Implementation of Microsoft 365 Copilot with Cybersecurity Considerations in Organizations

University of Turku
Department of Computing
Master of Science (Tech) Thesis
Information and Communication Technology,
Communication and Cyber Security Engineering
May 2026
Salla Sipilä

Supervisors:
Kim Blomberg (Twoday Oy)
Kaitai Liang (University of Turku)
Jouni Isoaho (University of Turku)

UNIVERSITY OF TURKU
Department of Computing

Salla Sipilä: Implementation of Microsoft 365 Copilot with Cybersecurity Considerations in Organizations

Master of Science (Tech) Thesis, 73 p., 7 app. p.
Information and Communication Technology,
Communication and Cyber Security Engineering
May 2026

Generative AI tools are becoming widely utilized assistants in organizations and this thesis aims to productize an implementation model for Microsoft 365 Copilot with cybersecurity considerations in organizational settings. The theoretical implementation model is created based on literature from Microsoft, Artificial Intelligence, adoption models, and regulatory requirements. The model is validated with qualitative study with questionnaire and mixed data analysis. Analysis consisted of thematic data analysis and descriptive statistics. The results of qualitative study and mixed data analysis findings indicate that as a baseline framework, the implementation model is feasible but fully successful productization requires strategic optimization across the themes that were identified. This thesis delivers an empirically validated blueprint for Microsoft 365 Copilot implementation productization, while demonstrating that enterprise AI adoption relies on bridging the gap between technical delivery, strategic leadership, and robust regulatory governance.

Keywords: Microsoft 365 Copilot, Microsoft, Generative AI, Cybersecurity, TOE, DOI, TAM, EU AI Act, NIS2

TURUN YLIOPISTO
Tietotekniikan laitos

Salla Sipilä: Implementation of Microsoft 365 Copilot with Cybersecurity Considerations in Organizations

TkK-tutkielma, 73 s., 7 liites.
Tietotekniikka, Tietoliikenne- ja kyberturvallisuusteknologia
Toukokuu 2026

Generatiiviset tekoälytyökalut ovat yleistymässä organisaatioiden avustajina ja tämän opinnäytetyön tavoitteena on tuottaa Microsoft 365 Copilotin käyttöönottomalli, joka huomioi kyberturvallisuuden organisaatioympäristöissä. Teoreettinen käyttöönottomalli on laadittu kirjallisuuden pohjalta, jossa yhdistyy Microsoftin, tekoälyn, käyttöönottomallien ja lainsäädännöllisten sääntelyiden kirjallisuus. Mallia validoitiin laadullisella tutkimuksella, jossa käytettiin kyselyä sekä data-analyysiä. Analyysi koostui temaattisesta data-analyysistä ja kuvailevasta tilastotieteestä. Laadullisen tutkimuksen tulokset ja data-analyysin havainnot osoittavat, että ylätason ohjeistuksena käyttöönottomalli on toteutettavissa, mutta täysin onnistunut kaupallistaminen edellyttää strategista optimointia tunnistettujen teemojen osalta. Tämä opinnäytetyö tarjoaa empiirisesti validoidun toimintamallin Microsoft 365 Copilotin käyttöönoton tuotteistamiseksi ja osoittaa samalla, että tekoälyn onnistunut käyttöönotto organisaatiossa riippuu teknisen toteutuksen, strategisen johtajuuden sekä vahvan lainsäädännöllisen sääntelyiden hallinnan saumatonta yhteensovittamisesta.

Asiasanat: Microsoft 365 Copilot, Microsoft, Generatiivinen tekoäly, Kyberturvallisuus, TOE, DOI, TAM, EU AI Act, NIS2

Contents

1 Introduction **1**

1.1 Commissioning Organization 1

1.2 Research Problem and Questions 2

1.3 Thesis Structure 3

2 Literature Review **4**

2.1 Overview of Artificial Intelligence 4

2.1.1 Artificial Intelligence 4

2.1.2 Generative AI 5

2.1.3 Large Language Models 6

2.1.4 AI Agents 7

2.2 Enterprise Use 8

2.2.1 Adoption Models 9

2.2.2 AI Roadmaps 12

2.3 Legislation 13

2.3.1 NIS2 13

2.3.2 EU AI Act 15

2.4 Microsoft's Artificial Intelligence and Security 16

2.4.1 Copilot Products 17

2.4.2 Microsoft 365 Copilot 20

2.4.3 Security, Governance & Compliance 23

3 Research Methods **29**

3.1 Literature Review 29

3.2 Implementation Model 30

3.3 Qualitative Research & Analysis 31

4 M365 Copilot Implementation Model **37**

4.1 Strategy 38

4.2 Plan 41

4.3 Pilot 43

4.4 Rollout 44

4.5 Monitor 46

5 Validation **48**

5.1 Qualitative Study Results 49

5.1.1 Thematic Data Analysis 49

5.1.2 Descriptive Statistics 64

5.2 Qualitative Study Limitations 67

6 Discussion **68**

6.1 Evaluation of the Implementation Model 68

6.2 Future Work 69

6.3 Thesis Limitations 70

7 Conclusion **72**

References **74**

Appendices

A Qualitative study questions **A-1**

B Declaration of the Use of AI **B-1**

List of acronyms

AI Artificial Intelligence

AIMS Artificial Intelligence Management System

AML Adversial Machine Learning

CoE Center of Excellence

DLP Data Loss Prevention

DOI Diffusion of Innovation

EFTA European Free Trade Association

EU AI Act European Parliament Artificial Intelligence Act

GDPR General Data Protection Regulation

GenAI Generative AI

GPT Generative pre-trained transformer

HIPAA Health Insurance Portability and Accountability Act

ISMS Information Security Management System

KPIs Key Performance Indicators

LLMs Large Language Models

MAS Multi-Agent AI System

MFA Multifactor Authentication

NIS Network and Information Systems

NLP Natural Language Processing

OCM Organizational Change Management

PIM Privileged Identity Management

ROI Return of Investment

SFI Secure Future Initiative

SIEM Security Information and Event Management

TAM Technology Acceptance Model

TOE Technology-Organization-Environment

1 Introduction

Generative AI has become widely used tool across industries and organizations, as well as ordinary people. Microsoft offers various Copilot products and Microsoft 365 Copilot is LLM powered AI tool that can be utilized and integrated to organization, offering large scale of features for different use cases and working roles to harness its full potential. This thesis introduces structured implementation model for M365 Copilot deployment to organization with security first in mind. The model is to be handed over for commissioning organization for further development and real world customer project utilization. Implementation model is supported by adoption models and regulatory compliance. M365 Copilot Implementation model is validated with qualitative study and mixed data analysis through its potential in productization credibility and measures with security, user adoption, and regulatory requirements.

1.1 Commissioning Organization

This thesis is commissioned for Twoday, a leading Microsoft Cloud and AI partner in the Nordics. Twoday operates in five countries (Norway, Sweden, Finland, Denmark, and Lithuana), has more than 3000 professionals and over 800 customers. Twoday delivers a large variety of digital solutions like Data & AI, Software engineering, Digital experiences, Business applications and Cloud Platforms & Security. Organization's customers come from many different industries, such as government,

energy & utilities and health & life science. [1]

I work as a developer and consultant in Twoday Oy Finland. I mostly act as a Dynamics 365 developer in various customer projects. My daily work includes consulting customers, operating Microsoft Dynamics 365 Power Platform applications like Power apps, Power Automate, Power BI with the enhancement of M365 Copilot tools and agents. I also develop technical customized on demand solutions to customer D365 tenants with C# plug-ins and JavaScript.

1.2 Research Problem and Questions

The purpose of this thesis is to produce a product for resale for commissioning organization that combines the implementation of Microsoft 365 copilot in organization environment with cybersecurity considerations, targeted especially for organizational customers. The business unit I work for has a wide range of customer from various industries and of all sizes. Projects where implementing of M365 Copilot for organization is a part or the main goal is not utilized as a clear operating model as of now. Commissioning organization wishes to establish a straightforward framework for implementation that maintains a focus on cybersecurity and is utilizing Microsoft security related products, boosts sales operations, and reduces complexity of implementing process for M365 Copilot.

In this thesis the aim is to answer the following research questions:

RQ1: How can a secure Microsoft 365 Copilot implementation be effectively productized into a organizational service offering?

RQ2: How well does the proposed implementation model drive user adoption, while ensuring security and regulatory compliance?

1.3 Thesis Structure

Thesis consists of seven chapters in total. Chapter 2 comprehends literature review of main topics of the thesis to have necessary conceptual background for the later chapters. This chapter is divided into four sections: Overview of Artificial Intelligence, Enterprise Use, Legislation, and Microsoft's Artificial Intelligence and Security.

Chapter 3 includes the research methods utilized in this thesis. Thesis study involved a literature review, the development of the implementation model for M365 Copilot, and qualitative study with mixed data analysis to validate the implementation model. This chapter is divided into three sections: Literature review, Implementation Model, and Qualitative Research & Analysis.

Chapter 4 consists of the M365 Copilot implementation model created for commissioning organization in the context of this thesis. This chapter is divided to directly reflect on the implementation model phases: Strategy, Plan, Pilot, Rollout, and Monitor.

Chapter 5 gathers the results and limitations of the qualitative study. It describes the themes identified in the thematic data analysis in detail. Descriptive statistics support the thematic analysis with quantitive study results. Study limitations are also explained. This chapter is divided into two sections: Qualitative Study Results and Qualitative Study Limitations.

Chapter 6 aims to evaluate the implementation model based on the qualitative study findings and answer the research questions. It will reflect on the study results and validate the implementation model, what are the strengths and areas for improvement for future work. This chapter is divided into three sections: Evaluation of the Implementation Model, Future Work, and Thesis Limitations.

Chapter 7 gives comprehensive conclusion of this whole thesis and aims to summarize the key findings and results of the study.

2 Literature Review

This chapter introduces some main basic concepts that will help reader with overall understanding of the main topics in this thesis. Key concepts are Artificial Intelligence, AI in enterprise use & adoption models, and cybersecurity. Lastly Microsoft's Copilot products and other related products, topics, and details reflecting on AI, security, and compliance manners are introduced.

2.1 Overview of Artificial Intelligence

In this section concepts inside Artificial Intelligence (AI) field are explained with the necessary detail. Artificial Intelligence, Generative Artificial Intelligence (GenAI), AI agents, and Large Language Models (LLMs) are introduced and reviewed. This section helps the reader understand the context of the later sections in this thesis.

2.1.1 Artificial Intelligence

AI refers to a term that was introduced in the 1950's and started as a study of how machines could simulate human intelligence and various activities. Today, AI is used as a general term for the science of artificial intelligence. AI is used in computers to simulate human intelligence and train them to learn human-like behaviour (judgment, learning, and decision-making) and many other demanding tasks like speech recognition, translation, and Natural Language Processing (NLP). The term Artificial intelligence can be used to describe the broader concept that includes for

example generative AI and LLMs which will be discussed later in this section [2]. AI is also strongly connected to computer science, logic, biology, psychology, among many other disciplines. The rapid development of artificial intelligence in recent years has changed the course of, for example people's lifestyles, research, finance, marketing, and education.[3]

The concept of AI that is existing now is so called weak AI, that means it has very limited cognition and lack of human consciousness even though it can simulate them very well in some situations. The next hypothetical step for AI is to become so called strong AI, that could be capable of real human consciousness and other human tasks like reasoning and learning from experience. [4]

While the usage of AI is becoming part of daily lives of private individuals and organizations and it is capable of enormous scale of tasks, the security part should also be taken into consideration from the beginning and especially data protection is vital through the whole AI system [5]. The are many cybersecurity attack types aimed for traditional AI and one primary risk is the manipulation of the models input data to deceive the models decisions (Adversial Machine Learning (AML)). AML includes attack types like evasion & poisoning attacks, and model inversion & extraction. The main objective of these attacks are mainly targeted at the training data to alter or steal data. [6]

The usage of AI in cybersecurity threat detection has also become a great assistant for cybersecurity professionals, even though there is still some lacking in detection accuracy and interpretability. The tools used can not often explain why some events are flagged in operations. [7]

2.1.2 Generative AI

GenAI is subtype in Artificial Intelligence that was created in the late 2010's and has become more commonly used in the recent years [8]. GenAI more precisely, is

a term for computational techniques that are capable of generating many sorts of information and original content from training data. It can for example create text, images, videos, and audio. There are wide spread of use cases for GenAI, and it's not just for simple artistic purposes, but for assisting humans in all kinds of tasks from question-answering to complex decision-making and problem-solving [9]. GenAI can learn any complex subject like programming languages, human languages, chemistry, arts etc. GenAI's are trained with machine learning models like LLMs to get more advanced in the tasks they already master [8].

While GenAI's are already highly advanced in many complex tasks and has high efficiency, predictive analytics, and data augmentation, the algorithms GenAI uses might still be vulnerable and at risk of manipulation and attacks [10]. Cybersecurity attacks aimed at GenAI have become increasingly more common. There are for example Deepfake and identity thefts, polymorphic malware, and phishing attacks. Deepfake is a technology that is powered by GenAI and it is capable of creating realistic synthetic media, like altering facial attributes, swap faces, and produce specific person's voice. [11]

GenAI's also pose ethical risks. There have been rising issues with users' "overuse" of GenAI, which can lead to using it to every minor issue and danger of using the responses as absolute truth. These models might produce false information (hallucination) and user's should be aware of the limitations. [12]

2.1.3 Large Language Models

Large Language Models are big part of NLP models that are used to process various tasks like generating text, video, translations, question answering, text summarization and more [13] [14]. LLM powered AI engines have multi-purpose use in the field of many applications like education, business, social, and healthcare [15].

The development journey of LLMs have progressed from the 1990's and one of the

most significant achievement with LLMs have emerged just in the recent years, when generative pre-trained transformer (GPT) models have faced rapid speed in their development cycles. GPT models are extremely precise in advanced tasks. Known and popular open source GPT models are for example GPT, PaLM, LLaMA, and Gemini. [13] [16]

Certainly one of the most famous GPT models at the moment are provided by OpenAI and the company's GPT family. OpenAI published ChatGPT to the public in 2022 and has developed the model even further ever since [17]. GPT-5.5 was introduced as the newest AI system from OpenAI in April of 2026 [18].

LLMs face many kinds of risks in the form of cybersecurity attacks. There are for example data poisoning and prompt injection. Data poisoning refers to situations where bad actors manipulate LLM training data that could lead to misinformation and cause supply chain disruptions [19]. Prompt injections are one of the greatest risks of LLM applications and they occur when user input is directly and unintentionally altering the models behaviour (direct prompt injection) or LLM reads input from external sources and that content alters the models behaviour without the user knowing about it (indirect prompt injection). [20].

2.1.4 AI Agents

AI Agents are type of software systems that use artificial intelligence to perform tasks autonomously and proactively. AI Agents can process for example text, voice, video, audio, and code. Agents can perform these tasks simultaneously while doing reasoning, learning and decision making [21]. Agents use LLM's and generative models for advanced structured memory, learning and coordination. [22].

AI Agents have usually somewhat different use cases than with traditional GenAI. AI Agents' goal is to be autonomous creators for multiple purposes whereas GenAI mainly exists to simply create what user input that demands to be answered or

solved. [9] [22]

These AI agents can also work together as multi-agent AI system (MAS), where individual AI agents work in collaboration with each other to achieve more complex objectives and perform continuous learning [23]. The possibilities with MAS could be almost unlimited in the near future, they have already been used with for example complex analyses, marketing, and questionnaires [24]. In practice MAS can be used for example, healthcare patient care coordination, financial services with loan applications, in supply chain logistics with shipping operations, and retail with monitoring store inventory and staffing schedules [25].

AI agents are capable of autonomous tasks like planning and executing API calls. AI agents are at risk of being targeted by multiple types of cyber attacks, for example excessive agency, and chained vulnerabilities & cross-agent escalation [26]. Excessive agency simply put means granting an agent more permissions than is necessary. For example agent has access to systems that are not needed in the intended operation of the agent or agent is let to verify high-impact activities where failed approval can lead to losing crucial data [26]. Chained vulnerabilities & cross-agent escalation refers to the possible situations where in multi-agent systems a flaw or critical issue could cascade to other related agents if for example some low-privileged agent is compromised and then used to affect a high-privileged agent into doing some actual harmful actions like releasing sensitive data. [27]

2.2 Enterprise Use

This section discusses the use of AI in enterprise environments and what factors are affecting positively or negatively to adoption progression of new systems or tools in general. Adoption models Technology Acceptance Model (TAM), Diffusion of Innovation (DOI), and Technology-Organization-Environment (TOE) are introduced. They are frameworks for organizations to utilize when attempting to adopt new

tools (AI) into organization. Roadmaps from the point of view of AI are presented in general and how organization should utilize them in AI adoption.

The use of AI and LLMs have increased in the past years and many enterprises have started to take advantage of these new kind of "assistants" in various work sectors like healthcare, finance, education, and software engineering. LLMs have the possibility to enhance efficiency, innovation and decision making. Enterprises have many options what kind of LLMs to use and rather than using general-purpose models, fine-tuned smaller models can be made more efficient with domain-specific data. Enterprises are in the moving phase from simple chat based LLMs to more process targeted automations (like ERP) [28]. [29]

The usage of AI can also come with downsides as there are many risks and limitations to consider before adapting too fast or carelessly into using LLMs in enterprise environments. Data privacy and security must always be ensured and uploading company data to certain public models propose a risk of leakage. Ethical concerns might also arise, while models can grow into being biased because of their possibly corrupted training data. LLMs are not always reliable and can hallucinate some information. Using and training models can be expensive and the usage also consumes energy. [29]

2.2.1 Adoption Models

Technology Acceptance Model (TAM)

TAM is a theoretical framework created by Fred Davis in 1986 [30]. Framework was developed for understanding how new system and it's characteristics influence user acceptance, especially in computer-based information systems. The model includes two core components: perceived usefulness and perceived ease of use. Perceived usefulness defines the degree that individual user believes the new system will enhance their job performance. Perceived ease of use defines the degree that individual

user believes the new system will be easy enough to use, without too much physical and mental effort. According to Davis' model, technology acceptance consist of three-staged process, where system's design trigger users' perceived ease of use and perceived usefulness. These cognitive responses form response of attitude toward using the technology that has influence in the use behaviour. Lastly the level of actual use of the technology can be predicted by the expected level of easiness to use of the technology. The more easy to use the system is, the more likely it will stimulate acceptance of the system for end users. [30]

Study published by Estocapio et al. in 2025 [12] used TAM as a theoretical lens to investigate pre-service teachers (PSTs) perceptions of GenAI and its benefits and ethical risks in lesson planning. Study results are indicating that PSTs are perceiving GenAI positively and it also benefits in saving time, quality, and personalized learning. PSTs also show critical awareness of GenAI related risks, like bias, misinformation, and automated overreliance on the AI system. These two perspectives indicate that PSTs are becoming more mature digital users and are receptive to GenAI innovations while maintaining critical and ethical thinking. [12]

Diffusion of Innovations (DOI)

DOI theory was developed by Everett Rogers in 2003 [31]. Theory provides a theoretical framework for understanding how, why and at what rate new technologies spread in social systems. Theory concludes five main attributes: relative advantage, compatibility, complexity, trialability, and observability. Relative advantage is defined as *"the degree to which an innovation is perceived as being better than the idea it supersedes"*. Compatibility is defined as *"the degree to which an innovation is perceived as consistent with the existing values, past experience, and needs of potential adopters"*. Complexity is *"the degree to which an innovation is perceived as relatively difficult to understand and use"*. Trialability is defined as *"the degree to which*

an innovation may be experimented on a limited basis". Lastly observability is *"the degree to which the results of an innovation are visible to others"*. These attributes determine how individuals adopt new innovations. Four of the five attributes are positively related to adoption rate and one attribute has negative relation to adoption rates. Relative advantage, compatibility, trialability, and observability of an innovation are positive factors. Complexity is a negative factor of an innovation. Rogers' theory represents a five phase process in which user is proceeding from the first knowledge of innovation through persuasion, decision, implementation to lastly confirmation. [31]

Research article by Albishri et al. [32] investigates GenAI adoption and organizational use in Saudi business executives using DOI theory framework. Quantitative study collected data from 342 executives from different industries. Study results indicate that GenAI's relative advantages (faster outcomes and workflow compatibility) are increasing executives' trialability, observable benefits and social influence to promote wider adoption. While complexity lowers trialability, compatibility mitigates the lowered trialability effect. Result analysis shows that trialability has crucial linking to relative advantage and compatibility which directly impacts on continued usage. [32]

Technology-Organization-Environment (TOE)

TOE framework was created by Tornatzky and Fleischer in 1990 [33]. Framework is broken to three foundational parts to analyze in enterprise level the process of adopting, implementing, and perceiving technological innovations: technological context, organizational context, and environmental context. Technological context refines the internal and external technologies that are relevant to the enterprise, and it includes existing technologies being used and available technologies in the market. Organizational context is defined by enterprise's internal characteristics, resources, and key

factors. Key factors include firm size & scope, centralization, human resources, and communication processes (formal and informal) among employees. Environmental context is shaped by the area in which the enterprise is conducting its business. This means industry structure & market, competitors, and regulatory environment. These three context have direct affect on organizations' technological innovation decision making. Tornatzky and Fleicher suggest in their framework that organization should be consistent in their environmental surroundings and needs determined by internal and external factors. [33]

Study by Zhang et al. [34] examines GenAI applications in the fashion retail industry. Study proposes TOE based framework for fashion retailers to guide GenAI innovations in their field. Extensive literature review revealed challenges in data issues, technical constraints, output reliability, and social concerns towards GenAI in fashion retail business. On the other hand literature review proves that GenAI also elevates productivity across the fashion retail industry that results in enhanced design & operations, improved marketing & customer experiences, and more optimized decision-making. Authors' TOE based framework proposes practical guide to assist fashion retailers to navigate through these GenAI complexities and challenges to harness its potential. [34]

2.2.2 AI Roadmaps

Roadmap is a strategic plan created in high-level to represent goals and the steps to achieve some certain technology or topic for organization to follow. It helps organization to navigate through the details and ensures that every part of the organization follows the same path in development. Roadmaps can be altered based on the goal and objectives. [35]

AI has become such widely used tool and selling point amongst organizations and enterprises, that roadmap for AI development inside companies are becoming

essential parts of businesses. For AI roadmap development, there are couple of key stages to take into consideration. The stages and characteristics of the roadmaps may wary for different kinds and scales of organizations. Experiment & prepare, pilots & capabilities, AI ways of working, and readiness for AI future are higher-level topics that could be considered in the roadmap's planning phase. [36]

OpenAI published an article at the end of 2025 [37] that introduces the state of enterprise AI report, where data is collected from their enterprise customers. They declare that AI adoption in enterprises is reshaping how people work, team collaboration, and product building & delivery. Four key findings indicate that enterprises are scaling AI with deeper workflow integrations, productivity and business impact are leveraging, growth is global and rapid, and the gap between leading AI adopters and laggards are becoming more obvious. The report concludes that AI in enterprises is still in its early stages and awaits maturing, transforming AI capabilities into products, services, and new experiences which lead to great revenue growth. [37]

2.3 Legislation

In this section the most relevant regulations for the purpose of this thesis regarding AI usage in Europe are introduced: EU AI Act, and NIS2. Clarification is needed for reader to grasp what kind of legal and policy aspects are directed at AI in the region of European Union.

2.3.1 NIS2

European Parliament has established Network and Information Systems (NIS) directive, NIS2 (2022/2555) in 2022 [38]. The directive creates a unified and legal framework to maintain cybersecurity across the EU in 18 specified sectors. The

directive mandates that every member country needs to adopt a national cybersecurity strategy, that includes policies three key factors: supply chain security, vulnerability management, and cybersecurity education & awareness. The NIS2 directive is continuum to NIS1, which already covered healthcare, energy, transport, water management, digital infrastructures, digital providers, banking, and financial market infrastructure sectors. In NIS2, manufacturing, waste management, space, waste water, public admin, ICT service management, research, food production and distribution, postal and courier services, and manufacture production and distribution of chemicals sectors were added to the directive's scope. These 18 sectors are divided to highly critical and critical sectors, based on their characteristics. Energy, transport, banking, financial market infrastructures, health, drinking water, wastewater, digital infrastructure, ICT service management, public administrations, and space are classified as highly critical sectors. The rest of the sectors, including postal and courier services, waste management, manufacture, production and distribution of chemicals, manufacture, production and distribution of food products, manufacturing, digital providers, and research are classified as critical sectors. [39]

Article 23 [40] mandates the reporting obligations that essential and important entities are required to follow. Early warning (24h) notification is required when significant incident occurs. Incident notification (72h) is detailed update regarding the early warning notification and it must include initial assessment, severity, impact and initial indicators of compromise. Final report (1 month) is a comprehensive report of the incident and it should cored detailed description, root cause, mitigation measures, and cross-border effects. [40]

Bolgouras et al. [41] analyzed EU's regulatory ecosystem for ethical AI systems and it included the analysis of multiple regulatory requirements within the EU. The focus was primarily binding EU AI Act, GRPR, NIS2, CRA (Cyber Resilience Ac), and DMA (Digital Markets Act). Authors did not analyze these regulations individ-

ually since they argue that these regulations must be interpreted in parallel in order to maintain ethical AI deployments. NIS2 focuses on risk management, incident reporting and overall cybersecurity, forming so called cybersecurity pillar. On the other hand, NIS2 does not cover data governance or algorithmic transparency. [41]

2.3.2 EU AI Act

European Parliament Artificial Intelligence Act (EU AI Act) (2024/1689) [42] is a regulation that aims in responsible and safe usage of AI and AI systems to be transparent, non-discriminatory, traceable and environmentally friendly [43]. The proposal for this act was introduced back in 2021 and it's endorsement has started in 2024 when the European Council formally adopted the act. The act classifies AI by how high the risk level is [44]. The risk levels are: Unacceptable risk, high risk, limited risk, and minimal risk. Unacceptable risk level AI applications have been banned in the EU, such application could be for example biometric identification and categorization of people, behavioural manipulation of people or vulnerable groups, and facial recognition in public spaces [43]. High risk AI systems can be for example medical devices, cars, toys, law enforcement, education, and operation of critical infrastructure [43].

Article 26 [45] describes the obligations of deployers of high-risk AI systems. Article requires deployers to use systems as they are instructed to be used, assign human-in-the-loop operator, ensure that input data is relevant, and observe the system's operations. If deployers identify a risk, they must inform provider and relevant authorities. Logs generated by the AI system must be restored at least six for months. [45]

Study article by Beltrán [46] examines GDPR, DSA, CRA and EU AI Act as key regulations aimed at algorithmic security and privacy in the EU. For EU AI Act, the author collects the crucial requirements for high-risk AI systems established in

the regulation. The requirements forces high-risk AI systems to have risk management system, data governance, technical documentation, transparency & provision of information to users, human oversight, accuracy & robustness, and cybersecurity. [46]

Recent study published by Kim et al. [47] in 2025 shows that Europe is behind in the general and recent research trends in AI governance in the context of EU AI Act. The regulation constitutes rather small portion of overall AI research landscape and many existing research papers are focusing on ChatGPT alone, even though AI landscape is already rather extensive with other models like Gemini, Claude, Grok, and DeepSeek. The development of relevant policies are lagging behind concerning the fast pace of technology advancement surrounding AI in the EU AI act. Study findings suggest that there is significant gap between governance framework research and institutional mechanisms (fostering and supporting practical cooperation and communication) that include diverse stakeholders (technology, developers, policy-makers, users, and civil society). [47]

2.4 Microsoft's Artificial Intelligence and Security

This section focuses on Microsoft-related topics and products, particularly from the perspective of AI and security, alongside compliance and governance. Specific attention is given to Microsoft Copilot products. How Microsoft has managed to adopt it's marketplace approach in the world of AI. Microsoft's AI strategy consist of key idea about inside-out thinking, meaning that the company first build AI tools within their own businesses to test out their products reliability, safety, and operational efficiency. [48]

2.4.1 Copilot Products

Copilot is Microsoft's virtual assistant that is powered with AI. Copilot uses LLMs to solve task, answer questions with prompt and response interaction. There are various types of Microsoft's Copilots based on licensing and personal or organizations' needs. The Copilot family is extended to consumer and organization wide and Copilot's features depend on the type and purpose. This thesis focuses on especially Microsoft 365 Copilot (later referred as M365 Copilot), but other Copilot types Microsoft has to offer for companies are also introduced alongside AI Agents for M365 Copilot. Products from Copilot family that are introduced: Microsoft Copilot, Microsoft 365 Copilot Chat, Microsoft Security Copilot, GitHub Copilot, and Microsoft Copilot Studio. [49]

Microsoft Copilot is available free in the web for everyone, but it can also be used as a logged in user with M365 subscription. The features of Microsoft Copilot depend on whether the user is logged in and whether they have M365 subscription activated. With Microsoft Copilot users can for example draft an simple email, get faster answers from internet and create simple images. There is also mobile app version for Microsoft Copilot that can be also used for free or with M365 subscription [50]. [49]

Microsoft 365 Copilot Chat is an add-on AI prompt and response experience that is included with several Microsoft 365 subscriptions. It is enterprise baseline standard version and it has additional features comparing to the free consumer version, for example creating images with Copilot pages, handling IT controls, enterprise data protection, using Microsoft 365 apps (Word, Teams, Excel, PowerPoint, OneNote, and Outlook). This Copilot is not integrated with organizational data (for example emails, files, and chats) and only uses data from the web, but user can refer to single documents directly in a chat prompt. Copilot Chat can also access certain content that is currently open in user's desktop, like Word, Excel, and Outlook, that way

Copilot Chat has additional limited access to user's and organizational data. [51]

M365 Copilot has even more features than the previously mentioned. The usage is licensed by working organization and it can be used for example with Microsoft 365 apps (Teams, Outlook, Word, Excel, and PowerPoint), creating Copilot Agents, measuring insight with Copilot Analytics, and Microsoft Graph assisted work-based chat. What makes this Copilot assistant different from the other versions is that it has access to users' and their organization's data, such as email and files, via Microsoft Graph with organizational Microsoft Entra account. This feature allows M365 Copilot to find information from Outlook emails and SharePoint documents, create meeting agendas and get Teams meeting summary for instance. M365 Copilot is also available to use with mobile devices [52]. M365 Copilot and its architecture, use cases etc. will be discussed further in 2.4.2. [53]

Microsoft Security Copilot is mainly used by security professionals, licensed by their working organization. Security Copilot is generative AI-powered security assistant with incident response, threat hunting, posture management, intelligence gathering, and many other capabilities. Security Copilot provides immersive standalone experience and embedded experiences available in Microsoft security products (Microsoft Defender XDR, Microsoft Sentinel, Microsoft Entra, and Microsoft Intune). [54]

GitHub Copilot is AI-powered coding assistant for developers in working organizations. Within code files Github Copilot can give code suggestions, assist in research & planning, and create pull requests. Github Copilot is capable of operating in any platform or code repository [55]. Github Copilot is available to use in for example users IDE, Github Mobile, command line and website. [56]

Microsoft Copilot Studio is a low code graphical tool used to create agents and connections to various data sources. Agents are used to customize working organization's Copilot experience with automated business processes (help desk, managing

meetings, change management) [57]. Copilot Studio is often used when for example data is fetched outside Microsoft Graph, data needs to be integrated to external systems, complex decision logic is needed or use case demands specialized automation that is beyond general productivity [58]. Copilot Studio is licensed by working organization and consumes Copilot Credits. Copilot Studio can also be connected to M365 Copilot Subscription with the integrations already available within M365 Subscription services. [58]

AI Agents for M365 Copilot are not explicitly a product inside Copilot family, but extensions to M365 Copilot acting as a specialized AI assistants fitted for specific domains. Agents can apply organizational knowledge and automations in order to enhance decision making, improve efficiency, and streamline business processes. Microsoft offers two type of AI Agents to extend M365 Copilot: declarative agents and custom engine agents. Declarative agents use Copilot's AI infrastructure, orchestrator, and model. With declarative agents organization can gain additional knowledge and activate actions to automate business processes. Custom engine agents are fully customized and suitable for complex workflows, orchestration, or specific LLMs. They might require more pro-code understanding and implementing with Visual Studio or Visual Studio Code. [59]

M365 Copilot includes two pre-configured AI agents, Researcher agent and Analyst agent, that users can utilize in their work. Research agent can be used to deepen reasoning for user tasks, for example to do in-depth research from multiple resources and get clear citations [60]. Analyst agent acts as a skilled data-analyst and helps make sense of large data sets, thus is time saving and generated readable reports [61]. [59]

2.4.2 Microsoft 365 Copilot

As previously discussed in subsection 2.4.1 M365 Copilot has large set of use cases, features and methods to utilize them. In this subsection we will deepen the architecture, user prompts and responses for M365 Copilot, and studies aimed at M365 Copilot from different contexts.

When Microsoft 365 subscription purchase is made, a tenant is automatically created for organization. That tenant lies inside Microsoft 365 service boundary and that is how M365 Copilot can access organization's data. Microsoft 365 service boundary holds inside M365 Copilot, Microsoft Graph, user accessible data (OneDrive files, SharePoint data, Microsoft Teams data, and Exchange mailboxes), and LLM that is held within Azure OpenAI service that is not part of OpenAI publicly available services. Thus OpenAI does not have access to this data for training purposes. Inside Microsoft 365 service boundary all the data is encrypted in transits. [62] [63]

Microsoft Graph is a gateway tool to integrate to data and intelligence in Microsoft's Cloud services (Microsoft Entra and Microsoft 365). Microsoft Graph offers three main components in M365 platform to facilitate the access and flow of data: Microsoft Graph API, Microsoft 365 Copilot connectors and Microsoft Graph data connects. Microsoft Graph API offers a single endpoint that provides access to data and insights that are rich and people-focused. It is possible to develop custom apps that support M365 tenant with REST APIs or SDKs. Microsoft 365 Copilot connectors are used to deliver incoming data outside Microsoft Cloud services and connectors can be used for example in Google Drive and Jira. Microsoft Graph Data Connect is a set of tools that provide straightforward and secure delivery of Microsoft Graph data to Azure data stores. Inside Azure development tools, cached data can be utilized in building intelligent applications. [64]

Grounding process is crucial part of prompting activity, since it handles the

connection to contextual and relevant data sources. M365 Copilot uses three types of grounding: work grounding, web grounding, and local data grounding. Work grounding accesses information that is specific to user's organization, like emails and files. Web grounding fetches publicly available data from the web (Bing search). Local data grounding uses content user attaches to singular prompt. [65]

User prompting begins with a prompt that is given to M365 Copilot within any app it has access to (for example Word). That prompt is first preprocessed in the grounding process, data is fetched from Microsoft Graph API and the grounding type is used that is relevant in each case. After pre-processing, Copilot sends modified prompt to LLM that is being used in that prompting scenario (for example GPT-5.3). LLM handles the modified prompt and returns a response suitable for the user's context to Copilot. Lastly M365 Copilot goes to post-processing phase and accesses Microsoft Graph for compliance and Purview actions in order to maintain data governance and compliance. Then M365 Copilot returns a final response to user via the app they are using. [63] [66]

M365 Copilot is compliant with Microsoft's privacy, security, and compliance commitments including General Data Protection Regulation (GDPR), EU AI Act, EU Data Boundary, ISO/IEC 2700, ISO/IEC 42001, and HIPAA. Prompts, responses and data that is accessed through Microsoft Graph is not used to train LLMs. M365 Copilot is protected by multiple functions like blocking harmful content, detecting protected material, and blocking prompt injections. More about compliance requirements for M365 Copilot will be discussed in 2.4.3. [62]

M365 Copilot can only access the data that is authorized to the user using Copilot. Copilot utilizes Microsoft Graph to access data in user's unique context. Copilot also cannot access any data that user does not have permission to view. Copilot honors multifactor authentication (MFA) and conditional access policies. User can later examine their chat history through previous prompts and delete

them if desired. [63]

For organization to successfully implement M365 Copilot into organization, Microsoft has compiled "Copilot Success Kit" that frames the most important steps for organization to implement the tool. Microsoft partner organizations that are providing Microsoft products can also make use of this kit. In this mostly complete documentation is integrated many resources and advices from Microsoft solutions, tools, and product families, like Zero Trust, Responsible AI, Microsoft Graph, and many more that are relevant for M365 Copilot. [67]

Literature of M365 Copilot

A survey published by Bano et al. [68] in 2024 showed that M365 Copilot can improve efficiency, productivity, creativity, and save time. 300 licenses were distributed for Australia's National Science Agency (CSIRO) and users had six-month trial with the AI assistant. Quantitative surveys were conducted for the participants before and after the trial time period. Participants used M365 Copilot for routine tasks like drafting emails and summarizing meetings. More complex tasks like problem-solving, decision-making, and domain-specific knowledge functionalities had some gaps for the participants. Ethical concerns were arose after the trial, especially about data privacy. [68]

The same study for CSIRO was also conducted on qualitative focus by Bano et al. [69] where 27 users were interviewed about the six-month trial with M365 Copilot. One main finding of this survey was so called productivity paradox, where time was saved by automating some routine tasks but on the other hand more complex tasks required more extensive oversight to verify that M365 Copilot's outputs where correct. Authors conclude that while M365 Copilot brings great value in specific operational tasks, it has some usability limitations in deep contextual understanding and domain-specific knowledge. [69]

A thesis study [70] for Swedish construction industry was made in 2025 where quantitative survey and qualitative interviews were utilized to identify what administrative areas can be supported with M365 Copilot. Copilot was used primarily for document management, reporting, and communication. Study shows that the AI assistant increased productivity and quality of written work and additionally it was time saving. Some challenges were faced with legal uncertainty, data security concerns, organizational resistance, and lack of training. [70]

2.4.3 Security, Governance & Compliance

This subsection introduces the security, compliance, and governance offerings that are relevant in the topic of this thesis and adaptable to Microsoft's M365 Copilot. Microsoft declares that their mission is to enable AI that is trustworthy, secure, and safe. Microsoft commits to keep all data private with transparent policies and regulate confidence with compliance frameworks [71]. Microsoft provides sufficient security, privacy, and compliance services for every product individually. Products are distributed in product families like Azure, Microsoft 365, Microsoft Dynamics 365, and Power Platform. M365 Copilot is included in Microsoft 365 family. [72]

Microsoft has identified six principles to guide responsible AI usage: justice, reliability & safety, data protection & security, inclusivity, transparency, and responsibility. Justice aims in AI systems that treat all people fairly while distributing opportunities, resources and information. Reliability & safety aims in AI systems that operate reliably and securely, for AI system to perform well in changing situations and contexts. Data protection & security's goal is to protect data and secure AI systems, to design AI system that supports those metrics. Inclusivity's target is for AI systems be able to assist everyone regardless of their background and disabilities, to accommodate user personas with different abilities. Transparency aims in transparent and understandable AI systems, to ensure that users understand AI

system's features accordingly. Lastly responsibility states that us human should be responsible for AI systems and maintain oversight for control and accountability. [73]

Security

Microsoft Secure Future Initiative (SFI) is a multiyear security initiative launched in 2023. The approach aims in learning, and improving existing methods and practices to ensure security in products and services. Secure by design, secure by default, and secure operations are the three principle anchors that leads the initiative. The initiative also focuses on six key pillars that drive the improvements: protect identities and secrets, protect tenants and isolate systems, protect networks, protect engineering systems, monitor and detect cyberthreats, and accelerate response and remediation. With these measures security levels are improved and for example the risk of unauthorized access is reduced and all tenants and production environments are safeguarded. [74]

Microsoft follows Zero Trust strategy which implements three core security principles: verify explicitly, use least privilege access, and assume breach. It is not a singular product, but an architectural framework for all Microsoft customer and partner businesses to follow [75]. Verify explicitly refers to the demand of always authenticating and authorizing based on available data point. Least privilege user access means to limit user access to a level that is just enough for the context. Assuming breach helps in minimizing access points and segment access and to verify end-to-end encryption with the assistance of analytics, threat detection and improved defences. Zero Trust is meant to adapt in complex environments and extend throughout organizations [75]. Zero Trust is also extended to cover M365 Copilot and documentation explicitly demonstrates what actions organization must take in order to be compliant with Zero Trust core principles. The core principles are di-

vided inside seven layers of protection in M365 tenant: data protection, identity & access, app protection, device management & protection, threat protection, secure collaboration with Teams, and user permission to data. [76]

Microsoft Purview is a set of solutions, a tool that assist organization that unifies data security, data governance and data compliance into one product offering. Data security is a robust and coordinated security solution that dynamically secures data throughout its lifecycle. Data security solution includes Data Loss Prevention, Data Security Investigations, Information Barriers, Insider Risk Management, and Privileged Access Management. Data governance manages data services and assist in governing data and aims to unlock business innovations. Data governance solution includes Data Map and Unified Catalog. Data compliance helps organization minimize compliance risk and assists in regulatory requirements. Data compliance solution includes Audit, Communication Compliance, Compliance Manager, Data Lifecycle Management, eDiscovery, and Records Management. [77]

Microsoft Sentinel is cloud-native Security Information and Event Management (SIEM) solution that is scalable across multicloud and multiplatform environments, combining AI, automation, and threat intelligence in order to support threat detection, response, investigation, and proactive hunting. Sentinel offers data collection, threat detection, threat investigation, and threat response features. Data collection features include: out of the box data connectors, custom connectors, and data normalization. Threat detection features include: analytics, MITRE ATT&CK coverage, threat intelligence, watchlists, and workbooks. Threat investigation features include: incidents, hunts, and notebooks. Threat response features include: automation rules and playbooks. [78]

Microsoft Defender for Endpoint is a security platform designed to assist organizations to prevent, detect, investigate, and respond to advanced threats that are targeted at their endpoints. The term endpoints covers: laptops, PCs, phones,

tablets, access points, routers, and firewalls. Defender for Endpoint is a part of Microsoft Defender XDR solutions, and it can be integrated with for example previously presented Microsoft Sentinel. Microsoft Defender for Endpoint has six key capabilities: APIs, attack surface reduction, automated investigation and remediation, Endpoint attack notifications, Endpoint detection and response, Microsoft Secure Score for devices, and next-generation protection. [79]

Governance

Data privacy for Microsoft is anchored in the principle that customer always controls their own data. This is operationalized through four key pillars: control your data, where your data is located, securing your data, and defending your data. Customer has always full ownership of their data and Microsoft acts as a data processor for the chosen services. Data residency depends on the organization physical location, organizations in EU are applied with the EU Data Boundary. All data is protected with encryption at rest and in transit and customer has options on how to manage encryption keys. Data is defended through well-established response policies and processes. [80]

Microsoft's EU Data Boundary is a boundary where Microsoft has committed to certain storing and processing services for countries in the EU and European Free Trade Association (EFTA). EU Data Boundary is included in Microsoft enterprise online services (Azure, Dynamics 365, Power Platform, and Microsoft 365). Microsoft stores customer data (text, images, video, and software), professional services data (Microsoft's technical support and consulting related data), and system-generated logs (logs created during service operations). [81] [82]

Compliance

Microsoft's compliance approach helps organizations to navigate through complex and dynamic regulatory environment. Compliance has three core resources: compliance offerings, audit reports, and shared responsibility model. Compliance offerings depend on the country of the organization and possible specific regulations that country might have. Globally for example ISO/IEC 27001 and SOC 1-3 standards are supported for large variety of products. In EU, GDPR for example is a forced regulatory. Customers can access their audit reports and resources to control requirements, verify technical compliance and support their security professionals. Shared responsibility model emphasizes the fact that compliance is partnership between Microsoft and organization. Microsoft as a cloud provider manages the security of the cloud, while customer organizations is responsible for the security in the cloud [83]. Microsoft Purview's Data compliance introduced in Security 2.4.3 governs and manages critical risks and regulatory requirements. Microsoft Purview Compliance Manager tool additionally offers guidance regarding regulatory compliance for various sectors across the globe [84]. In the EU NIS2 and EU AI Act directives are enforced and supported [85]. [86]

As mentioned in 2.4.2 M365 Copilot respects wide range of regulatory requirements targeted at this AI system, these include GDPR, ISO/IEC 27001, ISO/IEC 42001, and Health Insurance Portability and Accountability Act (HIPAA) [62]. ISO/IEC 27001:2013 [87] is standard for Information Security Management Systems (ISMS) and it acts as a formal specification, mandating implementing, monitoring, maintaining and improving the ISMS. Additionally it delivers best practices of documentation, divisions of responsibility, availability, access control, security, auditing, and corrective & preventative measures. ISO/IEC 42001:2023 [88] is also standard for management systems, but specifically aimed at Artificial Intelligence Management Systems (AIMS). The standard aims in providing guidance in the rapidly

changing AI era that we are living at the moment. It also addresses unique challenges AI might pose, ethical considerations, transparency and continuous learning. It collects structured way to manage AI related risks and opportunities for organizations. GDPR [89] is regulation aimed in protecting and processing personal data in the EU. This gives individuals the right to manage their personal data that is collected by organization. HIPAA are set of healthcare laws taking place in the U.S. HIPAA aims to cover entities that create, maintain, transmit, or access patients protected health information. Since HIPAA is not mandated in the EU, and does not affect the scope of this thesis, this act won't be discussed further. [62]

3 Research Methods

The purpose of this chapter is to explain the research methods conducted in this thesis. Thesis includes literature review of relevant topics, creation of implementation model for M365 Copilot, qualitative study and mixed data analysis. The study aims to validate the proposed implementation model for M365 Copilot.

This study was conducted in aiming to answer the following research questions:

RQ1: How can a secure Microsoft 365 Copilot implementation be effectively productized into a organizational service offering?

RQ2: How well does the proposed implementation model drive user adoption, while ensuring security and regulatory compliance?

3.1 Literature Review

A literature review of Artificial Intelligence, AI usage in enterprises, legislation related to AI and cybersecurity and Microsoft's AI tools and security measures was conducted in this thesis to identify the necessary information and details to compile M365 Copilot implementation model.

Search queries were targeted across various databases to gain relevant peer reviewed articles and conference papers. Databases included the following: Google Scholar, ScienceDirect, ACM Digital Library and IEEE Xplore. Google Scholar is a search engine, unlike the other databases so some searches may have resulted in duplicate results. Queries were done in many ways, depending on the topic that was

under review.

To gain even deeper search for related articles, AI tools (M365 Copilot and Gemini) were assigned to search relevant peer reviewed articles as some topics was particularly difficult to find suitable sources, for example M365 Copilot adoption and implementation in organizational settings. More detailed explanation of AI usage in this thesis can be found from Appendix B.

Microsoft related resources were mainly utilized from Microsoft's Learn domain [90], other documentation and articles maintained by Microsoft as M365 Copilot and other relevant information is very domain specific to Microsoft products.

3.2 Implementation Model

Literature review that was conducted in the beginning of this research, revealed that there are little to no publicly available peer reviewed academic writings about implementation of M365 Copilot in organizational settings. Multiple academic literature handles analysis and studies regarding adoption models (TAM, TOE, DOI) that are conducted mostly separately from each other. Academic literature handling GenAI applications with regulatory environment like EU AI Act and NIS2 was not identified. This thesis aims to combine these factors together.

The implementation model aims to base M365 Copilot implementation on Microsoft resources and enhance them by using additional Microsoft security related products, Copilot Success Kit, collecting key points from all three adoption models (TAM, TOE, DOI), and regulatory requirements that are affected towards AI usage and cybersecurity (NIS2 & EU AI Act).

3.3 Qualitative Research & Analysis

To validate the M365 Copilot implementation model, a qualitative study with questionnaire and mixed data analysis of the results were conducted in this thesis. Qualitative study was chosen, because suitable customer project or any similar possibility to demonstrate the created implementation model in real-life scenario was not identified in the given timeline. Qualitative questionnaire was identified as the best option in this case for validation. Qualitative interviews were not chosen, because of the strict time limit. Quantitative study and questionnaire was not chosen, because it would have required significantly more people to give responses to reliably validate the implementation model. Content analysis was not chosen because it relies heavily on counting the presence of certain words, phrases or themes/categories and not diving to thematic meanings at the same level of depth as thematic analysis does.

Mixed data analysis methods included thematic data analysis of open-ended questions and descriptive statistics of Likert scale questions to validate the whole survey data properly. Descriptive statistics for Likert scale questions were chosen to summarize certain patterns across roles, explain what measured, and support the overall qualitative themes. Descriptive level was identified as necessary level of statistics, as it aims to identify general trends of related topics related to associated roles, rather than to proof statistical significance.

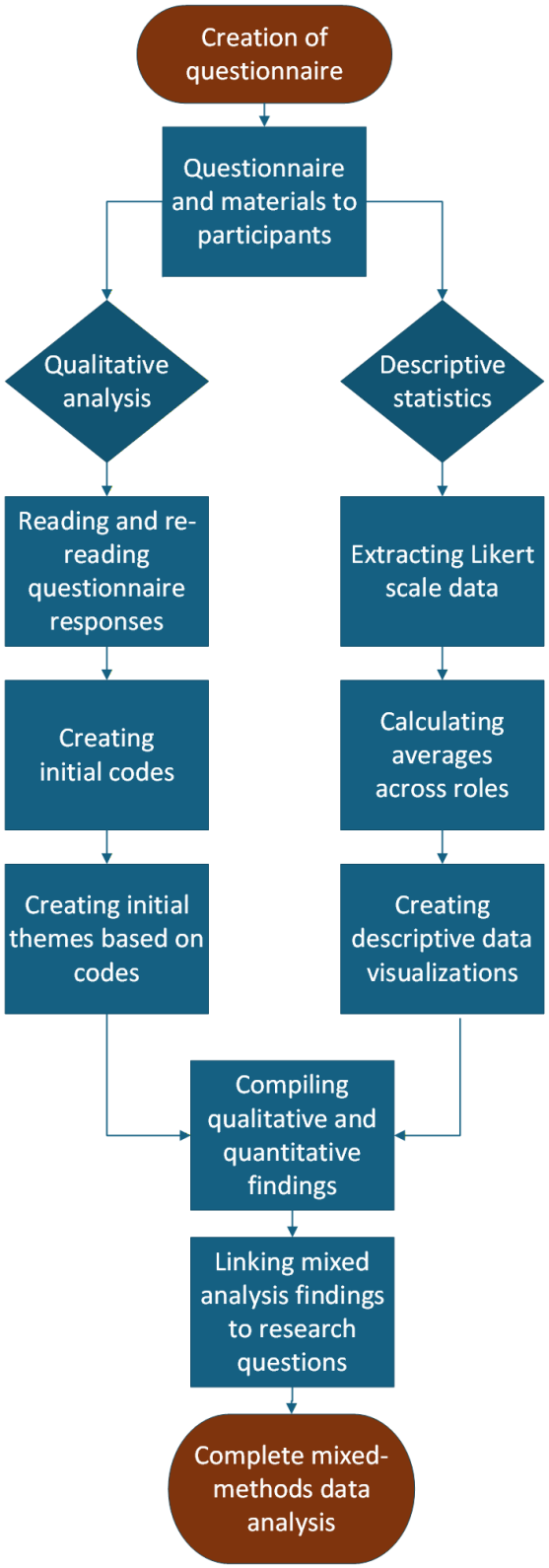

Figure 3.1: Validation process flowchart

Figure 3.1 clarifies the validation process that was processed during the study. First questionnaire was created to reflect the contents of the implementation model and research questions. Questionnaire and materials were sent to colleagues and responses were handled from the perspective of qualitative analysis and descriptive statistics. Qualitative analysis side consists of every step that was done for the open-ended questions responses towards creating themes. Descriptive statistics side consists of every step that was taken for the Liker scale questions responses to calculate average values of each role identified from responses. Both analysis materials where compiled and linked to research questions in order to complete the mixed data analysis.

Questionnaire

Questionnaire alongside the M365 Copilot implementation model materials were sent to 25 colleagues from three business units of Twoday. Colleagues with various roles, expertise and backgrounds were identified internally with the assistance of commissioning organization. In those 25 colleagues where workers with more advanced AI and M365 Copilot experience and colleagues with less experience with AI tools or Microsoft's security measures in order to obtain as wide a range of responses as possible. The questionnaire and implementation model resources were sent to respondents via Teams chat. Questionnaire was made with Microsoft Forms and all questions were in English. Introduction text was in Finnish and in English. The questionnaire responses were collected anonymously and the respondents had 14 days to complete the questionnaire before data analysis had to be started due to limited time window. In the end 19 colleagues responded to the questionnaire.

Questionnaire was compiled based on the main topics of M365 Copilot implementation model, questionnaire questions are available in Appendix A. Questionnaire consisted of 24 questions in total. 17 of the questions were open questions. 23 of the

24 questions were mandatory to answer. Seven of the questions were Likert scale questions with scale 1-4 to be chosen. Scale from 1 to 4 was chosen to avoid responses in the middle ground. Every one of the Likert scale questions were mandatory to answer. Likert scale questions were added to questionnaire to keep the length and complexity of questionnaire as low as possible and reduce cognitive load of completing the questionnaire. Questionnaire was divided into six themes to reflect on the implementation model: basic information, measuring user expectations and user behaviour, measuring organizational fit, structural readiness, security, compliance, and regulatory requirements, and model validation.

Basic information section consisted of five questions (Q1-Q5). The main purpose of this section was to gather basic information from the respondent that can be reflected to the rest of the questionnaire. This section reveals the respondent's background, role description, experience with M365 Copilot, familiarity with Zero Trust measures, comfortability to adopt new tools, and repetitive tasks where M365 Copilot could help or already does.

Measuring user expectations and user behaviour section consisted of two questions (Q6-Q7). The main purpose of this section was to reflect on TAM framework that explicitly measures perceived usefulness and perceived ease of use of the target system, M365 Copilot in this case.

Measuring organizational fit consisted of six questions (Q8-Q13). The main purpose of this section was to reflect on DOI framework that identifies five attributes to measure diffusion of innovation: compatibility, observability, relative advantage, complexity and trialability. Questions related to each attribute was identified correlating the implementation model and M365 Copilot. Question directed at complexity was divided into two parts to gather more insight from the respondents (Q11 & Q12).

Structural readiness section consisted of three questions (Q14-Q16). The main

purpose of this section was to reflect on TOE framework that is divided into three foundational parts: technology, organization, and environment. Questions related to each part was identified correlating the implementation model.

Security, compliance and regulatory requirements part consisted of five questions (Q17-Q21). The main purpose of this section was to reflect to some security measures for implementing M365 Copilot and compliance of EU AI Act and NIS2 directives in this implementation model for maintaining regulatory requirements.

Model validation section consisted of three questions (Q22-Q24). The main purpose of this section was to identify opinions, views, and validation for the commercial viability of the implementation model. Respondents had to reflect on real or fictional customer case and if there was some improvement ideas or critically missing parts in the implementation model based on their knowledge and expertise.

Mixed Data analysis

Mixed data analysis consisted of thematic data analysis of open-ended questions and descriptive statistics of Likert scale questions. Data analysis methods had to be converted to this type of mixed data analysis, because of two types of questions were utilized in the questionnaire.

Thematic data analysis part was done according to Ahmed et al. [91]. Thematic analysis was aimed at the open-ended questions which were question numbers 5, 6, 9, 10, 12-20, and 22-24. Analysis started with reading and re-reading questionnaire responses and getting familiar with the survey data. After initial reading, responses were divided into descriptive codes manually in Excel sheets. These codes were meant to identify meaningful features, patterns, and summarize data segments from the responses. 281 descriptive codes were identified in total from the open-ended question responses. Codes where compiled from responses that had same message, this way codes bundled the massive response data into smaller parts. After initial

coding, questions were divided based on the research question they have focused angle on. Questions 14, 15, 22, 23, and 24 were targeted at RQ1 which aims to answer how M365 Copilot can be productized. Questions 6-13, and 16-21 were targeted at RQ2 which aims to validate the implementation model created within the scope of this thesis from various perspectives. After this, codes were converted to themes by thematic mapping within Microsoft Visio app that assisted in visualizing the process of creating themes based on the codes.

Descriptive statistics of Likert scale questions were utilized for seven questions (Q2-4, Q7, Q8, Q11, Q21) to comprehend the quantitative aspect of the study with numeric analysis. Responses were grouped by working role (Architect, Consultant, Developer, and Strategic leadership) and average values of Likert scale questions were calculated in the accordance of role group in Pivot table in Excel.

4 M365 Copilot Implementation Model

The implementation model for Microsoft 365 Copilot with cybersecurity considerations is divided into five phases: Strategy, Plan, Pilot, Rollout, and Monitor. Each of the steps include high-level detailed instructions on how to deliver the implementation of M365 Copilot in organization with cybersecurity manners. The implementation model is created based on Microsoft Copilot Success Kit [67] enhanced with Microsoft products that support the Zero Trust framework, TAM model [30], TOE framework [33], and DOI theory [31]. It also guides at glance EU's NIS2 [38] directive and EU AI Acts [42] compliance and regulatory demands.

Microsoft's Copilot Success Kit gives great basics on how to deliver the implementation of M365 Copilot into organization, but gives rather broad and large scale guidelines. In this model it is attempted to make it more precise and add specific tools outside the Copilot Success Kit, like Microsoft Purview and Microsoft Sentinel, that are still very essential options to comply with Zero Trust framework.

TAM, TOE, and DOI were chosen as the adoption model baseline because individually they lack critical parts of adoption process context. TAM gives good angle to individual user acceptance and psychological beliefs, but lacks organizational context. DOI does not consider environmental and regulatory requirements, but explains characteristics of the technology and explains the rate of spread. TOE gives

excellent arguments about technology, organization, and environmental aspects but lacks individual user experience. This model aims to combine TAM, DOI, and TOE to fulfill in much deeper sense individual users' psychology, organizational context, environmental, and regulatory operations and requirements.

NIS2 directive and EU AI Act were added into this model to give more depth and enhancement of regulatory compliance in the era of AI where private individuals and organizations live at the moment. Copilot Success Kit does not directly address these regulations at all.

The implementation model described in this thesis is not an exact replica of that document that was handed to commissioning organization in order to maintain academic style and protect the organizational confidentiality, specific details and instructions have been omitted or generalized. Commissioning organization version also included preface chapter that introduced reader with TAM, TOE, DOI frameworks and NIS2 directive and EU AI Act to get better grasp of the whole document.

4.1 Strategy

In the beginning of implementation process, it is important to evaluate and ensure that customer's tenant is prepared technically, financially, and legally. In Strategy phase M365 Copilot is introduced, business values defined, Copilot implementation readiness checklist is reviewed and implementation roadmap is comprehended for customer case.

Microsoft 365 Copilot Overview

Overview is meant to introduce customers to M365 Copilot's capabilities and brief technical details in order for them to understand better what M365 Copilot offers and how it connects people, content, and tasks with organizational data and Microsoft Graph. Microsoft documentation materials [92] [93] give sufficient support to present

the product for customer.

Business

Business part will cover customer organization's values, needs, goals, and budget regarding the implementation process and project of M365 Copilot [67]. Key Performance Indicators (KPIs) [94] and success measurement plans are important to track the implementation process, Return of Investment (ROI), perceived ease of use and perceived usefulness [30]. KPIs are like organizations scorecard, a meter to measure whether the implementation process is delivering the right objectives [94]. A project framework and roadmap will be created in accordance of customer specific values, needs, goals, and budget.

Copilot Implementation Readiness Checklist

Copilot Implementation Readiness Checklist will assist in evaluating customer organization's M365 tenant and whether they meet the technical prerequisites to support the engine for M365 Copilot. This part consists of five steps: Microsoft 365 Copilot optimization assessment, licensing, organizational data audit, Zero Trust assessment, and organizational governance and adoption plan.

Microsoft 365 Copilot optimization assessment [67] helps organization to understand current tenant license profile, collaboration tools, sensitive data handling, and security controls. Assessment aids in identifying clear path to implementing M365 Copilot.

Customer organization's licenses must be clearly evaluated in order to every necessary user to access Copilot's features. Users must be assigned the prerequisite licenses for M365 Copilot usage. Additionally every user must have Microsoft Entra account for authentication. [95]

Organizational data audit is a crucial step in this phase, the purpose is to review

organization's SharePoint sites and OneDrive files and identify and delete outdated, irrelevant, and duplicate sites and files before Copilot indexes them [96]. For SharePoint sites, Restricted Content Discovery is recommended to be enabled to maintain data governance. Restricted Content Discovery lets organization limit specific SharePoint sites of being surfaced in organization-wide search and M365 Copilot, unless user has had a recent interaction [97]. [67]

Zero Trust assessment [98] is meant to evaluate customer tenants readiness for Microsoft's Zero Trust strategy and execution. Identity, access, and security are the key topics in this step. First Zero Trust Assessment is run in customer tenant. Assessment will reveal any missing best practices and vulnerabilities in customer tenant. After Zero Trust assessment review, all user identities in tenant are enforced MFA authentication. Tools like Microsoft Purview [77], Microsoft Defender for Endpoint [93], and Privileged Identity Management (PIM) [99] are highly encouraged. These tools assist in data security, data governance, and data compliance, ensuring that all devices meet security baseline, reducing risk of compromised credentials.

Last step in M365 Copilot implementation readiness checklist is organizational governance and adoption plan. The main purpose is to define clear AI usage policies for customer organization. According to EU AI Act article 14 AI-generated content should always have human oversight [42]. For adoption plan to be even more successful, early adopters should be identified and selected to be the first users of M365 Copilot, this should include workers with various roles, like business leaders and technically skilled personnel [31]. Leadership and management department should be aligned with specific KPIs and expected business value outcomes [94].

Copilot Implementation Roadmap

To successfully see the implementation project to completion, a roadmap for project execution must be built. Metrics like customer needs, wished, size, and type must

be taken into consideration while building a roadmap [36]. Theoretical example implementation roadmap was consisted in the implementation plan materials based on existing customer case identified internally can be seen high-level in 4.1. The example roadmap divides timeline based on the phases (Strategy-»Plan-»Pilot-»Rollout-»Monitor) and summarizes what steps are included in every section of the roadmap. The total duration and actions of the project and the duration of its various phases depend largely on the customer organization, data in their tenant, and budget. More detailed roadmap could be compiled for the team primarily responsible for executing the tasks during the implementation process. [67]

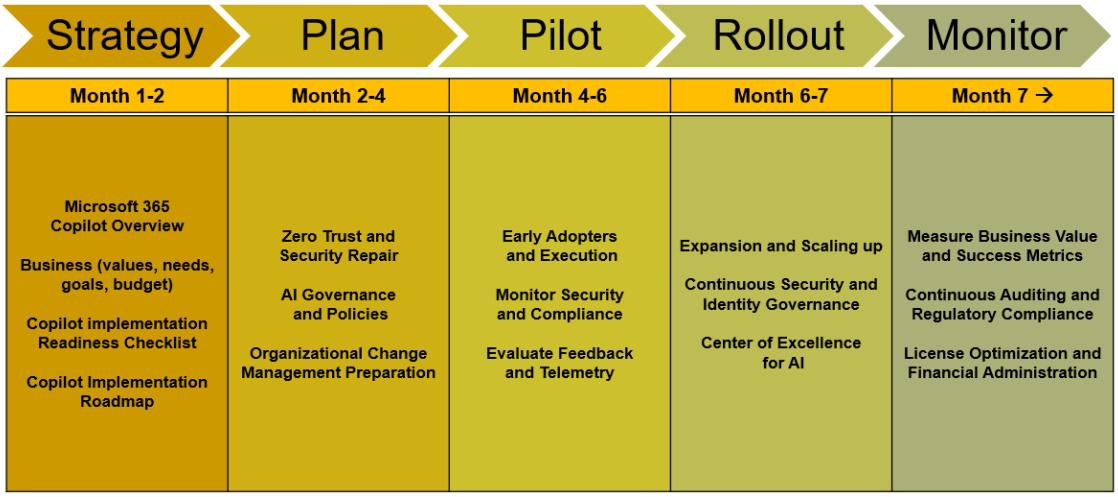

Figure 4.1: Theoretical roadmap for M365 Copilot implementation

4.2 Plan

The second phase of the implementation model shifts the focus from high-level alignment to hand-on technicalities and Organizational Change Management (OCM) measures. In Plan phase Zero Trust & Security Repair is utilized, AI governance and policies are formed, and OCM preparations are launched in organization.

Zero Trust and Security Repair

To address the possible gaps identified in Strategy phase to comply with Zero Trust framework and secure customer tenant, SharePoint Advanced Management (SAM) [96], Microsoft Purview's sensitivity labels [100] and Data Loss Prevention (DLP) alerts [101] tools should be configured. Zero Trust documentation for M365 Copilot explicitly provides guidance in the seven layers of protection for M365 tenant, for example how to deploy and validate threat protection services [76]. It must also be noted that Zero Trust measures might affect on users' perceived usefulness by not cleaning organizational data thoroughly and letting the Copilot engine to surface irrelevant, outdated, or even unauthorized data [30].

AI Governance and Policies

To establish refined AI guidelines and policies for organization, a cross-functional "AI Council" should be comprised. AI Council should include senior IT staff, human resources, and security personnel to observe the deployment of AI tools and manage AI-related risks. This is supported by Tornatzky's and Fleischer's TOE framework. [33] Organization should also publish corporate policy to mandate human oversight (human-in-the-loop) of all AI generated content [42]. If organization wishes to utilize AI agents, they should also be administered and governed properly [102].

Organizational Change Management Preparation

Successful implementation and adoption plan identifies where AI assistant delivers maximum business impact and organization should gather list of high-impact business scenarios, for example how sales department can utilize M365 Copilot in Teams or financial analysts how to do reporting with M365 Copilot. Mapping M365 Copilot capabilities directly to workers daily routines, the need for perceived usefulness it meets [30] and shapes organization's internal operation models [33].

In this step the planning of user training is crucial. Case-driven approach for training will probably lead to more comprehensive understanding, than generic technology based reading material and tutorials [30]. Kick-off webinars and workshops can drive learning curve, maximize adoption and minimize cognitive burden in end users [31].

Competence gap in prompting with M365 Copilot can lead to anxiety and difficulty to produce well written prompts in order to end with wanted results from M365 Copilot. User training should especially cover how to write proper prompts [103]. Microsoft also offers customizable Prompt Coach Agents to assist in prompt training [104].

Lastly in this step, a communication plan dedicated for organization should be designed to highlight the relative advantage of M365 Copilot. These could mean for example hours saved, and reduced administrative burden. [31]

4.3 Pilot

The third phase launches a piloting of M365 Copilot in customer organization. Highly controlled and monitored pilot helps validating technical configurations and stress-test adoption strategy before moving on to organization-wide deployment. This phase includes early adopters execution, security and compliance monitoring, and collecting feedback and telemetry.

Early Adopters and Execution

Pilot phase begins with activating M365 Copilot licenses to small early adopters group that was identified in Strategy phase. Early adopters are assigned the high-impact business scenarios that were identified in Planning phase to actively validate the perceived usefulness of M365 Copilot [30]. Pilot group must also receive initial training and hands-on support to enhance the perceived ease of use [30]. Lastly in

this step some kind of community for M365 Copilot early adopters should be put together, for example in Teams or Viva Engage, or other communication channel organization is using. In these communities early adopters can share their experiences, concerns, ask questions and find training resources [67].

Monitor Security and Compliance

In this part earlier utilized security measures like Mircosoft Purview DLP alerts are monitored and responded accordingly. DLP alerts dashboard and DLP analytics assist in monitoring activities. Microsoft Sentinel can validate logging and anomaly detection to capture AI-related security events to maintain alignment with NIS2 and EU AI Act directives and their reporting and log storage period mandates [40][45].

Evaluate Feedback and Telemetry

After the initial start of Pilot phase, the pilot group's engagement level and feedback of M365 Copilot must be evaluated and analyzed. Microsoft offers usage reports and Viva Insights dashboard to access metrics [67]. Qualitative feedback can be recorded from pilot group via using Microsoft Viva Pulse or Microsoft Forms questionnaires to get a grasp of pilot groups perceived ease of use and perceived usefulness [30]. Then hard telemetry (engagement levels) and qualitative feedback (questionnaires) must be analyzed in combination. Workflows, prompt libraries, and training materials can be adjusted based on the data analysis findings. This part is crucial to catch anything lacking or problem areas from early adopters before moving to organization-wide scaling [67].

4.4 Rollout

Fourth phase, Rollout, begins when early adopters have successfully harnessed M365 Copilot in their daily workflows. In this phase, M365 Copilot is integrated systemati-

cally into the whole organization with expansion, continuous security and governance measures, and Center of Excellence (CoE) for AI.

Expansion and Scaling Up

Customer organization must be guided to avoid deploying the whole organization at once, unless they are very small company. Deployment can be divided by for example departments, geographic regions, teams, or defined user personas. Some of the early adopters might become so called "Copilot Champions" who can act as a localized experts and demonstrate M365 Copilot's relative advantage and influence on possible skeptical early majority through peer-to-peer observability demonstrations. [31] [67]

Organization should continuously gather feedback during scaling up period and continue to improve M365 Copilot related materials (training and communication) to match organization's methods of use and workflows based on user feedback [67].

Continuous Security and Identity Governance

Expansion of M365 Copilot users, Microsoft Purview DLP alert count might increase. Security personnel must continuously monitor and fine-tune policies to reduce alerts and block unauthorized data transfers [38]. If customer integrations to external connections are to be developed with M365 Copilot, all third-party components must be risk-assessed and block unreviewed ones [38]. [67]

Center of Excellence for AI

Customer organization is guided to establish CoE for AI from the AI Council that was gathered in Strategy phase. This body will continue to manage the changing cultural customs, maintains repository of best practices, and reviews new use cases for M365 copilot and other AI tools. Organization must define the responsibilities of this CoE body, for example AI strategy, developing AI skills, pilot AI projects,

define & enforce AI standards, and manage AI services.[67] [105]

4.5 Monitor

Fifth and final phase of this implementation model, Monitor, represents the ongoing and so called operational state of the M365 Copilot deployment. Organization relies on telemetry data to optimize costs and ensure compliance and regulatory requirements.

Measure Business Value and Success Metrics

After company-wide scaling up is complete, continuous feedback and telemetry should be monitored to identify active M365 Copilot users and those who lag behind and the reason for possible low utilization rate [30] [31]. Success metrics (KPIs) should be evaluated to calculate the real business value. If organization is especially data driven, they could be recommended to use Copilot Analytics in Power Bi reports to get detailed data, for example business impact and adoption reports. [67]

Continuous Auditing and Regulatory Compliance

Customer M365 tenant should also be monitored for privacy incidents, oversharing events and DLP alert triggers. The CoE for AI body should continuously review and approve possible Copilot extensions or third-party components [38]. [67]

Organization should also evaluate compliance posture with NIS2 and EU AI Act directives with the assistance of Microsoft Purview Compliance Manager for example. Compliance Manager is a compact solution to assess and manage compliance across organization and will be useful to other cases than M365 Copilot and NIS2 and EU AI Act compliance. [84]

License Optimization and Financial Administration

Last step of the implementation model is to analyze M365 Copilot usage reports to identify users who do not use this tool, and should be revoked the M365 Copilot license. This action is important to prevent financial waste and maximize the ROI for M365 Copilot [33]. [67]

5 Validation

In this chapter the implementation model for M365 Copilot created in the scope of this thesis is validated with qualitative study findings. Qualitative study consisted of qualitative questionnaire targeted at commissioning organization's colleagues, who evaluated the implementation model by reading the materials and responding to the questionnaire. Questionnaire results where analyzed through thematic data analysis and descriptive statistics. Thematic data analysis resulted in nine themes in total. Four themes were aimed at RQ1 and five themes were aimed at RQ2.

The respondents were divided into groups based on their role and expertise to get a better view of the validation aspect and different views various roles and knowledge bases might have on this topic. Four role groups were identified: consultants, developers, architects, and strategic leadership. Consultants consisted of eight respondents, developers consisted of six respondents, architects consisted of three respondents, and strategic leadership consisted of two respondents, resulting in the total amount of respondents, n=19. The individuals who responded to this questionnaire are working primarily within M365 and D365 environments, as respondents were identified from business units working primarily on business application solutions.

Consultant is pretty generic term to clarify in detailed working role description itself, but in this context based on responses, they are primarily functional consultants for M365 and D365 customer organizations, working with AI solutions, M365

offerings (e.g. SharePoint Online/On-Prem, Microsoft Teams), Power Platform and Power Apps. Developers clearly identified themselves as more technical professionals and many responses referred themselves as "software developer", indicating they are more technically advanced than consultants. Architects are also working with M365 and D365 environments and their work focuses on designing, developing, and guiding in M365 and D365 solutions and project or service deliveries. Strategic leadership roles consist of consulting manager and project manager. Their roles clearly differ from the other respondents since their work is more in strategic level and project leading than technical expertise.

5.1 Qualitative Study Results

This section will define and describe the results of the qualitative study. Thematic data analysis of open-ended questions and descriptive statistics analysis of Likert scale questions are explained in depth.

5.1.1 Thematic Data Analysis

Questions related to RQ1 (Q14, Q15, Q22-Q24) were primarily targeted at the productization aspect of the implementation model for M365 Copilot. Their focus were on selling point, feasibility, service delivery, packaging, and sales. Focus was ultimately to bridge a gap between theoretical implementation and commercial reality when real-world implementation project of M365 Copilot to organization could not be utilized for this thesis study. Through the thematic analysis for questions related to RQ1, four themes were identified: Operational Readiness & Technical Standardization, Service Productization & Market Scalability, operational Governance & Compliance Assurance, and Modular Value & Continuous Development.

Questions related to RQ2 (Q6-Q13, Q16-Q21) were primarily targeted at the

validation of the implementation model for M365 Copilot from the perspective of user adoption, security and regulatory compliance. Thematic data analysis for RQ2 focused on open-ended questions (Q6, Q9, Q10, Q12, Q13, Q16-Q20) and through analysis, five themes were identified: Productivity-Trust Tension, Peer-driven Adoption, Value Framing & Adoption Anxiety, Structured Rollout Dynamics, and Practical Compliance Boundaries.

Operational Readiness and Technical Standardization

This theme captures the productization idea of the implementation process of M365 Copilot into organization. Most consistently identified component is standardized baseline for readiness that act as a repeatable service offering. Securely implementing M365 Copilot begins with readiness evaluation and includes customer tenant technical compatibility, security posture check, and licensing prerequisites. Respondents agree that these assessments are good way to prevent failures during the deployment process with e.g. licensing mistakes and data oversharing, thus making this model standardized package and professional service offering.

Consultants showed most fragmentation in this theme, half of the consultants explicitly state their limited ability to evaluate the technical prerequisites of the Zero Trust and Copilot Optimization assessments of the implementation model. Many of them stated something in the lines of *"Outside my are of expertise"*, and *"I dont't feel I have sufficient understanding of this topic"*. The other half treat the optimization assessments as necessary with licensing and tenant baselines: *"The Zero Trust assessment is very effective way to address technical compatibility or customers tenant security wise. It uses the standard security principles that are widely used in everywhere."*

Developers evaluated the readiness assessments in the terms of whether they fit the ecosystem, meaning Microsoft-native alignment and whether they will actually

prevent issues in later deployment phases. Some developers also state their lack of expertise in this area to evaluate further. All in all developers state that productization should include structured baseline and concrete mechanism to translate baseline into actions for developers to execute. Actions would include tasks related to permissions and licensing, data hygiene, and technical controls.

Architects strongly agree that readiness should assess risk prevention and mandate these readiness assessments to prevent data oversharing or licensing issues. They also state that these assessments are important and necessary, but only form baseline of risk mitigation and are insufficient on their own. Secure deployment depends on later remediation: *"Success still depends on later actions like access cleanup, governance and labeling, DLP, and user preparation."*

Strategic leaders are clearly contributing to this theme from decision-making and readiness validation perspective. They are emphasizing that assessments should provide comprehensive insight of organizational readiness before scaling M365 Copilot usage organization wide, rather than just narrow technical checklist: *"I would recommend completing the pilot with our baseline assessment covering areas such as Purview, data management, and Zero trust. This would provide a more comprehensive understanding of the organization's readiness and help ensure that key security, compliance, and data governance considerations are addressed before scaling further."*

Service Productization and Market Scalability

This theme describes the tension between hypothetical model and delivery reality. Customers are likely to face fast rollout pressures, resource constraints, and organizational bottlenecks that make it possibly hard to execute all five phases of the implementation model. Responses imply that implementation model should have non-negotiable and stable core actions that handles the most important steps for

deployment: security and governance fundamentals. Additionally tailoring based on customer organizational or data maturity is offered to remain feasible across various organizations.

Consultants emphasize the feasibility constraints such as cost and pressure to skip steps for faster deployment, especially in the steps where multiple stakeholders must be engaged (IT, HR, leadership etc.). Commercial reality with large scope of execution and significant financial investment is identified: *"Needs lots of internal motivation from customer side, bust might be possible with a dedicated customer team."* Consultants agree that many customers push to skip steps of deployments, but it also depends on organization: *"I think companies will skip a lot of steps, but depends very much of the organization and the data and material in their M365."*

Developers are divided by optimistic and pessimistic thought on delivery realism of the implementation model. Some view executing all phases as realistic when compliance documentation is helping with regulatory expectations and customers are not willing to take shortcuts protecting their data. Others state that executing all phases is not realistic and customers want to outsource everything with minimal costs. These opinions imply that implementation model should be versatile to support multiple customer profiles, as other customers are more compliance-driven and some are cost-driven.

Architects define the implementation model as a base framework that can be tailored based on customer, but core steps must be identified that should not be skipped lightly. Core steps include data auditing, security and governance, pilot phase, and monitoring. This is conceptually building the foundation for this theme: tiered delivery with non-negotiables.

Strategic leaders are focusing less on individual technical tasks in implementation and more about whether customers have sufficient maturity and resources to travel through the model from beginning to end successfully. They also emphasize

the differentiation between customers and all five phases should be reviewed in collaboration with customer to validate what steps are essential and if they already possess some existing materials or practices regarding Copilot adoption: *"It should be jointly agreed that they are sufficient to ensure the required level of quality for the customer organization."*

Operational Governance and Compliance Assurance

This theme reflects the views of AI usage policies and their practicality. Respondents view this policy as necessary but it will likely become burden for organizations to utilize. AI policies should not be only paper policy, but be implemented as operating model that handles AI usage rules, training, communication, and review routines like human-in-the-loop.

Consultants agree that governance is treated as trust and usability issues, policies are valuable if they provide clear shared rules and reduce uncertainty in daily work with assistance of M365 Copilot. On the other hand governance policies must be communicated and embedded to organization rather than simply documented: *"They only create real value when combined with training, communication, and change management."*

Developers also treat governance policies as necessary but they state that guidance must stay high-level enough to be usable and avoid granularity of unrealistic rules in practice. There is still risk that without clear rules, users might adopt AI tools inconsistently and leak sensitive information: *"Clear AI usage policies grant users shared rules for Copilot and reduce uncertainty and the sharing of inaccurate and risky information."* Developers reinforce the argument that using Copilot requires governance that is designed for human behaviour and not only technical enforcement.

Architects tend to connect governance policies with security measures to achieve

broader control of customer environment: *"AI policies together with right security measures is how it becomes practical in my opinion."* This is implying that layered controls are better than relying on policies alone and treating governance as part of defense-in-depth.

Strategic leaders are framing governance policies as essential but at the same time difficult task since AI evolves rapidly and use cases between users and departments might vary a lot: *"Despite these challenges, establishing such policies is a must to manage risks related to data security, compliance and content accuracy."* Governance policies should be cross-functional and maintained over time, not just one time statement. This reinforces the fact that governance policies regarding Copilot and AI usage requires ongoing effort and possible support from commissioning organization experts.

Modular Value and Continuous Development

This theme captures recommendations from respondents for making this implementation model more easier to sell and deliver to customers. Implementation model could be shifted into modular service packages to make value per phase more explicit with clear outcomes, metrics, and monetary value. Tailored timelines for different customer types and sizes came up a lot in the responses. Lastly monitoring and searching for new Copilot capabilities over time is seen as a possibility develop AI usage possibilities continuously to keep up with rapid development of AI tools and Copilot.

Consultants are primarily providing sales-oriented thinking to make model more selling as a professional service offering. They highlight agentic use cases and possibility to create separate versions of implementation model based on customer size and maturity: *"Perhaps include evaluation of current processes and idenfitying agentic use cases to redefine use cases should stand out a little bit more as a part of the*

offering." Some respondents are concerned that the timeline presented in the implementation model is too long and selling this as a complete model could be hard because it requires multiple stakeholder profiles to participate and engage: *"It involves many different company stakeholders (IT&Security/HR/Leadership..) and might be difficult to "sell" in that sense, but shows very well it's not just plug and play to take Copilot into use."* Consultants are pushing for modular value with package offerings that reduce cognitive load and offers clear value promises and customer-specific examples.

Developers contribute two relevant messages for productization, firstly model should be scaled to customer needs with customer specific examples: *"In the selling moment, the model should be scaled to the customer's needs, and maybe even provide examples of customer specific effects."* Secondly some developers feel this model reveals the fact that M365 Copilot implementation is difficult task without sufficient knowledge: *"To me with no experience about implementing Copilot the model seems to be very complicated and hard to adopt."* Other developers also hesitate to give suggestion for productization, since this topic is outside their expertise area.

Architects are clearly advocating for AI capability lifecycle refresh, meaning that rapid development of AI capabilities should be kept under constant surveillance additionally to compliance and user metrics in the monitor phase of the model: *"Usage metrics and compliance is of course important but so might the new capabilities of Copilot."* Other respondent advices in converting model into cleared packages: *"I would probably try to convert this to some fixed service packages so there would be more ready-made stuff to select from."*

Strategic leaders are generally satisfied with the implementation model structure, one respondent would emphasize for customers concrete business values the would be getting out of implementation of M365 Copilot: *"I would focus more on really showing what the customer is getting out of each step, so it's clear what's being*

achieved and how success is measured. This way, the value is obvious and everyone can see the impact of each part of the process."

Productivity-Trust Tension

This theme captures the adoption incentive versus friction in output trust that might arise in users adopting Copilot. Responses are validating TAM framework's perceived usefulness rather strongly with practical examples like time saving, faster drafting and information retrieval. On the other hand, responses reflect also concerns about too generic and overwhelming responses, poor code quality, and the need for excessive prompting when working with M365 Copilot. In the scope of TAM framework, usefulness factors are present, but also damped with perceived cost of use and perceived risk of error.

Consultants frame perceived usefulness around content and communication, tasks like drafting presentations, summaries and emails, and cross-search across M365 tenant are identified: *"Creating content such as presentations, planning, visualizations. Copilots speed and quality is definitely enough."* Trust friction is also visible in multiple responses, articulating that Copilot's output can be generic and require significant validation: *"There will be quality issues as there are no or little sanity checks, also the wording is usually very generic and overwhelming."*

Developers are emphasizing usefulness similarly to consultants, via faster troubleshooting and information retrieval, and also support for complex problem-solving and documentation tasks: *"Significantly speeds up the automation of repetitive tasks, the preparation of summaries for large client portfolios, and the drafting of documentation."* Developers' trust friction leans more to technical side, as Copilot is seen producing low quality code and needing excessive amount of prompting from time to time: *"At least from my experience Copilot is incapable of doing quality code and it needs a lot of prompting to get it to work."*

Architects are defining usefulness of Copilot across various roles, like presales, and consulting: *"For example, if you work in presales, Copilot can summarize documents and help understand requirements. In consulting, you can brainstorm with Copilot regarding problems or solutions. In outlook, it helps understand long email chains."* Responses focus on strategic leverage and where Copilot accelerates synthesis and brainstorming rather than rework burden.

Strategic leaders reference productivity and usefulness through more operational terms than other role groups: *"Time used to find documentation easier with Copilot now. Easier to schedule meetings with more than one person, more effective, prioritizing your emails etc."* Indicating that reinforced and credible framing of impact must be visible to sustain acceptance.

Peer-driven Adoption

This theme reflects DOI framework's diffusion logic: adoption process of M365 Copilot is framed as social process, not just technical, where early adopters (Copilot champions) increase the observability factor of Copilot's benefits and use cases, and reduce uncertainty of Copilot usage through peer support. Early adopters normalize use through user training. Responses indicate that early adopters are rather essential part of user adoption and model's adoption effectiveness will depend on whether early adopters are added as a real infrastructure and not just informational add-on factor.

Consultants describe champions as central factors when they provide concrete examples and peer-to-peer support, lowering the barrier for users to seek help with Copilot. Responses clearly state the conditions of diffusion, champions must have consistent communication, dedicated time for championing, and peer to peer tone, not top to down "commanding": *"Early adopters are often crucial, as they help make Copilot's benefits concrete for colleagues through day-to-day work. Peer support and*

practical examples significantly reduce the adoption threshold during the rollout phase and build trust in the new tool." Some criticality is seen as one consultant states about the possibility of early adopters being skeptical: *"I still see a potential risk here, what if the early adopters does not think Copilot is the way to go. Will that effect other employees thoughts about Copilot negatively."*

Developers emphasize champions as practical validators and knowledge sharers, but they also highlight that adoption depends on whether champions are showcasing example scenarios and use cases that could actually benefit real work, rather than generic demos: *"Actually seeing others have AI perform tasks you still do by hand is likely to speed up adoption. We've all seen the polished Microsoft demoes, but their use cases can be far removed from our daily work. Early adopters will be the ones that make the difference."*

Between architects there is some granularity on this theme. Two architects clearly state that champions are the ones who distribute learning across organization and break the mindset of Copilot being optional, but one respondent believes that champions will have small impact and most efficient adoption results come from colleagues: *"I think they (early adopters) have a small impact as normally those are active in the organization anyway. Best usage comes from peer level colleagues."*

Strategic leaders are cheering champions as trusted advocates in the deployment process, setting standards and giving valuable feedback from Pilot phase to Rollout phase: *"They set the standard and are extremely valuable as support in the eventual Rollout-phase. During the Pilot phase feedback received from these Copilot Champions is highly relevant on what will be rolled-out and in which stages."*

Value Framing and Adoption Anxiety

This theme describes how adoption is shaped by credibility and emotional impact of value from M365 Copilot usage. Theme reflects DOI and TAM frameworks with

factors of relative advantage, observability, communication, and perceived value and trust. Responses indicate that generic claims of time savings and reduced administrative burden can fail if they are not role-specific, or aligned with real-life workflows. Hours saved by using M365 Copilot is also associated with adoption anxiety and fear of replacement, implying the importance of properly defined communication to users.

Consultants agree that time saving might be initial motivator for Copilot usage but insist that sustained adoption depends on perceived improvement in quality and speed: *"Time savings are an effective initial driver for Copilot adoption, but lasting engagement comes when users feel that Copilot enhances the quality of their work or thinking, not merely the speed."* The OCM preparation communication plan is seen as good in highlighting promises and advertising but they should be based on solid facts: *"Highlighted promises have to be realistic and close to the users actual work. There should be actual data to support these highlights and also real life examples and stories."*

Developers are lining up with consultants and are also strongly suggesting that demonstrations for specific tasks and roles are bringing the real value of OCM preparation communication plan: *"If you take an existing example from a person's work task and are clearly able to show the increased efficiency of using Copilot, the difference is easier to see and the strategy is effective. If the highlighted tasks have nothing to do with the person's own work, it is harder to tie into every day work."* Developers are also concerned about Copilot's ability to save working time and many responses reveal the fear of being replaced by AI: *"Usually people just think that half of the people get fired if the saving is 50% or 20 hours per week, so I would not use that for end users at all."* and *"Hours saved makes people anxious about the future."*

Architects share the fear with developers of being replaced by AI, if hours saved is showcased too much in the communication plan: *"It can also create some fear about being replaced by AI. So this should be part of the communication plan also to reduce*

adoption anxiety." Architects agree that the communication plan is reasonably good at strategic level and that all employees are eager to do fewer repetitive tasks. In summary communication plan is one way to highlight Copilot's benefits and help engage with it, but fear aspect of layoffs because of rapid and aggressive AI implementation must be handled with care.

Strategic leaders are pushing one of the most strict criterion for credibility, success must be defined and measured by department and user groups. Highlighting hours saved must have structured evidence and tailored success metrics: *"Copilot is not a one size fits all solution, its value depends on how well it is adapted to the unique needs and workflows of each team. Because employees will use Copilot in different ways, success metrics should also vary across departments, focusing on the outcomes that matter most to each group. Without this tailored approach, the impact can feel unclear or irrelevant to users."*

Structured Rollout Dynamics

This theme represents DOI's trialability and complexity perception, alongside pilot sufficiency and conditions for scaling up the deployment of M365 Copilot. Responses perceive five-phased model as adoption foundation that reduces uncertainty of structured progression, but also imply that too structured model can cause friction in administrative load and temptation to skip phases. Model drives adoption when its structure enhances clarity and learning cycles but might lead to friction in adoption if structure is experienced as bureaucratic mess.

Consultants are articulating structural issue with implementation model, clear steps are increasing control but the number of task and restrictions to adopt M365 Copilot make it feel more complex in practice: *"In in fact does reduce perceived complexity to have clear implementation model that has every step that needs to be done written down. But the fact that there is many phases with many tasks to be done*

it still unfortunately is pretty complex to implement Copilot in a proper manner." So in general consultants agree that model with separate steps and phases is necessary to achieve comprehensive implementation of M365 Copilot, but the deployment is bound to be tedious and complex in any case.

Developers similarly to consultants, are stating that phased implementation model is in place, but that does not necessarily mean it will not be complex to push through: *"I am not sure if it reduces complexity but I think it is not an easy process and following the implementation model the copilot implementation can be more successful than not having a model."* On Pilot phase developers are agreeing that group for pilot phase should be selected based on the size of the organization and distribution of various roles, every case must be presented and tested before moving on to scaling up the adoption of M365 Copilot.

Architects are also supporting phased approach of implementing AI tools, but some argue that timeline introduced in the model is too long and might reduce relevance due to rapid AI development that is at hand right now: *"The timeline feels rather long to me; within that time frame, new AI tools could already come into use."* On Pilot phase architects are implying that scaled up rollout requires continuous feedback, tuning, and monitoring, indicating that trialability does not end at Pilot phase.

Strategic leaders highlights that reinforcement for the five-phased model is required for sustained adoption rates: *"There need to be reinforcement included. If reinforcement is not in place, even the most well planned rollout can fail to create lasting change. Users may initially adopt Copilot, but without ongoing support, encouragement, and visible value, they are likely to fall back into old habits and manual ways of working."* On Pilot phase, both parties in this group agree that early adopters should be selected based on organization size and number of user groups or teams.

Practical Compliance Boundaries

This theme wraps up TOE framework's regulatory environment, security, and compliance requirements, as well as validation of EU AI Act and NIS2 directive included in the implementation model. Theme consolidates the compliance validation into argument about boundary conditions, respondents generally confirm the importance of security and governance controls, but also identify risks and operational feasibility as limiting factors. The responses also show high-level confidence in regulatory bridging between EU AI Act and NIS2 according to the implementation model, but widespread of uncertainty on this topic is clearly visible. Specific controls like the principle of least privilege, Restricted Content Discovery, sensitivity labeling, and human-in-the-loop are evaluated as effective and concrete methods if embedded within a robust permission governance that is continuously maintained.

Consultants are emphasizing that success rate of compliance controls are affected by underlying permission governance, controls like Restricted Content Discovery could overly restrict content and create tension between adoption and compliance. Restricted Content Discovery is seen as great way to address data exposure risks but wider mitigation requires addressing permission governance: *"The problem is that it (RCD) does not affect existing permissions so once again the company must go through permission in order to use this."* Many consultants are avoiding to answer topics related to regulatory requirements and are stating their insufficient expertise in regulatory field*: "Cannot say, needs more investigation and thought."*and *"Unfortunately it's difficult to answer this without proper knowledge of the regulatory."* This is suggesting that model should provide more detailed and operational translation for various roles to achieve confidence with compliance matters.

Developers are lining up with the consultants about their lack of knowledge about specific regulations and are not providing too detailed insights on those. On security part, they are focusing on scope and feasibility, whether the controls introduced

in the model concentrating too narrowly on SharePoint and how are formats not within Microsoft tenants covered for sensitivity labeling. Responses are especially highlighting the importance of maintaining human-in-the-loop with all AI related interaction: *"The importance of verifying and critical thinking towards AI output should be highlighted for the employee, so that the human-in-the-loop steps is of significance."* While some developers are more skeptical of the human-in-the-loop mandate, indicating that humans might not use AI ethically: *"Human-in-the-loop might still use AI very unethically."*

Architects are providing clear defense-in-depth framing for security concerns as principle of least privilege is seen as great practice in all data accessing, Restricted Content Discovery is in place to limit search results for SharePoint files in addition to maintain permission governance, and Purview sensitivity labeling is seen as practical, if automated to save cognitive load and time from customer. Architects are also not providing very detailed opinions on how EU AI Act and NIS2 are bridged to internal operations, but no concerns arise in this topic: *"I am not thoroughly familiar with EU AI Act or NIS2 but from what I know, it seems that his model reduces risk related to Copilot deployment significantly."*

Strategic leaders are identifying gaps between internal operations and external regulatory and responses state clearly that model provides clear definitions of EU AI Act and NIS2 directive and takes activities carried out at high level into account, but lacks detailed requirements directed at these regulations. Responses are indicating the need for deeper dive on topics like data location, data processing, and configuration settings that administrators need to understand. Customer organization must be provided with well defined handover for them to be able to maintain compliance after the implementation project ends: *"Without proper handover and enablement, there is a risk that the organization may struggle to maintain compliance once the partner steps away."* For security measures, this group thinks it is concep-

tually strong and correct but enhances the importance of operational sustainability, and whether customer organization truly understand the meaning behind security measures and use them properly over time: *"Maintaining Purview requires ongoing effort, and the related ownership and responsibilities mut be clearly defined to ensure it is effective in practice."*

5.1.2 Descriptive Statistics

Seven of the questions in the questionnaire where Likert scale questions (Q2-Q4, Q7, Q8, Q11, Q21) and they are all targeted at RQ2 which aims to validate the implementation model's security, user adoption, and regulatory compliance. Q2-Q4 were part of the questionnaire where users background was identified. Q7 aims to reflect on TAM framework's perceived ease of use through model's take on learning curve. Q8 aims to reflect on DOI framework's compatibility aspect with effectiveness of Organizational Data Audit, and Q11 to complexity aspect with reduced complexity of model's phased structure. Q21 aims to reflect on NIS2 directives reporting mandates.

Total response size for these questions where rather small (n=19) as this questionnaire aimed to be qualitative, rather than quantitative. Respondents were divided into groups based on their role: consultants (n=8), developers (n=6), architects (n=3), and strategic leaders (n=2). Role groups, role counts, questions and the average scale responses per role and total can be seen in Figure 5.1. Likert scale was 1-4, thus mathematical midpoint would be 2.50.

Role Group	Role count	M365 Copilot hands-on-experience (Q2)	Familiarity with security and compliance measures for M365 Copilot (Q3)	Comfortability of adapting new technologies and tools (Q4)	Effectiveness of Prompt libraries and Prompt Coach Agents on learning curve for users (Q7)	Effectiveness of Organizational Data Audit (Q8)	Anticipation of five-phased model's reduced perceived complexity (Q11)	Capability to recognize and report Copilot related incident under NIS2 directive (Q21)
Architect	3	3.33	2.33	3.67	2.67	3.00	3.00	1.67
Consultant	8	2.88	2.00	3.13	3.00	2.88	3.00	2.13
Developer	6	2.67	1.67	3.33	2.83	3.17	3.33	2.33
Strategic leadership	2	3.00	3.00	3.50	2.00	3.00	3.50	2.50
Total	**19**	**2.89**	**2.05**	**3.32**	**2.79**	**3.00**	**3.16**	**2.16**

Figure 5.1: Likert scale question averages divided per role group

As seen on the Figure 5.1, highest average across all roles of 3.32 was reached in Q4, indicating that individuals are comfortable and ready with adapting new technologies, especially AI tools. Also rather high average of 3.16 is seen in Q11, implying that anticipation that implementation model will reduce perceived complexity is rather likely based on respondents views. Lowest average across all roles of 2.05 was reached in Q3, indicating that there is some lack of confidence and understanding of security and compliance measures for M365 Copilot.

Based on background questions (Q2-Q4) all roles are rather experienced with M365 Copilot and are comfortable with adopting new tools into their daily work. Architects are especially driven by Copilot, since they possess the highest average of hands-on-experience (3.33). Architects are also the most comfortable with adopting new tools (3.67). Familiarity with security and compliance methods targeted at M365 Copilot has lower rate of confidence in all roles, especially developers with only average of 1.67 in Q3. Indicating that Zero Trust framework and related security measures are not likely part of the daily work of these roles and individuals.

TAM framework's perceived ease of use reflected on effectiveness of Prompt libraries and Prompt Coach Agents (Q7) are seen as somewhat effective, as total average of all roles reaches over the midpoint. Consultants are most hopeful that identified methods to boost user's perceived ease of use of M365 Copilot will be

effective (3.00). Strategic leaders are most skeptical of these methods with only the average of 2.00.

DOI framework's compatibility aspect on Organizational Data Audit (Q8) is seen as rather effective across all roles with the average of 3.00. Developers are most convinced that Organizational Data Audit will be effective in ensuring that Copilot's output is always consistent with existing data structure of the organization. Reduced perceived complexity of five-phased implementation model (Q11) is also seen rather likely with overall average of 3.16. Strategic leaders are most agreeing that the implementation model's phases are giving good structure for the implementation process.

Capability to recognize reporting mandates related to NIS2 (Q21) has the second lowest average across all roles, with only 2.16. Architects seem the most uncertain whether they are able to recognize and report Copilot related incident under NIS2 directive, with only 1.67. Strategic leaders are sitting directly at the midpoint of 2.50.

Parts of Likert scale responses are clearly strengthening the themes identified from the qualitative aspect by showing broad role-level alignment with the validation aspect of implementation model. Q7 with perceived ease of use is linked to theme Productivity-Trust Tension and is indicating that the effectiveness to overcome learning curve to reduce adoption friction is likely to be visible among end users. Q8 and Q11 with compatibility and complexity measures are linked to theme Structured Rollout Dynamics and are supporting the fact that responsdents generally perceive the five-phased implementation model as compatible structured baseline and that Organizational Data Audit is perceived as practical and efficient method to monitor Copilot's outputs. Q21 with NIS2 reporting mandate is linked to theme Practical Compliance Boundaries and aligns with the visible uncertainty directed at the regulatory requirements presented in the implementation model.

5.2 Qualitative Study Limitations

Qualitative study conducted in this thesis faced some limitations that may have an effect on the results comprehended from the questionnaire results.

Based on responses, qualitative interviews could have resulted in more comprehensive data than questionnaire, since people tend to find it easier to speak than write. Electronic survey resulted in many empty responses or questions were simply brushed aside with statements like *"I don't know"* and *"I don't feel I can comment on this"*, although in an interview settings they probably would have said something more substantial. Additionally to that, respondents had only 14 days to give responses to questionnaire, which might have led to a sense of urgency and this way could have lowered the quality of responses.

Questionnaire collected 19 responses in total, which is sufficient amount of respondents for qualitative questionnaire in the scope of this thesis, but for descriptive statistics it might be insufficient due to small amount of responses to draw hard statistical conclusions. Four role groups were identified from the responses and their relation to each other is uneven. The responses from consultants and developers more likely to provided a more comprehensive picture, since there were more of them than architects and strategic leaders. Some deficiency in the knowledge of security measures and Microsoft specific security tools is clearly noticeable from the respondents. This might have have affect on the validation aspect of the security critical matters. Similar deficiency in the knowledge of the EU AI Act and NIS2 is rather obvious.

6 Discussion

In this chapter discussion of the proposed implementation model is evaluated through the research questions in this thesis and validation with qualitative study and related thematic analysis and descriptive statistics. Future work for implementation model is identified and limitations of this thesis are reviewed.

6.1 Evaluation of the Implementation Model

Research question 1 (RQ1) asked how can a secure Microsoft 365 Copilot implementation be effectively productized into a organizational service offering. Proposed model was conducted after thorough literature review of relevant topics in Chapter 2. Implementation model for M365 Copilot is described in Chapter 4. Model was validated with qualitative study, including thematic data analysis where themes were identified specifically around this research question during analysis process. Themes are Operational Readiness & Technical Standardization, Service Productization & Market Scalability, operational Governance & Compliance Assurance, and Modular Value & Continuous Development. Themes were analyzed in depth in Chapter 5. Themes are successfully capturing the key points of effective productization and organizational service offering. Themes are reflecting on the level of expertise respondents have on this topic and clearly highlights what worked well in the model and what needs to be improved and clarified.

Research question 2 (RQ2) asked how well does the proposed implementation

model drive user adoption while ensuring security and regulatory compliance. Same implementation model as in RQ1 is validated with the same qualitative study, including thematic analysis where themes identified specifically around this research question were analyzed in Chapter 5. Themes are Productivity-Trust Tension, Peer-driven Adoption, Value Framing & Adoption Anxiety, Structured Rollout Dynamics, and Practical Compliance Boundaries. Additionally descriptive statistical analysis was also necessary as Likert scale questions in questionnaire were also aimed to answer this research question and they were closely aligned with relevant themes in Chapter 5. Themes are successfully capturing the key points of user adoption, security, and regulatory requirements. Themes reflect on the respondents views of how high rate of user adoption and high-quality user experience are being achieved for M365 Copilot with proposed model and which parts require special attention. Themes reveal that respondents have wide range of skill levels and experience regarding security and regulatory measurements. This variation of expertise was reflected in the responses as uncertainty.

6.2 Future Work

For future work the goal is to continue to work with the M365 Implementation model for commissioning organization after the proposal of this baseline framework created in the scope of this thesis. This means making changes based on the recommendations and expertise comments identified from the questionnaire. Another goal in the future is to use the implementation model in a real-world customer project, to continue validating and improving the model based on customer feedback and encountered setbacks or shortcomings.

Themes for RQ1 focused on productization and service offering aspects. Based on the responses and thematic analysis, to make implementation model more effective as product and service offering, small refinements are in place. Model should include

stable core actions that focus on security and governance. On top of these, tailoring based on customer case can be done and offered. Even tiered service packages for different level of AI and data maturity could be considered for development. Security posture check at the beginning of implementation process is seen as very important and must be sufficiently emphasized. Operational governance, and especially communication must be done carefully and thoughtfully, depending on customer, in order to avoid fear of being replaced by AI.

Themes for RQ2 focused on user adoption, security and regulatory compliance from the perspective of M365 Copilot implementation. User training and especially practical use case demonstrations for specific user and expert roles. Difficulty and challenges with prompting is clearly noticeable and needs addressing in user training. Commissioning organization already possess training material for M365 Copilot usage, but they will be improved based on the questionnaire results. Responses also emphasize that M365 Copilot implementation must be seen as social process and not only technical process. Role of champions must be clear and refined in order to serve their purpose in user adoption and diffusion of M365 Copilot. While security measures are generally considered sufficient, specific tasks and steps to ensure holistic safety of system and user, are to be defined in more detail into the implementation model. Similarly the role of EU AI Act and NIS2 should be refined to clearly state the necessary steps to be compliant from the start and after implementation project is successfully brought to an end.

6.3 Thesis Limitations

Some limitations were encountered during the thesis working process. During the literature review it was noticed that there is not much availability of peer reviewed articles and other publications regarding M365 Copilot or Microsoft's Copilot products in general. This is because Copilot products are fairly new and in constant and

rapid cycle of development. This is the reason thesis does not reference too many peer reviewed articles regarding Microsoft Copilot products, lowering the total reference amount of reliable publications.

Implementation model for M365 Copilot relies on many online sources, mostly Microsoft's documentation. Implementation model was build based on Microsoft's recommendations and to utilize Microsoft pre-configured security products and set of tools. This is based on request from commissioning organization, which ultimately is a Microsoft partner and the fact that as mentioned, there were only few available reliable publications around this topic.

Validation of implementation project would have ideally been based on implementation of M365 Copilot in actual customer project to showcase real user experiences and results. Qualitative study was after all highly theoretical and high-level study that merely points the way toward real-world outcomes. Other limitations regarding qualitative study are discussed in 5.2.

7 Conclusion

The rapid implementation pace of GenAI tools has created challenge for consulting and other IT companies, how to transform theoretical and technical framework consisting of multiple phases and tasks into professional service offering for customer organizations. This thesis aimed to address this challenge by proposing five-phased implementation model for M365 Copilot, Microsoft's top LLM powered AI assistant. Utilizing qualitative study with thematic data analysis and descriptive statistics to validate implementation model. Study gathered 19 responses for questionnaire that consisted of open-ended and Likert scale questions. Respondents consisted of IT experts with various skill levels and expertise regarding AI and security knowledge. The primary object of qualitative study was to answer how could proposed implementation model be efficiently productized as professional service offering and how well does it correspond to user adoption, security and regulatory compliance requirements regarding M365 Copilot.

Qualitative study findings validate that while implementation model is structurally sound, it cannot be perfectly productized without some strategic optimization. In total nine thematic themes were identified during the thematic analysis process and these themes were used to evaluate the modification needs for implementation model regarding it's productization, user adoption, security, and regulatory requirement needs. First, changes in emphasizing specific phases and tailoring opportunities based on customer project must be utilized. Secondly user experience,

training and overall user adoption must be addressed with necessary communication methods. Thirdly, details in security and regulatory requirement measures must be deepened in order for them to be seen as critical steps resulting in better holistic understanding of them. Regulatory compliance parts especially targeted at the EU AI Act and NIS2 must be explained more clearly and explicitly state what actions are to be taken to be fully compliant.

Primary practical implication of this thesis is the delivery of implementation model for M365 Copilot with cybersecurity considerations for commissioning organization. By integrating the study findings, the proposed model has been translated into professional service offering that can be further developed to satisfy all needs. For the commissioning organization, this thesis provides a blueprint for M365 Copilot service productization that builds a bridge between operational strategic leadership and technical delivery of M365 Copilot into organizations.

From academic perspective, this thesis contributes in literature related to AI, cybersecurity, dedicated adoption models, and regulatory compliance with specified regulations. While existing research still grasps a weak connection between AI adoption in enterprises, with necessary security and regulatory measures, this thesis provides empirical evidence that GenAI implementation models must embed strict data, security, and compliance frameworks in order to be theoretically complete.

As discussed in Section 5.2, the findings and results of this study are based on theoretical evaluations and opinions from a specialized panel audience, rather than empirical field data. Therefore, future research should focus on actual case study or customer project where this proposed model is actively deployed within organization's tenant. Monitoring real-world implementation project, would allow researchers to measure operational metrics in more concrete sense and monitor any shortcomings in security or regulatory compliance.

References

[1] Twoday. "Twoday - we develop it solutions that make an impact", Accessed: Oct. 16, 2025. [Online]. Available: https://www.twoday.com/.

[2] Toloka. "Difference between ai, ml, llm, and generative ai", Accessed: Oct. 22, 2025. [Online]. Available: https://toloka.ai/blog/difference-between-ai-ml-llm-and-generative-ai/.

[3] C. Zhang and Y. Lu, "Study on artificial intelligence: The state of the art and future prospects", *Journal of Industrial Information Integration*, vol. 23, p. 100 224, Sep. 2021, ISSN: 2452-414X. DOI: 10.1016/J.JII.2021.100224.

[4] P. Bory, S. Natale, and C. Katzenbach, "Strong and weak ai narratives: An analytical framework", *AI and Society*, vol. 40, pp. 2107–2117, Apr. 2025, ISSN: 14355655. DOI: 10.1007/S00146-024-02087-8/METRICS.

[5] D. Puthal and S. Mohanty, "Cybersecurity issues in ai", *IEEE Consumer Electronics Magazine*, vol. 10, pp. 33–35, Jul. 2021, ISSN: 21622256. DOI: 10.1109/MCE.2021.3066828.

[6] A. Oyatomi, "Adversarial attacks and defense in ai systems: A review of cybersecurity problems and new protection", *International Journal for Multidisciplinary Research (IJFMR)*, vol. 7, 6 2025, ISSN: 2582-2160. DOI: 10.36948/ijfmr.2025.v07i06.57627.

[7] V. Z. Mohale and I. C. Obagbuwa, "A systematic review on the integration of explainable artificial intelligence in intrusion detection systems to enhancing transparency and interpretability in cybersecurity", *Frontiers in Artificial Intelligence*, vol. 8, p. 1 526 221, 2025, ISSN: 26248212. DOI: 10.3389/FRAI.2025.1526221.

[8] Amazon Web Services, AWS. "What is generative ai?", Accessed: Nov. 6, 2025. [Online]. Available: https://aws.amazon.com/what-is/generative-ai/.

[9] S. Feuerriegel, J. Hartmann, C. Janiesch, and P. Zschech, "Generative ai", *Business and Information Systems Engineering*, vol. 66, pp. 111–126, 1 Feb. 2024, ISSN: 18670202. DOI: 10.1007/s12599-023-00834-7.

[10] Z. L. Teo, C. W. N. Quek, J. L. Y. Wong, and D. S. W. Ting, "Cybersecurity in the generative artificial intelligence era", *Asia-Pacific Journal of Ophthalmology*, vol. 13, p. 100 091, 4 Jul. 2024, ISSN: 2162-0989. DOI: 10.1016/J.APJO.2024.100091.

[11] R. Babaei, S. Cheng, R. Duan, S. Zhao, R. Babaei, S. Cheng, R. Duan, and S. Zhao, "Generative artificial intelligence and the evolving challenge of deepfake detection: A systematic analysis", *Journal of Sensor and Actuator Networks 2025, Vol. 14,*, vol. 14, 1 Feb. 2025, ISSN: 2224-2708. DOI: 10.3390/JSAN14010017.

[12] V. Estocapio, R. M. Bilog, J. Cacananta, J. M. Corpuz, B. I. Jr., S. Paneda, and R. J. Asuncion, "Examining the potential benefits and ethical risks of genai in lesson planning: A tam approach", *Journal of Teaching and Learning*, vol. 19, pp. 179–197, 4 Oct. 2025. DOI: 10.22329/jtl.v19i4.10056.

[13] H. Naveed, A. U. Khan, S. Qiu, M. Saqib, S. Anwar, M. Usman, N. Akhtar, N. Barnes, and A. Mian, "A comprehensive overview of large language models",

ACM Transactions on Intelligent Systems and Technology, pp. 1–72, Oct. 2025, ISSN: 2157-6904. DOI: 10.1145/3744746.

[14] Google Cloud. "Large language models powered by world-class google ai", Accessed: Nov. 13, 2025. [Online]. Available: https://cloud.google.com/ai/llms.

[15] M. A. K. Raiaan, M. S. H. Mukta, K. Fatema, N. M. Fahad, S. Sakib, M. M. J. Mim, J. Ahmad, M. E. Ali, and S. Azam, "A review on large language models: Architectures, applications, taxonomies, open issues and challenges", *IEEE Access*, vol. 12, pp. 26 839–26 874, 2024, ISSN: 21693536. DOI: 10.1109/ACCESS.2024.3365742.

[16] Z. Wang, Z. Chu, T. V. Doan, S. Ni, M. Yang, and W. Zhang, "History, development, and principles of large language models: An introductory survey", *AI and Ethics 2024 5:3*, vol. 5, pp. 1955–1971, 3 Oct. 2024, ISSN: 2730-5961. DOI: 10.1007/S43681-024-00583-7.

[17] OpenAI. "Introducing chatgpt | openai", Accessed: Dec. 3, 2025. [Online]. Available: https://openai.com/index/chatgpt/.

[18] OpenAI. "Introducing gpt-5.5 | openai", Accessed: May 5, 2026. [Online]. Available: https://openai.com/index/introducing-gpt-5-5/.

[19] D. Humphreys, A. Koay, D. Desmond, and E. Mealy, "Ai hype as a cyber security risk: The moral responsibility of implementing generative ai in business", *AI and Ethics 2024 4:3*, vol. 4, pp. 791–804, 3 Feb. 2024, ISSN: 2730-5961. DOI: 10.1007/S43681-024-00443-4.

[20] S. Gulyamov, S. Gulyamov, A. Rodionov, R. Khursanov, K. Mekhmonov, D. Babaev, and A. Rakhimjonov, "Prompt injection attacks in large language models and ai agent systems: A comprehensive review of vulnerabilities, at-

tack vectors, and defense mechanisms", *Information 2026, Vol. 17,*, vol. 17, p. 54, 1 Jan. 2026, ISSN: 2078-2489. DOI: 10.3390/INFO17010054.

[21] Google Cloud. "What is an ai agent?", Accessed: Nov. 12, 2025. [Online]. Available: https://cloud.google.com/discover/what-are-ai-agents.

[22] S. Gao, A. Fang, Y. Huang, V. Giunchiglia, A. Noori, J. R. Schwarz, Y. Ektefaie, J. Kondic, and M. Zitnik, "Empowering biomedical discovery with ai agents", *Cell*, vol. 187, pp. 6125–6151, 22 Oct. 2024, ISSN: 0092-8674. DOI: 10.1016/J.CELL.2024.09.022.

[23] F. Tian, A. Luo, J. Du, X. Xian, R. Specht, G. Wang, X. Bi, J. Zhou, A. Kundu, J. Srinivasa, C. Fleming, R. Zhang, Z. Liu, M. Hong, and J. Ding, *An outlook on the opportunities and challenges of multi-agent ai systems*, 2025. arXiv: 2505.18397 [cs.MA]. [Online]. Available: https://arxiv.org/abs/2505.18397.

[24] M. Casalaina. "Exploring multi-agent ai systems", Accessed: Jan. 17, 2026. [Online]. Available: https://techcommunity.microsoft.com/blog/azure-ai-foundry-blog/the-future-of-ai-exploring-multi-agent-ai-systems/4226593.

[25] AI21. "What is a multi-agent system (mas)? | ai21", Accessed: Jan. 17, 2026. [Online]. Available: https://www.ai21.com/knowledge/multi-agent-system/.

[26] OWASP. "Llm08: Excessive agency - owasp gen ai security project", Accessed: Dec. 11, 2025. [Online]. Available: https://genai.owasp.org/llmrisk2023-24/llm08-excessive-agency/.

[27] B. Klein, C. Lewis, R. Isenberg, D. Gabrielli, H. Möllering, R. Engler, and V. Yuan. "Agentic ai security: Risks & governance for enterprises | mckinsey", Accessed: Dec. 12, 2025. [Online]. Available: https://www.mckinsey.com/ca

pabilities/risk-and-resilience/our-insights/deploying-agentic-ai-with-safety-and-security-a-playbook-for-technology-leaders.

[28] S. Sarferaz, "Implementing generative ai into erp software", *IEEE Access*, vol. 13, pp. 73 342–73 354, 2025, ISSN: 21693536. DOI: 10.1109/ACCESS.2025.3564133.

[29] R. Pasupuleti, R. Vadapalli, C. Mader, and N. Timothy, "Popular llm-large language models in enterprise applications", in *2024 2nd International Conference on Foundation and Large Language Models, FLLM 2024*, Institute of Electrical and Electronics Engineers Inc., 2024, pp. 125–131, ISBN: 9798350354799. DOI: 10.1109/FLLM63129.2024.10852443.

[30] F. D. Davis, "A technology acceptance model for empirically testing new end-user information systems: Theory and results", Ph.D. dissertation, Sloan School of Management, Massachusetts Institute of Technology, Cambridge, MA, 1986. [Online]. Available: https://dspace.mit.edu/handle/1721.1/15192.

[31] E. M. Rogers, *Diffusion of Innovations*, 5th. New York, NY: Free Press, 2003.

[32] N. Albishri, J. S. Rai, R. Attri, M. Z. Yaqub, and S. T. Walsh, "Breaking barriers: Investigating generative ai adoption and organizational use", *Journal of Enterprise Information Management*, vol. 39, pp. 267–288, 1 Feb. 2026, ISSN: 17410398. DOI: 10.1108/JEIM-01-2025-0010.

[33] L. G. Tornatzky and M. Fleischer, *The Processes of Technological Innovation*. Lexington, MA: Lexington Books, 1990.

[34] Y. Zhang, C. Liu, and S. Xia, "From hype to value: Harnessing generative ai in fashion retailing from a technology-organization-environment perspective", *Journal of Electronic Business & Digital Economics*, vol. 4, pp. 203–219, 2 Dec. 2025, ISSN: 2754-4214. DOI: 10.1108/jebde-11-2024-0042.

[35] Atlassian. "Technology roadmap: What it is and how to create one", Accessed: Dec. 4, 2025. [Online]. Available: https://www.atlassian.com/agile/project-management/technology-roadmap.

[36] MIT, Center for Information Systems Research. "Building enterprise ai maturity", Accessed: Dec. 4, 2025. [Online]. Available: https://cisr.mit.edu/publication/2024_1201_EnterpriseAIMaturityModel_WeillWoernerSebastian.

[37] OpenAI. "The state of enterprise ai | openai", Accessed: Jan. 17, 2026. [Online]. Available: https://openai.com/index/the-state-of-enterprise-ai-2025-report/.

[38] European Parliament and Council of the European Union, *Directive (EU) 2022/2555 of the European Parliament and of the Council of 14 December 2022 on measures for a high common level of cybersecurity across the Union (NIS 2 Directive)*, Official Journal of the European Union, L 333/80, 2022. Accessed: Mar. 13, 2026. [Online]. Available: https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX:32022L2555.

[39] European Comission. "Nis2 directive: Securing network and information systems | shaping europe's digital future", Accessed: Mar. 13, 2026. [Online]. Available: https://digital-strategy.ec.europa.eu/en/policies/nis2-directive.

[40] Cyber Risk CmbH. "Nis 2 directive, article 23: Reporting obligations", Accessed: Apr. 16, 2026. [Online]. Available: https://www.nis-2-directive.com/NIS_2_Directive_Article_23.html.

[41] V. Bolgouras, A. Zarras, C. Leka, I. Stylianou, A. Farao, and C. Xenakis, "Eu regulatory ecosystem for ethical ai", *AI and Ethics 2025 5:5*, vol. 5, pp. 5063–5080, 5 Jun. 2025, ISSN: 2730-5961. DOI: 10.1007/S43681-025-00749-X.

[42] European Parliament and Council of the European Union, *Regulation - eu - 2024/1689 - en - eur-lex*, 2024. Accessed: Mar. 20, 2026. [Online]. Available: https://eur-lex.europa.eu/eli/reg/2024/1689/oj/eng#pbl_1.

[43] European Parliament. "Eu ai act: First regulation on artificial intelligence", Accessed: Nov. 26, 2025. [Online]. Available: https://www.europarl.europa.eu/topics/en/article/20230601STO93804/eu-ai-act-first-regulation-on-artificial-intelligence.

[44] "The eu artificial intelligence act: Up-to-date developments and analyses of the eu ai act", Accessed: Nov. 25, 2025. [Online]. Available: https://artificialintelligenceact.eu/.

[45] Future of Life Institute. "Article 26: Obligations of deployers of high-risk ai systems | eu artificial intelligence act", Accessed: Apr. 16, 2026. [Online]. Available: https://artificialintelligenceact.eu/article/26/.

[46] M. Beltrán, "Ai algorithms under scrutiny: Gdpr, dsa, ai act and cra as pillars for algorithmic security and privacy in the european union", *Computers & Security*, vol. 158, p. 104 628, Nov. 2025, ISSN: 0167-4048. DOI: 10.1016/J.COSE.2025.104628.

[47] B.-J. Kim, S. Jeong, B.-K. Cho, and J.-B. Chung, "Ai governance in the context of the eu ai act", *IEEE Access*, vol. 13, pp. 144 126–144 142, 2025, ISSN: 2169-3536. DOI: 10.1109/ACCESS.2025.3598023.

[48] M. Durairaj, K. Bagilesh, A. Sathyamoorthy, and K. Shanmugam, "Inside-out ai strategy at microsoft: From capability building to commercialization", *Journal of Information Technology Teaching Cases*, 2025, ISSN: 20438869. DOI: 10.1177/20438869251383032.

[49] Microsoft. "Which copilot is right for me or my organization? | microsoft learn", Accessed: Oct. 22, 2025. [Online]. Available: https://learn.micro

soft.com/en-us/copilot/microsoft-365/which-copilot-for-your-organization.

[50] Microsoft. "Microsoft copilot: Your ai companion", Accessed: Oct. 30, 2025. [Online]. Available: https://copilot.microsoft.com/.

[51] Microsoft. "Overview of microsoft 365 copilot chat | microsoft learn", Accessed: Oct. 30, 2025. [Online]. Available: https://learn.microsoft.com/en-us/copilot/overview.

[52] Microsoft. "Download microsoft 365 copilot app on windows, mac, android & ios", Accessed: Oct. 30, 2025. [Online]. Available: https://www.microsoft.com/en-us/microsoft-365-copilot/download-copilot-app#downloadthemobileapp.

[53] Microsoft. "What is microsoft 365 copilot? | microsoft learn", Accessed: Oct. 16, 2025. [Online]. Available: https://learn.microsoft.com/en-us/copilot/microsoft-365/microsoft-365-copilot-overview.

[54] Microsoft. "What is microsoft security copilot? | microsoft learn", Accessed: Oct. 30, 2025. [Online]. Available: https://learn.microsoft.com/en-us/copilot/security/microsoft-security-copilot.

[55] GitHub Docs. "What is github copilot? - github docs", Accessed: Oct. 30, 2025. [Online]. Available: https://docs.github.com/en/copilot/get-started/what-is-github-copilot.

[56] Microsoft Azure. "Github copilot for any platform or code repository", Accessed: Oct. 31, 2025. [Online]. Available: https://azure.microsoft.com/en-us/products/github/copilot.

[57] Microsoft. "Copilot studio overview | microsoft learn", Accessed: Oct. 30, 2025. [Online]. Available: https://learn.microsoft.com/en-us/microsoft-copilot-studio/fundamentals-what-is-copilot-studio.

[58] A. Hesp-Gollins. "Microsoft copilot vs copilot studio: Differences, licensing & uses (2026)", Accessed: Jan. 4, 2026. [Online]. Available: https://www.hso.com/blog/microsoft-copilot-vs-studio.

[59] Microsoft. "Agents for microsoft 365 copilot | microsoft learn", Accessed: Apr. 13, 2026. [Online]. Available: https://learn.microsoft.com/en-us/microsoft-365/copilot/extensibility/agents-overview.

[60] Microsoft. "Get started with researcher in microsoft 365 copilot - microsoft support", Accessed: Apr. 16, 2026. [Online]. Available: https://support.microsoft.com/en-us/topic/get-started-with-researcher-in-microsoft-365-copilot-e63ab760-f3de-4c47-ae87-dad601b0e9c4.

[61] Microsoft. "Get started with analyst in microsoft 365 copilot - microsoft support", Accessed: Apr. 16, 2026. [Online]. Available: https://support.microsoft.com/en-us/topic/get-started-with-analyst-in-microsoft-365-copilot-ff505b9c-a06c-4be9-b855-69d89b1d25d2.

[62] Microsoft. "Data, privacy, and security for microsoft 365 copilot | microsoft learn", Accessed: Oct. 16, 2025. [Online]. Available: https://learn.microsoft.com/en-us/copilot/microsoft-365/microsoft-365-copilot-privacy.

[63] Microsoft. "How does microsoft 365 copilot work? | microsoft learn", Accessed: Oct. 2, 2025. [Online]. Available: https://learn.microsoft.com/en-us/copilot/microsoft-365/microsoft-365-copilot-architecture.

[64] Microsoft. "Overview of microsoft graph | microsoft learn", Accessed: Oct. 31, 2025. [Online]. Available: https://learn.microsoft.com/en-us/graph/overview.

[65] Microsoft. "What information does copilot use to answer my prompt? - microsoft support", Accessed: Mar. 19, 2026. [Online]. Available: https:

//support.microsoft.com/en-gb/topic/what-information-does-copilot-use-to-answer-my-prompt-934f537d-ff7d-4059-9fec-a751e4651307.

[66] Microsoft. "Semantic indexing for microsoft 365 copilot - data flows | microsoft learn", Accessed: Apr. 10, 2026. [Online]. Available: https://learn.microsoft.com/en-us/microsoftsearch/semantic-index-for-copilot#data-flows.

[67] Microsoft. "Copilot success kit – microsoft adoption", Accessed: Apr. 9, 2026. [Online]. Available: https://learn.microsoft.com/en-us/office365/servicedescriptions/office-365-platform-service-description/microsoft-365-copilot?toc=%2Fcopilot%2Fmicrosoft-365%2Ftoc.json&bc=%2Fcopilot%2Fmicrosoft-365%2Fagent-framework%2Fbread%2Ftoc.json.

[68] M. Bano, D. Zowghi, J. Whittle, L. Zhu, A. Reeson, R. Martin, and J. Parsons, *Survey insights on m365 copilot adoption*, 2024. arXiv: 2412.16162 [cs.HC]. [Online]. Available: https://arxiv.org/abs/2412.16162.

[69] M. Bano, D. Zowghi, J. Whittle, L. Zhu, A. Reeson, R. Martin, and J. Parsons, *A qualitative study of user perception of m365 ai copilot*, 2025. arXiv: 2503.17661 [cs.CY]. [Online]. Available: https://arxiv.org/abs/2503.17661.

[70] B. Erdal and M. Ibrahim, "Ai-assisterad administration i byggsektorn: En studie av microsoft 365 copilot", 2025. [Online]. Available: https://urn.kb.se/resolve?urn=urn:nbn:se:liu:diva-215446.

[71] Microsoft. "Microsoft trust center | data security, privacy, and compliance", Accessed: Dec. 11, 2025. [Online]. Available: https://www.microsoft.com/en-us/trust-center.

[72] Microsoft. "Trusted products and services | microsoft trust center", Accessed: Dec. 11, 2025. [Online]. Available: https://www.microsoft.com/en-us/trust-center/product-overview.

[73] Microsoft. "Vastuulliset tekoälyperiaatteet ja lähestymistapa | microsoft ai", Accessed: Apr. 15, 2026. [Online]. Available: https://www.microsoft.com/fi-fi/ai/principles-and-approach?msockid=3be31cda99b962db1b5a0a8398f063ed#responsible-ai-standard.

[74] Microsoft. "Secure future initiative (sfi) | microsoft trust center", Accessed: Dec. 11, 2025. [Online]. Available: https://www.microsoft.com/en-us/trust-center/security/secure-future-initiative.

[75] Microsoft. "What is zero trust? | microsoft learn", Accessed: Apr. 12, 2026. [Online]. Available: https://learn.microsoft.com/en-us/security/zero-trust/zero-trust-overview.

[76] Microsoft. "How do i apply zero trust principles to microsoft 365 copilot? | microsoft learn", Accessed: Apr. 12, 2026. [Online]. Available: https://learn.microsoft.com/en-us/security/zero-trust/copilots/zero-trust-microsoft-365-copilot.

[77] Microsoft. "Learn about microsoft purview | microsoft learn", Accessed: Apr. 12, 2026. [Online]. Available: https://learn.microsoft.com/en-us/purview/purview.

[78] Microsoft. "What is microsoft sentinel siem? | azure docs", Accessed: Apr. 12, 2026. [Online]. Available: https://docs.azure.cn/en-us/sentinel/overview.

[79] Microsoft. "Microsoft defender for endpoint - microsoft defender for endpoint | microsoft learn", Accessed: Apr. 12, 2026. [Online]. Available: https://le

arn.microsoft.com/en-us/defender-endpoint/microsoft-defender-endpoint.

[80] Microsoft. "Microsoft privacy principles | microsoft trust center", Accessed: Dec. 11, 2025. [Online]. Available: https://www.microsoft.com/en-us/trust-center/privacy.

[81] Microsoft. "What is the eu data boundary? | microsoft learn", Accessed: Nov. 6, 2025. [Online]. Available: https://learn.microsoft.com/en-us/privacy/eudb/eu-data-boundary-learn.

[82] J. Brill and P. Lorimer. "Microsoft completes landmark eu data boundary, offering enhanced data residency and transparency", Accessed: Dec. 11, 2025. [Online]. Available: https://blogs.microsoft.com/on-the-issues/2025/02/26/microsoft-completes-landmark-eu-data-boundary-offering-enhanced-data-residency-and-transparency/.

[83] Microsoft. "Compliance offerings for microsoft 365, azure, and other microsoft services. | microsoft learn", Accessed: Dec. 11, 2025. [Online]. Available: https://learn.microsoft.com/en-us/compliance/regulatory/offering-home.

[84] Microsoft. "Microsoft purview compliance manager | microsoft learn", Accessed: Apr. 19, 2026. [Online]. Available: https://learn.microsoft.com/en-us/purview/compliance-manager.

[85] Microsoft. "Microsoft purview compliance manager regulations list | microsoft learn", Accessed: Apr. 12, 2026. [Online]. Available: https://learn.microsoft.com/en-us/purview/compliance-manager-regulations-list.

[86] Microsoft. "Managing cloud compliance | microsoft trust center", Accessed: Dec. 11, 2025. [Online]. Available: https://www.microsoft.com/en-us/trust-center/compliance/compliance-overview.

[87] Microsoft. "Iso/iec 27001:2013 information security management standards - microsoft compliance | microsoft learn", Accessed: Apr. 28, 2026. [Online]. Available: https://learn.microsoft.com/en-us/compliance/regulatory/offering-iso-27001.

[88] International Organization for Standardization (ISO). "Iso/iec 42001:2023 information technology — artificial intelligence — management system", Accessed: Dec. 5, 2025. [Online]. Available: https://www.iso.org/standard/42001.

[89] Microsoft. "General data protection regulation - microsoft gdpr | microsoft learn", Accessed: Apr. 28, 2026. [Online]. Available: https://learn.microsoft.com/en-us/compliance/regulatory/gdpr.

[90] Microsoft. "Microsoft learn: Build with answers in reach", Accessed: Apr. 20, 2026. [Online]. Available: https://learn.microsoft.com/en-us/.

[91] S. K. Ahmed, R. A. Mohammed, A. J. Nashwan, R. H. Ibrahim, A. Q. Abdalla, B. M. M. Ameen, and R. M. Khdhir, "Using thematic analysis in qualitative research", *Journal of Medicine, Surgery, and Public Health*, vol. 6, p. 100 198, Aug. 2025, ISSN: 2949-916X. DOI: 10.1016/J.GLMEDI.2025.100198.

[92] Microsoft. "What is microsoft 365 copilot? | microsoft learn", Accessed: Apr. 9, 2026. [Online]. Available: https://learn.microsoft.com/en-us/microsoft-365/copilot/microsoft-365-copilot-overview.

[93] Microsoft. "Microsoft 365 copilot", Accessed: Apr. 9, 2026. [Online]. Available: https://learn.microsoft.com/en-us/office365/servicedescriptions/office-365-platform-service-description/microsoft-365-copilot?toc=%2Fcopilot%2Fmicrosoft-365%2Ftoc.json&bc=%2Fcopilot%2Fmicrosoft-365%2Fagent-framework%2Fbread%2Ftoc.json.

[94] Microsoft. "Using key performance indicators (kpis) to meet your business goals - business central | microsoft learn", Accessed: Apr. 13, 2026. [Online]. Available: https://learn.microsoft.com/en-us/dynamics365/business-central/analytics-about-kpis.

[95] Microsoft. "License options for microsoft 365 copilot | microsoft learn", Accessed: Apr. 13, 2026. [Online]. Available: https://learn.microsoft.com/en-us/microsoft-365/copilot/microsoft-365-copilot-licensing.

[96] Microsoft. "Get ready for microsoft 365 copilot with sharepoint advanced management - sharepoint in microsoft 365 | microsoft learn", Accessed: Apr. 14, 2026. [Online]. Available: https://learn.microsoft.com/en-us/SharePoint/get-ready-copilot-sharepoint-advanced-management.

[97] Microsoft. "Restrict discovery of sharepoint sites and content - sharepoint in microsoft 365 | microsoft learn", Accessed: Apr. 14, 2026. [Online]. Available: https://learn.microsoft.com/en-us/sharepoint/restricted-content-discovery.

[98] Microsoft. "Zero trust assessment overview | microsoft learn", Accessed: Apr. 15, 2026. [Online]. Available: https://learn.microsoft.com/en-us/security/zero-trust/assessment/overview.

[99] Microsoft. "What is privileged identity management? - microsoft entra id governance | microsoft learn", Accessed: Apr. 15, 2026. [Online]. Available: https://learn.microsoft.com/en-us/entra/id-governance/privileged-identity-management/pim-configure.

[100] Microsoft. "Use sensitivity labels to protect collaborative workspaces (groups and sites) | microsoft learn", Accessed: Apr. 16, 2026. [Online]. Available: https://learn.microsoft.com/en-us/purview/sensitivity-labels-teams-groups-sites.

[101] Microsoft. "Learn about investigating data loss prevention alerts | microsoft learn", Accessed: Apr. 16, 2026. [Online]. Available: https://learn.microsoft.com/en-us/purview/dlp-alert-investigation-learn.

[102] Microsoft. "Administering and governing agents | agent governance whitepaper", Accessed: Apr. 16, 2026. [Online]. Available: https://adoption.microsoft.com/files/copilot-studio/Agent-governance-whitepaper.pdf.

[103] Microsoft. "Learn about copilot prompts - microsoft support", Accessed: Apr. 16, 2026. [Online]. Available: https://support.microsoft.com/en-us/topic/learn-about-copilot-prompts-f6c3b467-f07c-4db1-ae54-ffac96184dd5.

[104] Microsoft. "Create a prompt coach agent from a template | microsoft learn", Accessed: Apr. 16, 2026. [Online]. Available: https://learn.microsoft.com/en-us/microsoft-365/copilot/extensibility/agent-template-prompt-coach.

[105] Microsoft. "Establish an ai center of excellence - cloud adoption framework | microsoft learn", Accessed: Apr. 16, 2026. [Online]. Available: https://learn.microsoft.com/en-us/azure/cloud-adoption-framework/ai/center-of-excellence.

Appendix A Qualitative study questions

This appendix presents the questionnaire that was used to validate the Microsoft 365 Copilot Implementation Model made in this thesis. The questionnaire was hosted on Microsoft Forms.

Introduction

Tämän kyselyn tarkoituksena on tarkastella ja validoida diplomityötäni (Turun Yliopisto) varten luotua Microsoft 365 Copilotin implementointimallia. Malli on kehitetty Twodaylle tarjoamaan strukturoitu ja kyberturvallisuuteen painottuva kehys Copilotin käyttöönotosta organisaatioissa, erityisesti asiakasprojekteissa. Implementointimalli on luotu tietoturvallisuus aspekti edellä, sisällyttäen adaptaatiomallit ja lainsäädöllisten regulaatioiden noudattamisen.

Kaikki vastaukset käsitellään anonyymisti ja yksittäistä vastaajaa ei pysty tunnistamaan kyselyn tuloksista. Vastaukset tullaan poistamaan tutkimuksen ja vastausten analysoinnin jälkeen pysyvästi.

Tutustu liitteenä saamaasi implementaatiomalliin ja vastaa sitten kysymyksiin. Kokonaisuudessaan tähän kuluu noin yksi tunti aikaa.

Vastaathan avokysymyksiin mahdollisimman kattavasti, välttäen yksinkertaisia "Kyllä"/"Ei" tyylisiä vastauksia.

Kiitos osallistumisesta!

//

The purpose of this survey is to review and validate the Microsoft 365 Copilot implementation model created for my master's thesis (University of Turku). The model was developed for Twoday to provide a structured framework focused on cybersecurity for the adoption of Copilot in organizations, particularly in customer projects. The implementation model was created with a particular emphasis on information security, incorporating adaptation models and compliance with legal regulations.

All responses will be treated anonymously, and individual respondents cannot be identified from the survey results. The responses will be permanently deleted after the study and analysis of the responses.

Please review the implementation model attached to this survey and then answer the questions. The entire process will take approximately one hour.

Please answer the open-ended questions as thoroughly as possible, avoiding simple "Yes" or "No" type answers.

Thank you for participating!

Basic information

1. What is your primary role and job description in your business unit? How long have you worked in this position?

2. How much hands-on experience do you have with Microsoft 365 Copilot in

your daily work or customer projects? (1 = no experience, 4 = very much experience)

3. How familiar are you with the security and compliance measures (e.g., Zero Trust, Microsoft Purview) that must be utilized when using Microsoft 365 Copilot? (1 = not familiar at all, 4 = very familiar)

4. How comfortable are you with adopting new technologies (e.g., AI tools) in your daily work? (1 = not comfortable at all, 4 = very comfortable)

5. What is the most time-consuming or repetitive task in your daily work that Copilot could assist with, or already assists with?

Measuring expectations and user behaviour

6. Based on Microsoft 365 Copilot's capabilities, how do you anticipate it will impact the speed and quality of users' daily work? Please provide examples if possible.

7. Considering the risk of *prompt anxiety* among new Copilot users, how effective do you anticipate role-specific prompt libraries and the Prompt Coach Agent will be in helping users overcome the learning curve? (1 = not effective at all, 4 = very effective)

Measuring organizational fit

8. How effectively does the *Organizational Data Audit* (Strategy phase) ensure that Copilot's output is consistent with the organization's existing data structures and values? (1 = not effective at all, 4 = very effective)

9. Expansion of Copilot usage relies on early adopters ("Copilot Champions") who support and train others. How much, and in what ways, do you estimate

early adopters will contribute to making Copilot's benefits visible during the Rollout phase?

10. The OCM preparation communication plan (Plan phase) highlights "hours saved" and "reduced administrative burden" to increase user engagement compared to manual workflows. How effectively does this strategy demonstrate Copilot's advantages over existing manual workflows?

11. How much do you anticipate that the five-phased implementation model will reduce the perceived complexity of Copilot implementation? (1 = does not reduce complexity, 4 = reduces complexity very strongly)

12. What factors influenced your answer to the previous question?

13. Is the proposed Pilot phase involving 5–30 users sufficient to validate the implementation strategy before moving to organization-wide deployment? Why or why not?

Structural readiness

14. How effectively do the Microsoft 365 Copilot Optimization and Zero Trust assessments included in the Implementation Readiness checklist address technical compatibility and the current state of a customer tenant? Why?

15. How practical is it for organizations to define clear AI usage policies to manage organizational risks associated with Copilot-generated content? Why?

16. How well does the model bridge the gap between internal operational practices and external regulatory requirements (EU AI Act and NIS2)? Are any elements missing?

Security, compliance, and regulatory requirements

17. How effectively does the principle of least privilege mitigate the risk of Copilot accessing unauthorized data? Why?

18. Users may have concerns regarding Copilot's ability to summarize files. Does the *Restricted Content Discovery* feature (Strategy phase) for SharePoint sites sufficiently address the risk of data exposure? Why or why not?

19. Is the requirement to apply Microsoft Purview sensitivity labels before activating Copilot a practical method for maintaining data boundaries? Why or why not?

20. Does the combination of an AI council and the human-in-the-loop mandate provide a robust framework for meeting the ethical and transparency requirements of the EU AI Act? Why or why not?

21. Under the NIS2 Directive, significant cybersecurity incidents must be reported to authorities within 24 hours. If you noticed Copilot accessing confidential data that it should not have access to, how capable do you feel in recognizing such an incident and reporting it within the required time frame? (1 = not capable at all, 4 = very capable)

Model validation

22. Some customers may wish to bypass certain implementation phases (e.g., organizational data review). Based on your experience with customer projects, how realistic is it to execute all five phases as defined without skipping steps?

23. What changes would you suggest to the implementation model to improve its effectiveness as a professional service offering or sales framework?

24. Do you have any additional comments or feedback regarding the implementation model or this questionnaire? (optional)

Appendix B Declaration of the Use of AI

AI tools were applied for this thesis for auxiliary tasks in accordance with the guidelines of the University of Turku. M365 Copilot chat (GPT 5.4) and Google Gemini (3.1 Pro) models were utilized for this thesis. These models were primarily used to support with wording, grammar correction, and give suggestions on improving structure of the thesis text. Questionnaire's question formulation and reviewing of responses where refined with M365 Copilot in Word and Excel. The models were secondarily used to do deep research of relevant sources related to the topics of this work (AI, Microsoft products, adoption models, relevant regulatory requirements, and cybersecurity frameworks). All sources that were ultimately referenced, were manually confirmed and verified by the author. The AI tools were not used to generate the substance of this thesis text and author is responsible for the accuracy in this thesis.