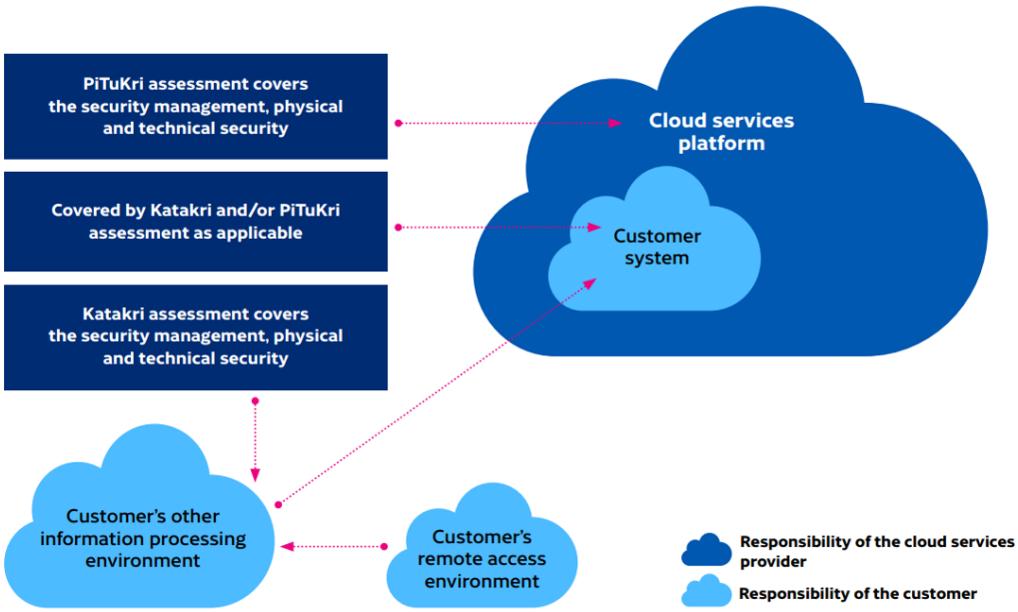

Figure 6. Division of responsibilities for processing environments (National Cyber Security Centre 2020).

3.3.2 Katakri

Katakri is a security audit tool for authority information, and it can be used to estimate the target organization's capability to protect national or international classified information (Finlex (2)). Katakri combines national regulation and international obligation based on minimum legal acts. Katakri in itself does not set unconditional requirements for information security (Finlex (1)), but the requirements combined in it are based on the legislation effective and the international information security obligations binding Finland. The main sources of requirements based on international legislation are the Act on Information Management in Public Administration (Finlex (1)) and the Government Decree on Security Classification of Documents in Central Government (Finlex (2)), that are used in Finland in the protection of both nationally and internationally classified information. The EU safety rules (EU-law (2)) which contains the minimum standards and basic principles for EU classified information have been used as the international source. (National Security Authority 2020.)

Katakri can be used as an audit tool when evaluating the company implementation of security arrangements in the corporate security report and security assessments of public authorities' information systems. Katakri can also be used to help businesses, communities as well as other security work, in developing them. The assessment of security arrangements should be based on a systematic risk assessment. Security risk management must be pursued to implement a combination of security measures to achieve a satisfactory balance between user requirements, costs, and residual safety risk. (National Security Authority 2020.)

National and EU classified information protection requirements are largely the same. Individual differences appear in the references. Katakri can be used for evaluating the protection for both nationally and internationally classified information. The protection of non-classified national information may be mirrored to the requirements applicable of security class IV to an extent. Katakri is not intended to be used as such as a security requirement for public procurement.
(National Security Authority 2020.)

In public procurement, the exact requirements should be determined separately, considering the procurement requirement risks and special needs. An individual project may include also other requirements than the ones concerning Katakri processing and protection of classified information. The fulfillment of requirements not included in the Katakri can be assessed for example by the project-specific evaluation from the authority who owns the information.
(National Security Authority 2020.)

Katakri is divided into three subdivisions. The subdivision on security management (T) seeks to ensure that the organization has a functioning information security management system and adequate personnel security procedures for the protection of classified information. The subdivision on physical security (F) describes the security requirements for the physical environment in which the classified information is to be used. As for the subdivision on Information assurance (I), the safety requirements for technical computing environment are described. The requirements are described in a way that it allows different implementations. (National Security Authority 2020.)

Security Management (T)

The security management section deals with the methods by which safety and its management is implemented into the entire organization's activities. It covers administrative information security and staff security. Safety management requirements aim to ensure that the organization has a functioning information security management system as well as adequate procedures to ensure that the personnel working with authority's classified information are doing it properly. (National Security Authority 2020.)

Security management processes should be treated as a whole. The procedures should be proportionate to the information to be protected, on the basis of a risk assessment and the activities of the target organization. Appropriate use of the security management component requires an assessment allocation to that part of the organization that manages the computing environment, for example a subsidiary or equivalent. Especially for assessing the criteria for personnel security, it should be noted that the adequate implementation may vary between subjects. For example, the content in the instructions for personnel working in security class II data processing environment usually differs significantly from the general instructions for the entire organization. The organization shall ensure that the obligations for classified information are also observed in situations where information is processed on behalf of the organization. (National Security Authority 2020.)

Good security management includes procedures and in particular, risk assessment documentation. The plans and guidelines as well as the results of the evaluation and conclusions related to security management should be presented literary. It is advisable to supply the documents with the information on the implementation of the measures. Measures taken may demonstrate that the security management assessment has been productive. Documentation is something that can be made in textual form, such as an Intranet page or/and Enterprise Resource Planning (ERP) work order (ticket). (National Security Authority 2020.)

Physical Security (F)

Physical security refers to the implementation of technical and physical security measures in such a way that: unauthorized access to classified information is

prevented. It is possible to use physical security sector for assessing the measures taken to protect the physical security of national or international classified information (Vna 1101/2019, 9 § (Finlex (2)); KvTituL 588/2004, 10 § (Finlex (3)).
(National Security Authority 2020.)

Authorities' data must be processed and stored in premises which are sufficiently secure to meet the requirements of the data's confidentiality, integrity, and availability (L 906/2019, 15 § (Finlex (1)). For new premises, the physical security requirements and the definition of their functional specifications must be part of the design and construction of the premises. For existing premises, physical safety requirements must be implemented as perfectly as possible (2013/488/EU, II annex, paragraph 7 (EU-law (2)). (National Security Authority 2020.)

For physical protection of classified information, there are two types of physically protected security areas: administrative areas and security areas - this includes technically protected security areas. The physical security measures must be met before the security areas can be approved. The physical security risk assessment as well as individual security measures in security restricted area and the effectiveness of the multi-level protection, shall be re-evaluated at cyclic intermissions and in the context of each audit (2013/488/ EU, II annex, paragraph 11 (EU law (2)). Areas where international classified information is retained, is always approved by the National Security Agency (NSA) unit of the State Department and the Finnish Security Intelligence Service acting as its authority, or General Staff of the Armed Forces (KvTituL 588/2004, 4 § (Finlex (3)); 2013/488/ EU, 8. Article (EU law (2)). (National Security Authority 2020.)

The structure of the section for physical security is designed so that the minimum requirements for safety zones have been compiled for each safety zone to its own subchapters. With this redesigned structure it is possible for the auditor to see all the minimum requirements and additional information for the safety area under assessment in a structured way without having to go through different requirements as the minimum requirements are partly overlapping. The selection of the adequate security measures is always based on a risk assessment, but on the Target level-

column, which is added to the minimum requirements, shows a sufficient multi-level protection solution standard class or instruction.
(National Security Authority 2020.)

Information Assurance (I)

Katakri in the field of technical information security describes the requirements with which applied, are pursued to ensure the adequacy of security arrangements in the electronic security platforms for authority's classified information. The requirements are divided into telecommunication, information system and operational safety sections. For certain subject areas, for example management connections, wireless networks, remote access, and backup, the related requirements are grouped. (National Security Authority 2020.)

In situations where the goal of the organization is to get the information system competent authority's approval granted, the safeguarding implemented by the organization shall be adequate in relation to both of the organization's own and the competent authority's risk assessment. The role for risk assessment is also emphasized in change management. For example, new services or adding interfaces to an existing computing environment can bring risks that changes for which to reduce, it is justified to make changes also to the existing parts of the computing environment as well as security maintenance activities. (National Security Authority 2020.)

4 COMMON PRACTICES

4.1 GDPR

Mapping personal information. GDPR defines the concept of personal data very broadly: all information that can be linked to a person with reasonable effort is personal information. They do not have to be in any register, but all personal data are covered by the regulation. However, it makes sense to start with bigger data systems and move on to individual data that can be found in many places. At first finding out what all the personal information is in the organization and grouping it into meaningful aggregations such as employee information and customer contacts. (Korpisaari et al. 2018, XVII.)

Finding out the purpose and cleaning up the data. Once all the personal information for each entity is listed, defining why that information is needed in the organization. If some information is no longer needed, it is worth deleting it immediately. It is also a good idea to go through the data anyway and at least clear outdated or incorrect data. (Korpisaari et al. 2018, XVII.)

Making a risk assessment. Going through every entity in a thought process and thinking what harm it could cause to the people whose information is in question as if the data would for example be destroyed or fall into the wrong hands. Categorizing risks according to how plausible they are and how much damage it could cause. Planning measures to combat at least the most serious risks. (Korpisaari et al. 2018, XVIII).

Documentation. Listing all the results of the previous sections. All individuals have a lot of rights under the Data Protection Regulation. For example, anyone using any services can require the service provider to provide information processed about them. When all the data is documented, it is much easier to respond to the customer. (Korpisaari et al. 2018, XVIII.)

4.2 IAM

Evaluating the company's IAM maturity. How well-defined is the governance structure of the company? How well-integrated and optimized are the present business processes? Where are the data assets that are critical to the organization's success? Is IAM delivering business value - and if not – is there a plan in place to make it so? It is critical to select the correct solution provider partner for all of these metrics. (Egberink 2017.)

Prior to turning business needs into technology requirements, business needs must be identified. Getting IAM right is first and foremost a business issue; technology comes second. When there is a separation between the business and IT, IAM projects fail. Starting by creating a clear picture of both business and technical IAM procedures. What happens when an employee leaves or changes roles? How is granting access to systems handled in the organization? How are password resets done? IAM must reflect current business processes and play a part in optimizing them as organizations adapt, respond to Mergers and Acquisitions (M&A) as competition and business processes evolve. Too many organizations make this mistake of securing a flawed process and then wonder why their IAM initiatives are failing. (Egberink 2017.)

Identifying the key stakeholders. These range from key individuals to internal line of business managers. It is critical to get all of these individuals together right away to work out any strategic and practical difficulties. The fact that IAM is not an IT project will be highlighted through board-level sponsorship. Finding someone who understands and supports the need for more effective IAM and can push the initiative is a smart idea. (Egberink 2017.)

Making the most of all available resources and knowledge. Organizations that already have a partnership with a cyber security provider may want to expand it in order to boost IAM. However, generic security suppliers may not often have the depth of knowledge required to successfully implement IAM. The project's needed expertise could be a combination of internal capabilities and supplier capability, as well as ad hoc expertise from external consultants such as project managers. The correct solution

provider can connect all the skills needed, either via their own resources or through third-party contacts. (Egberink 2017.)

Establishing reliable data sources, such as payroll and HR systems, as well as customer relationship management (CRM) software. These will give the identification data that will be used to drive the IAM automation that is required for governance. Many IAM efforts fail from the outset because they assume data is correct and clean. (Egberink 2017.)

4.3 Information Management in Public Administration

Finding out what the Data Management Act is about in order to understand from what perspective the organization should approach it. Reading the Public Administration Information Management Act (906/2019) (Finlex (1)) helps to familiarize with the implementation. After this the conclusions should be:

- What are the requirements of the Information Management Act?
- What is the purpose of the information management model?
- How the information management model can be leveraged in the organization in operation? (Talentbase n.d.)

At the phase of planning, the objectives are defined even more precisely as well as limiting the content to match the organization objectives. At this point, finding out what things can be done internally and where external help can be used. Creating an information management model and operations according to it, requires collaboration between different experts. Prioritizing activities and identifying dependencies between projects so the correct people will be able to participate in the making on the implementation phase. The outcome of this phase is:

- The target state of the data management model is defined
- For the implementation of the project - which is required for the changes by the information management model – has been started, responsibility has been assigned and resourced
- The organization has a project plan that directs operations in the implementation phase. (Talentbase n.d.)

Finding out about the current readiness of the organization for creating a data management model in the implementation phase. Learning of the current situation for the following descriptions:

- Overall architecture descriptions
- System descriptions
- Process descriptions
- Caption
- Archiving plan
- Information management plan
- Information security measures
- Transfer of data
- Archiving of data. (Talentbase n.d.)

Describing also the current situation:

- How the responsibilities required to achieve the goals have been described?
- How are the different roles and members defined in terms of responsibilities?
- How are the procedures defined?
- How is the monitoring implemented? (Talentbase n.d.)

Once the current situation has been solved, the basis for the information management model has been completed. After this, it can be seen what changes need to be made to current situation and implementation of these changes can start. After the completion of the current status:

- Identifying the differences between the current mode and the target mode
- Updating the descriptions as needed
- Producing missing descriptions
- Implementing roles, responsibilities, and practices into the organization activities so that information management will continue to be implemented according to the information management model. (Talentbase n.d.)

In the target mode, the data management model serves as a description of the information management that the organization has implemented, so it helps to understand how information is managed in the organization. (Talentbase n.d.)

The Information Management Act obliges the Information Management unit to maintain an up-to-date information management model, so in future:

- Ensuring that regulations, injunctions, and guidelines monitoring are followed throughout the organization. (Talentbase n.d.)

4.4 Implementing an IAM solution

To implement an IAM solution, there are important things to consider. I have interviewed a Lead Service Architect and a Senior IAM Consultant in Company X regarding compliance, security controls and information security management in IAM solution implementation.

Compliance

The interviews show that the most important thing to consider when implementing an Identity and Access Management solution is to be GDPR compliant, the other requirements are mostly given by the customer for whom the implementation is made for. The used product dictates a lot in making sure to be GDPR compliant during the implementation but as most of the modern products already have the best practices built in, the technical side is not such a big problem anymore.

The challenges of considering the GDPR compliances are of course different on different projects, but the most common challenges regarding it are that the user data which is sent to the company responsible for the IAM solution, gets more data than what is really needed. As the Article 5 (EU-law (10)) of the GDPR refers to ‘purpose limitation’, which means that the data should be collected for specified, explicit and legitimate purposes only and the Article 5 also states that the data needs to be limited to what is necessary in relation of the purposes for which the data is processed - which refers to ‘data minimization’ (GDPR EU n.d.). Since the company in charge of the IAM solution is acting as a Data Processor, the Data Controller should give them only

the necessary amount of data and the amount of data received is not a responsibility of the Data Processor but the Data Controller. In cases where the Data Processor can tell that the data received is for example illegal, they need to inform the Data Controller but normally the Data Processor can trust the data it receives, and it will be processed as instructed. To resolve these challenges, the key is to minimise the data in the supplier's systems, documentation, openness towards the customer of the potential security issues and agreeing with them that how these are handled. Mitigating the risks for GDPR is to secure the data in all phases with technical solutions.

Security Controls

Database security control - the modern IAM solutions have the capability to encrypt the database data. But if that is not the case for the used solution, the data is still highly secure as a result of well-defined database management processes which include maintenance and backups of the database and of data center security controls.

For accessing the data, it is dependent on the product used, but for example database management has access to the database according to their own processes. In addition, the database owner normally has access to the database, and it is possible to access to the raw database as a maintenance personnel. In summary, the people who are able to access the data - are listed people who are the only ones needed to access it.

It is also possible to protect the data with company standard datacenter tooling and processes, limiting the access to servers and tools and using personal accounts, so from the logs it is possible to see who has logged into the systems.

Document lifecycle management control – Maintaining and handling the lifecycle of documentation is normally based on company standards and industry standard tools are used, for example storing the documentation in SharePoint. It is also possible to have an agreement with the customer how they would like the documentation to be handled. Documentation containing personal data has its own storing requirements.

Information Security Management

ISO27001 - Risk Management and Third-Party Risk Management are a part of a generic risk management which is handled via the standard company Risk Management Process. Project managers typically maintain the lists with classifications, and it is an essential part of the steering group meetings.

Human Resources Security contains obligatory project specific online trainings and for example banking, finance and healthcare do have their own project specific security trainings for the personnel working with the projects.

5 DELIBERATION

The main purpose of the thesis was to bring knowledge for organizations on what Identity and Access Management is, open some of the most important regulations regarding Identity and Access Management, basic knowledge on common practices regarding the regulations and how these need to be taken into consideration when implementing the solution. Any organization considering IAM solution for their company would get a quick deep dive on the subject from technical and legal perspective.

When getting to know and understanding better the regulations used with IAM, there are a lot of them, and not all were mentioned in this thesis as it would have been very perfunctory in that case. The biggest and most important regulation is the General Data Protection Regulation as any company that stores or processes user data in the EU must comply with it. Identity and Access Management is based on customer data, so this is an important regulation for anyone working with IAM. If an organization is not able to comply with the GDPR or there would be a data breach, they could face a fine which can be up to 4% of the organization's annual turnover or 20 million euro. As we can see from the interviews, the biggest problems that the professionals have faced regarding compliance is that there is too much data shared to the Data Processor than what a Data Controller should share, so this is a complex regulation for any organization. Furthermore, we can see that GDPR is in a big role in the solution, but it also requires much more than just the GDPR.

The most challenging part of the thesis was creating the interviews, as the interviews were based on company X's Security Baseline and a Security Baseline is a huge combination of information security controls used to ensure that companies fulfill the enterprise's declared security objectives. To collect the ones regarding the regulations covered in the thesis and IAM and bundle them up, was tricky work. However, the interviews with professional IAM personnel can be a big learning point for the organizations interested in an IAM solution for their organization, as it also addressed from the vendor's perspective, not only from the customer's.

To improve this thesis and take it a bit further, this could be used as a base for implementing an IAM solution and documenting how all of the mentioned laws and regulations were used in that solution. Furthermore, as every company should have the Security Baseline in place, which contains information security management, security controls, and compliances, this could be investigated even more deeply if there is more controls in the Baseline which are mandatory for an IAM solution, than what is mentioned in this thesis.

As the technological and sociological environment continues to rapidly develop, IAM will become an increasingly important element of our personal and professional lives in the future.

REFERENCES

Akamai 2019. CIAM vs. IAM: Why Traditional IAM Should Not Be Used for Customers. Cited 31.7.2021.
CIAM vs. IAM: Why Traditional IAMs Should Not Be Used for Customers | Akamai

ATInternet n.d. Data Subject. Cited 25.1.2022.
https://www.atinternet.com/en/glossary/data-subject/#:~:text=Data%20subject%20refers%20to%20any,economic%2C%20cultural%20or%20social%20identity.

Badr, A. 2018. Our role as a data controller and what it means for you. Cited 3.7.2021.
https://gocardless.com/blog/data-controller/

Cloud Security Alliance n.d. Cloud Controls Matrix (CCM). Cited 19.4.2021.
https://cloudsecurityalliance.org/research/cloud-controls-matrix/

CSA cloud security alliance n.d. Cloud Computing Compliance Controls Catalogue. Cited 19.4.2021.
https://cloudsecurityalliance.org/research/cloud-controls-matrix/

Cyberark n.d. Customer Identity and Access Management (CIAM). Cited 31.7.2021.
https://www.cyberark.com/what-is/ciam/

DeltaNet n.d. What is GDPR in simple terms? Cited 25.1.2022.
https://www.delta-net.com/compliance/gdpr/faqs/what-is-gdpr-in-simple-terms

Efecte n.d. What is Identity and Access Management (IAM)? Cited 3.7.2021.
https://www.efecte.com/about-iam

Egberink, R. 2017. Five Tips to Get Identity and Access Management Right – the First Time. Cited 3.7.2021.

https://www.oneidentity.com/community/blogs/b/identity-governance-administration/posts/five-tips-to-get-identity-and-access-management-right-the-first-time

EU-Justice n.d. European Commission Article 29. Art. 29 WP. Cited 23.5.2021. https://ec.europa.eu/justice/article-29/documentation/opinion-recommendation/index_en.htm

EU-law (1) n.d. General Data Protection Regulation Article 32. 2016/679 with its amends. Cited 23.5.2021. https://eur-lex.europa.eu/eli/reg/2016/679/oj

EU-law (2) 2013. Council security rules for protecting classified information. 2013/488/EU. Cited. 16.5.2021. https://eur-lex.europa.eu/legal-content/EN/LSU/?uri=CELEX%3A32013D0488

EU-law (3) 2016. General Data Protection Regulation Article 24. 2016/679 with its amends. Cited 8.6.2021. https://eur-lex.europa.eu/eli/reg/2016/679/oj

EU-law (4) 2016. General Data Protection Regulation Article 26. 2016/679 with its amends. Cited 8.6.2021. https://eur-lex.europa.eu/eli/reg/2016/679/oj

EU-law (5) 2016. General Data Protection Regulation Article 29. 2016/679 with its amends. Cited 8.6.2021. https://eur-lex.europa.eu/eli/reg/2016/679/oj

EU-law (6) 2016. General Data Protection Regulation Article 15. 2016/679 with its amends. Cited 19.6.2021. https://eur-lex.europa.eu/eli/reg/2016/679/oj

EU-law (7) 2016. General Data Protection Regulation Article 4. 2016/679 with its amends. Cited 19.6.2021.

https://eur-lex.europa.eu/eli/reg/2016/679/oj

EU-law (8) 2015. Directive on payment services in the internal market. 2015/2366 with its amends. Cited 19.6.2021.
https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX%3A32015L2366

EU-law (9) 2016. General Data Protection Regulation Article 17. 2016/679 with its amends. Cited 20.6.2021.
https://eur-lex.europa.eu/eli/reg/2016/679/oj

EU-law (10) 2016. General Data Protection Regulation Article 5. 2016/679 with its amends. Cited 30.12.2021.
https://eur-lex.europa.eu/eli/reg/2016/679/oj

European Commission n.d. eIDAS Regulation. Cited 19.6.2021.
https://digital-strategy.ec.europa.eu/en/policies/eidas-regulation

Federal Office for Information Security n.d. Criteria Catalogue C5. Cited 10.4.2021.
https://www.bsi.bund.de/EN/Topics/CloudComputing/Compliance_Criteria_Catalogue/Compliance_Criteria_Catalogue_node.html

Finlex (1) 2019. Act on Information Management in Public Administration. 906/2019 with its amends. Cited 10.4.2021.
https://www.finlex.fi/en/laki/kaannokset/2019/en20190906?search%5Btype%5D=pika&search%5Bkieli%5D%5B0%5D=en&search%5Bpika%5D=906%2F2019

Finlex (2) 2019. Government Decree on Security Classification of Documents in Central Government. 1101/2019. Cited 10.4.2021.
https://www.finlex.fi/en/laki/kaannokset/2019/en20191101

Finlex (3) 2004. Laki kansainvälisistä tietoturvallisuusvelvoitteista. 24.6.2004/588. Cited 10.4.2021.
https://www.finlex.fi/fi/laki/ajantasa/2004/20040588

Frankenfield, J. 2020. General Data Protection Regulation (GDPR). Cited 29.5.2021. https://www.investopedia.com/terms/g/general-data-protection-regulation-gdpr.asp

Gartner n.d. Identity and Access Management (IAM). Cited 25.9.2021. https://www.gartner.com/en/information-technology/glossary/identity-and-access-management-iam

Haapala, A. n.d. Uusi tiedonhallintalaki – näin se vaikuttaa Organisaatioonne. Cited 31.7.2021. https://www.canon.fi/business/insights/articles/uusi-tiedonhallintalaki-nain-se-vaikuttaa/?&utm_campaign=fi_ds_tiedonhall&utm_medium=cpc&utm_source=google&utm_content=&utm_term=&utm_source=google&utm_medium=cpc&utm_campaign=fi_tiedonhall&utm_content=110507497915&utm_term=tiedonhallintalaki&gclid=Cj0KCQjw6ZOIBhDdARIsAMf8YyGnPCgod4JLnrMM7b8USbGxaeL5LSnPTlX7JjMmQPnHbXvdHYcoksQaAucpEALw_wcB

International Organization for Standardization (1) 2013. ISO/IEC 27001:2013. Cited 19.4.2021. iso.org/standard/54534.html

International Organization for Standardization (2) 2015. ISO/IEC 27017:2015. Cited 19.4.2021 https://www.iso.org/standard/43757.html

Isaca n.d. Creating an End-to End Identity Management Architecture. Cited 25.9.2021. https://isaca-rtc.org/chapter-events/chapter-past-events/83-november-4-session-creating-an-end-to-end-identity-management-architecture

Korpisaari, P., Pitkänen, O. & Warma-Lehtinen, E. 2018. Uusi tietosuojalainsäädäntö. Helsinki: Alma Talent. Cited 18.5.2021.

Ministry for Foreign Affairs n.d. Valid information security agreements. Cited 16.5.2021.
https://um.fi/voimassa-olevat-tietoturvallisuussopimukset

Ministry of Finance 2019. Ministry of Finance's public administration cloud services guidelines. Cited 10.4.2021.
https://julkaisut.valtioneuvosto.fi/handle/10024/161294

National Cyber Security Centre 2019. Tunnetko jo Pitukrin? Cited 18.5.2021.
https://www.kyberturvallisuuskeskus.fi/fi/ajankohtaista/tunnetko-jo-pitukrin

National Cyber Security Centre 2020. PiTuKri. Pilvipalveluiden turvallisuuden auditointikriteeristö. Cited 10.4.2021
https://www.kyberturvallisuuskeskus.fi/sites/default/files/media/file/Pilvipalveluiden_turvallisuuden_arviointikriteeristo_PiTuKri_v1_1.pdf

National Security Authority 2020. Katakri 2020. Cited 16.5.2021.
https://um.fi/documents/35732/0/Katakri+-+2020_1218.pdf/ab9c2d4a-5031-3670-6743-3f8921dce8c9?t=1608302599246

Netfort n.d. GDPR Data Protection Requirements. Cited 14.8.2021.
https://www.netfort.com/gdpr-data-protection-requirements/

Opentext n.d. How Identity and Access Management helps to meet the data protection requirements of GDPR? Cited 23.5.2021.
https://blogs.opentext.com/how-identity-and-access-management-helps-meet-the-data-protection-requirements-of-gdpr/

Poza, D. 2021. What is CIAM? Cited 31.7.2021.
https://auth0.com/blog/what-is-ciam/

Seppo, T. 2020. Tiedonhallinta. Cited 11.7.2021.

https://www.kuntaliitto.fi/osallistuminen-ja-vuorovaikutus/tietoyhteiskunta/tiedonhallinta

StealthLabs 2020. Why Companies Need Identity and Access Management? Cited 3.7.2021. https://www.stealthlabs.com/blog/why-companies-need-identity-and-access-management/

Talentbase n.d. Julkishallinnon tiedonhallintamalli. Cited 31.7.2021. https://www.talentbase.se/wp-content/uploads/2020/06/Tiedonhallintamalli_opas_TB.pdf

Ubisecure n.d. General Data Protection Regulation & Customer IAM. Cited 19.6.2021. https://www.ubisecure.com/wp-content/uploads/2019/05/GDPR-and-Customer-IAM-Ubisecure-White-Paper-6.18.pdf

Wilhelm, J. n.d. Achieving cost efficiencies in identity and access management. Cited 3.7.2021. https://advisory.kpmg.us/articles/2020/iam-achieving-cost-efficiencies.html

Yellowbook-CPE 2019. What is audit criteria? Cited 23.1.2022. https://yellowbook-cpe.com/what-is-audit-criteria.html