LUNDS UNIVERSITET

Ekonomihögskolan

Institutionen för informatik

Is it good enough

An analysis of Swedish universities information security requirements

Kandidatuppsats 15 hp, kurs SYSK16 i Informationssystem

Författare: Daniel Lindvall

Handledare: Blerim Emruli

Rättande lärare:

Is IT good enough: An analysis of Swedish universities information security

ENGELSK TITEL: Is IT good enough: An analysis of Swedish universities information security

FÖRFATTARE: Daniel Lindvall

UTGIVARE: Institutionen för informatik, Ekonomihögskolan, Lunds universitet

EXAMINATOR: Osama Mansour, PhD

FRAMLAGD: anuari, 2023

DOKUMENTTYP: Kandidatuppsats

ANTAL SIDOR: 64

NYCKELORD: information security policy, university, Sweden, security governance, information security management, information security awareness, institutional theory, institutional logics, general system theory, security, data breaches

SAMMANFATTNING (MAX. 200 ORD):

Previous research in information security research has pointed out the importance of aware employees, while practitioners have focused on technical safety measures, this while the geopolitical situation has rapidly changed. In this paper the public Swedish institutions of higher education are investigated to gain a more complete picture of the potential pitfalls that exist in Swedish government agencies. The study uses a mixed method approach, first a qualitative content analysis of ten Swedish institutions of higher education information security policy to identify any problem areas, further a quantitative survey was sent out to 85 IT-managers at thirty of the thirty-two Swedish institutions of higher education to investigate what issues they had observed. The findings show that information security awareness and education programs seem to have been neglected among the Swedish institutions of higher education, even though researchers have stressed their importance. The new geopolitical situation and the high return of investment on socially engineered attacks, highlights the importance of information security awareness, this before an information security crisis occurs.

Contents

Figures

Tables

1 Introduction

1.1 Problem area

The digitalization of society has come to change many of our institutions and their practices. These changes have in many cases improved the efficiency and simplified complex tasks, though it has brought with it many new external threats.

In 2021 two major information security incidents occurred in Sweden. The first and most famous one is the Kaseya incident, where the supermarket chain Coop had to close many of their supermarkets because a criminal network managed to get access and encrypt a large number of digital storage devices. The second one is the municipality of Kalix, where some external actor managed to get access and encrypt the whole system, which led to Kalix municipality having to revert to using pen and paper (Kalix.se, 2022).

The Swedish Civil Contingencies Agency (MSB) information security report for 2021 starts with bringing up the two previously mentioned, major information security incidents. These two negative incidents have brought awareness regarding information and cyber security among the Swedish population (Myndigheten för samhällsskydd och beredskap MSB, 2021). In their concluding remarks MSB draws parallels between information security and the climate crisis, this explicitly to alarm about the state of information and cyber security issues in the Swedish society (Myndigheten för samhällsskydd och beredskap MSB, 2021). What MSB hope for is that further media exposure of information and cyber security will lead to a higher ambition among nations and organizations when it comes to information security. MSB further sees citizen awareness about the potential effects of information system failures, as something positive (Myndigheten för samhällsskydd och beredskap MSB, 2021).

The Swedish National Audit Office (NAO, Riksrevisionen) have published several reports on how government agencies handle their information security, in these reports they conclude that none of the investigated governmental agencies live up to the information security regulations (Riksrevisionen, 2014). More alarming is that according to the National Audit Office, there exists a knowledge gap of how civil services have implemented their information security (Riksrevisionen, 2014). This makes it impossible to get an aggregated view of how the Swedish civil services can prevent and deal with an information security crisis.

In a follow up audit report published by NAO in 2016, the information security work at 9 different governmental agencies was scrutinized. In the report, a deeper investigation was carried out at three out of the nine investigated agencies. These three deeper analyzed agencies were the Swedish Public Employment Service (arbetsförmedlingen), Swedish Social Insurance Agency (försäkringskassan), and the Swedish Migration Agency (migrationsverket) (Riksrevisionen, 2016). The report sums up that all three of the further investigated agencies have an information security policy, but it appears as if the majority of employees are not aware of its existence, nor are they aware of what function the policy has or where to find said policy (Riksrevisionen, 2016). The awareness of what information classification is and how information classification is done in practice, is low among the employees (Riksrevisionen, 2016). The conclusion in the report is that the audited agencies have serious deficiencies when it comes to information security, none of the agencies manage to live up to the standards and the regulations regarding information security (Riksrevisionen, 2016). Further the necessary foundation regarding information security, that should have been provided by the government does not exist (Riksrevisionen, 2016).

Moreover Riksrevisonen (2016) concludes that none of the agencies are able to declare how much of their budget is spent on information and cyber security. More concerning is that the Swedish Security Service (Säkerhetspolisen) have found systematic shortcomings among the most crucial civil services when it comes to IT and information security (Riksrevisionen, 2014).

1.1.1 Who needs to report and what needs to be reported?

Since April 2016, Swedish government agencies are obliged by law to report any information security incident to the MSB (Myndigheten för samhällsskydd och beredskap MSB, 2021). Since 2017 MSB has published an annual report of the number of incidents, the severity and what type of security incidents Swedish public agencies have reported.

The year 2021 stands out as it is the first year with over 300 reported incidents, with a total of 343 security related incidents reported (Myndigheten för samhällsskydd och beredskap MSB, 2021).

This is an increase of 53 (or ~18%) reported incidents above the average of 290 per year that occurred during the period 2017 – 2020 (MSB, 2022). Out of these 343 incidents 113 were system errors and 87 were mistakes (Myndigheten för samhällsskydd och beredskap MSB, 2021).

There exist at least two possible reasons to this increase

1. The number of incidents increased.
2. The number of reports increased.

It may of course be both in conjunction.

According to MSB there is no major increase in the number of reported attacks aimed at Swedish government agencies (Myndigheten för samhällsskydd och beredskap MSB, 2021), although the number of reported incident has in fact increased in comparison with previous years. This suggests that the information security within Swedish government agencies is either in a degenerating spiral or that the tendency to report has improved.

MSB has published two documents with information security regulations that Swedish government agencies must oblige, MSBFS 2020:6 and MSBFS 2020:7. This study will investigate the former, MSBFS 2020:6, and focuses on the organizational capabilities of information security when it comes to governmental institutions.

Information security at the Swedish major educational institutions is an area that has been neglected by researchers, though NAO did several audits around the year 2010 and found severe issues at all the investigated institutions.

The closest contemporary data that is publicly accessible regarding institutions of higher education, is from the United Kingdom (UK). In the UK the Department for Digital, Culture, Media & Sport compiles a yearly report aptly named Cyber Security Breaches Survey, that contains a comparison between educational institutions and businesses.

In the survey almost 40% of the 1243 UK businesses have been able to identify a breach or attack during the last 12 months, while over 90% of the 37 higher educational colleges report that they have experienced the same (Educational Institutions Findings Annex - Cyber Security Breaches Survey 2022, 2022). Now clearly these numbers should be handled with caution since the sample size of higher education institutions are a lot fewer than the sample size of UK businesses.

Even with the highest suggested margin of error provided in the report the higher education institutions would end up at approximately 80% of the institutions experiencing attacks or breaches (Educational Institutions Findings Annex - Cyber Security Breaches Survey 2022, 2022). The higher education colleges report that 62% of them have been affected by some sort of attack at least once a week during the last 12 months, this coupled together with 71% of the higher educational institutions reporting that in the last 12 months they have had incidents with negative outcomes such as financial or data loss (Educational Institutions Findings Annex - Cyber Security Breaches Survey 2022, 2022). This indicates that higher educational institutions may be of particular interest for cyber criminals, though this may not be very controversial since they in general also have a larger funding than many other organizations. The most common attack vector in the UK in 2022, both from a business and educational perspective were phishing attacks, followed by impersonation attacks, both attacks focus on social engineering (Educational Institutions Findings Annex - Cyber Security Breaches Survey 2022, 2022).

On the 21st of December 2022 the Swedish newspaper Dagens Nyheter published an interview with Mats Persson, the Swedish minister of Education. Mats Persson says “We have been naïve. It is time for that to end, it is time for action.” this in regard to the IT-security at Swedish universities and college universities (Holmström, 2022). Persson brings up the changed security situation in the world and how certain actors have already shown an increased interest in gathering data from Swedish educational institutions (Holmström, 2022).

The new reality for information security professionals in educational institutions along with the lack of studies regarding educational institutions and information security in a Swedish context, justifies the study.

1.2 Question

From the problem area a two-fold research question has been formulated

RQ 1. To what degree does a sample size of Swedish universities follow the information security regulations provided by MSB?
RQ 2. How do information security employees at Swedish universities perceive these information security policy regulations?

1.3 Purpose

The purpose of this study is to provide researchers and practitioners with empirical data of how Swedish universities have implemented their information security programs. The intention with the study is to yield a deeper understanding of the universities regulations and policy documents, and how InfoSec perceive the information security within their institutions.

1.4 Limitations

This study will only look at hierarchical organizations within the context of Swedish universities and university colleges, this is further limited to only includes public universities.

The study will not discuss which standard the universities use, or which information security policy is better for a certain type of organization.

1.5 Disposition

This study first presents a literature review which explains three of the most common theoretical backgrounds within information security research, what research has been done prior and what is unclear within information security. The literature review also contains a segment to give the reader an understanding of the hierarchical organization structure.
The method then explains the process of how the data was collected, what was collected and how the survey was constructed.
The results contain a checklist used to control what regulations investigated universities follow. A small chapter where the structure of every organization and any interesting findings along with the survey answers and a summary of the survey.
The following discussion synthesizes the results with the literature from the literature review.
In the last chapter the conclusion is presented.

2 Literature review

2.1 Prior Information Security research within Information Systems

The purpose of information security documents, such as Information Security Policies (ISP), Cybersecurity Policies (CSP) and other information security governing documents is to protect the information of an organization.

A contemporary Scandinavian view of Information Security is that information security is a dichotomy of both technical and administrative rules, regulations, and guidelines (Siponen, 2000).

2.1.1 Organizations policy enforcement

Many information breaches have been due to organizations inability to enforce personnel to follow their ISP, this is due to

- Negligence or mistakes
- Complex or unclear ISP
- Non-compliance towards the ISP
- Contradicting business interests and ISP

(D'Arcy et al., 2014; Kajtazi et al., 2021; Hedström et al., 2011).

As the numbers of information breaches have increased, security research articles have decreased in information system journals, that may stem from a misalignment between researchers and practitioners, where researchers have focused on employee behaviours and compliance, while practitioners focus on IS security attacks (Siponen & Willison, 2007; D'Arcy et al., 2014; Dhillon et al., 2021).

Dhillon and Backhouse (2001) conducted a literature review of the security research and notes that much of the security research has been focused mainly on a technical and functionalist perspective. Within the functionalist paradigm the theories used tend to be either general systems theory or contingency theory (Dhillon & Backhouse, 2001; Klaić & Hadjina, 2011). Dhillon and Backhouse (2001) states that this functionalist way of thinking may have been useful when organizations where organized as hierarchies and contained a limited amount of processing power, but as organizations have moved towards network organizations where computers exist within all parts of an organization, these theories may not be as useful.

Aurigemma and Mattson (2019) on the other hand, notes a large portion of the research published in the basket of eight, regarding information security policies have tried to solve the problem with universal models and wishes to see a broader adaptation of contingency theory in information security research, since the universal models often are too general.

Not only are the models too general but there have been very few security models developed by researchers, security research also seems to have a knowledge gap when it comes to the social aspect of system security analysis and how organizations deal with conflicting internal interests such as efficiency versus security (Dhillon & Backhouse, 2001; Whitman et al., 2001; Siponen, 2005; Siponen, 2006; Hedström et al., 2011).

There appears to exist a lack of research regarding how ISPs are designed and implemented, how ISP compliance affects organization's security programs and how ISPs continue to evolve after it has been implemented (Cram et al., 2017).

2.1.2 The definition of what an ISP is

Another issue seems to be that the ISP lacks a clear definition of what it is, leading to confusion among information security practitioners and researchers alike (Cram et al., 2017; Paananen et al., 2020). Some scholars define the ISP as an information security governing document, that prepares an organization in case of an information breach, others as a manifesto of what organizations' want to achieve with their information security, finally some define the ISP as a document of actors and assets (Klaić & Hadjina, 2011; Chen & Li, 2014; Flowerday & Tuyikeze, 2016). In this study we will refer to the ISP definition where it is an information security governing document.

2.2 Theoretical background

2.2.1 Complex systems and General system theory

Several systematic patterns have had been successfully applied to different research subjects, examples of these patterns are the Pareto principle as it is called in economics, allometric growth in biology, in other disciplines it is known as the 80-20 rule. These generalizable laws or rules are also called isomorphisms since they show correlating properties between very different structures. This observation intrigued Ludwig von Bertalanffy to further investigate if there existed a so called "Unity of Science", as he saw concepts such as; wholeness, sum, mechanization, centralization, hierarchal order, stationary and steady states, and equifinality, as pillars of research that could be applied to several different branches of science

(Bertalanffy, 1950). This idea of isomorphic concepts being applicable to many different disciplines is usually called General System Theory (GST) (Bertalanffy, 1950).

In order to understand GST, a few of the fundamental key elements of the theory are presented and briefly explained.

1. A system consists of components or subsystems
2. Holism, where the sum of the parts is more than just the parts themselves.
3. Open and closed systems, where open system can exchange matter with the environment while closed cannot.
4. Input/Output transformation model, open systems can transform input into output.
5. Negative entropy, as closed systems become more disorganized due to increase in entropy, open systems can reorganize and thereby create negative entropy.
6. Steady state, a closed system will inevitably achieve a homeostasis, in contrast an open system can achieve a dynamic equilibrium due to a steady influx of resources.
7. Feedback is the control mechanism for a system to achieve the previously mentioned steady state.
8. Hierarchy, where a system contains components and/or subsystem.
9. Internal elaboration, while closed systems move towards entropy and disorganization, open systems move towards differentiation, elaboration, and organization.
10. Multiple goals, biological and social systems seek to achieve multiple different goals.
11. Equifinality of open systems, in a mechanical system (who per definition are closed systems) the initial conditions will affect the final state, though this does not seem to apply to open systems who instead may achieve the same results with different initial conditions.

(Kast & Rosenzweig, 1972)

Bertalanffy (1950) thought that systems could be defined as “a complex of interacting elements”. Simon (1962) on the other hand defined a complex system as a system built by multiple components interacting in a non-simplistic way, Simon explains it as:

> the whole is more than the sum of the parts, not in an ultimate, metaphysical sense, but in the important pragmatic sense that, given the properties of the parts and the laws of their inter- action, it is not a trivial matter to infer the properties of the whole (Simon, 1962).

Simon (1962) presents his hypothesis, that among many of the systems he studied, all show signs of what he terms hierarchy. As an example, an atom consists of neutrons, protons, and electrons, which in their own consists of quarks. This idea can be seen as sprung out of the philosophy of hierarchical ontologies. As the complex system is seen as more than just the sum of its parts, it is also important to note that the complex system can be decomposed into subsystems which in turn can be decomposed down to the fundamental building blocks, Boulding (1956) called these systems “systems of systems”.

In 1958 an article by J.W. Forrester, called Industrial Dynamics was published. In the article Forrester argued for the future possibilities of digital systems in the industrial sector. One of the fundamental pillars of the industrial dynamic is what Forrester calls the feedback control system which he based upon feedback theory (Forrester, 1958). A simplification of the feedback control system would be an iterative process in which there are actions and every action in the process has a reaction.

Ten years later Forrester published a retrospective in the Journal of Management Science. An important reflection Forrester had in this retrospective, is what Forrester refers to as *The Closed Boundary* (Forrester, 1968). *The Closed Boundary* is defined by Forrester as the feedback loop which begins as a closed process, where exogenous variables do not define the system, the first step of the feedback loop is to isolate the system and only later in the process, start implementing channels of communication between systems (Forrester, 1968). Forrester's theory of isolating the system and building the system components before connecting it with external systems, follows the hierarchical ontologies approach.

Another scholar with a similar theory is the late Nobel laureate Oliver Williamson, in his book Markets and Hierarchies**:** Analysis and Antitrust Implications, Williamson proposes that there may be more to economics than just the traditional markets. Williamson's theory was that there also exists hierarchies in economics, and one of the most important and fundamental hierarchy from what Williamson gathered was the trust hierarchy (Lodge et al., 2016). According to Williamson the trust hierarchy compared to the economic market tries to establish a communication medium based upon trust between two or more entities, whereas the market is purely supply and demand (Lodge et al., 2016).

The trust hierarchy is more interested in whether a supplier can be seen as a reliable source of a supply, if not, production should be done in a hierarchy, commonly referred to as internal production (Lodge et al., 2016).

In other words, if you find a market stall that sells apples at your local market at a low price that may be sufficient for you as an individual at that given point of time, but you cannot trust that the vendor will be there and sell the same variety of apples tomorrow.

If you instead are a commercial producer of apple pies, a steady stream of the same variety of apples is what is required to keep the business running, since there is a risk that your business may not be able to produce and sell apple pies, which in the end will result in financial loss. The options you are left with is either to start your own apple orchard or incorporate an apple producer into your own production cycle.

In this aspect both Forrester and Williamson agree that a balance within the system needs to be maintained, in other words the system needs to achieve a steady state, but what Williamson observed was that balance often meant an arbitrary and satisfactory state, defined by a human (Lodge et al., 2016). Williamson saw further possibilities for optimizing the performance of a system through the use of mathematics and statistics (Lodge et al., 2016).

Simon (1988) believes many complex systems are built in this system of systems form or boxes within boxes as he called it. With the ability to decompose a larger system into smaller systems who are independent from each other yet all part of the same larger system (Simon, 1988).

The introduction of computers into organizations led to electronic communication that allowed for electronic brokers and integration, Malone et al. (1987) has an interesting perspective here where the new digital landscape allowed organizations to transform from hierarchies into markets. The problem is that neither the strict hierarchical approach nor the market approach can solely explain how the modern network organizations are governed. Instead hybrid governance has been proposed, where parts of the market and hierarchy are combined together (Ebers & Oerlemans, 2016). In the networks that have been built up between institutions where data is transferred between them, hierarchical organizations would struggle to implement services provided by external actors, this due to the strict and rigorous trust that is required, as well as the seller's need to adapt to the buyer. On the other hand, in a market setting, the trust between the buyer and seller would be low, and the control over the data would be placed at the seller, not the buyer. One proposed theory to explain the hybrid governance phenomena is institutional theory (Ebers & Oerlemans, 2016).

2.2.2 Institutional theory

Institutional theory is concerned with how institutions emerge, how they evolve over time, and how they come to exert a powerful influence on the behaviour of individuals and organizations. Moreover, it is also concerned with how institutions can be changed or challenged, and the consequences of these changes for individuals and organizations.

Dimaggio and Powell (1983) state that a full bureaucratization of corporations has been completed, this bureaucratization is a so-called top-down approach has been adopted to raise organizational efficiency and to handle the external stress from competitors. Yet even though bureaucracy had managed to homogenize and improve the efficiency, the process of organizational homogenization had not stopped. This contradicted the contemporary organizational theory which at that time claimed a vast amount of heterogenization among organizations (Dimaggio & Powell, 1983).

This lead Dimaggio and Powell (1983) to propose isomorphism as a reason to explain their observations. Institutional isomorphism tries to explain how institutions converge on similar structures, practices, and norms. According to Dimaggio and Powell (1983) this can happen through three isomorphic processes

1. Coercive isomorphism is how actors force one institution to adapt certain rules or behavior.
2. Mimetic isomorphism where one organization tries to mimic a successful organization.
3. Normative isomorphism where a particular behavior is expected of the institution, in other words there exists a norm.

(Dimaggio & Powell, 1983).

In the field of information security, institutional theory has seen limited use, though the application of the theory has been successful. As an example, in New Zealand 59 government agencies were investigated to find the beneficial factors, when a national information security standard was adopted, the findings showed that resource allocation, managerial support and participation were important success factors (Smith et al., 2010).

Further two different types of institutional pressures have been identified, internal and external. Where the external manifest itself in the form of normative and coercive isomorphism, while the internal stemmed from two different streams, one top down perspective and one bottoms up perspective, that intertwine (Hu, Hart & Cooke, 2007).

2.2.3 Institutional logics

Institutional logics, builds upon institutional theory and refers to the introduction of new ideas, practices, or values that challenge and ultimately reshape existing institutions. These new ideas can come from a variety of sources, including societal changes, technological innovations, or the actions of individual actors within institutions, similar to coercive isomorphism. Where institutional logics differs from institutional theory is while the latter looks at the influence one stream of stress has on an organization, the former acknowledges that many conflicting sources of stress collide and develop new logics for the organization (Lounsbury & Boxenbaum, 2013). Executives may be interested in information security to protect data, as the data has a financial value, while the individual consumer instead may wish to protect their privacy, both logics yield the same outcome, but with completely different underlying motivations. Institutional logics posit three underlying mechanisms to which the organization adopts to, legitimacy, politics and assumptions (Thornton & Ocasio, 1999). Legitimacy is based upon the legitimacy of the actor, meaning that a chief officer may be perceived as a person with more legitimacy than an operative, because of their position of power. Politics are the perceived difficulties that the organization focus on solving or adopting to, an example of a political logic is the choice to become an environmentally friendly organization. Assumptions are derivatives of the overall strategies, in other words what the agents in the organization perceive needs to be done to achieve the goal of the strategies.

Thornton and Ocasio (1999) defined institutional logics as "the socially constructed, historical pattern of material practices, assumptions, values, beliefs, and rules by which individuals produce and reproduce their material subsistence, organize time and space, and provide meaning to their social reality", meaning that individuals themselves interpret their own reality and apply their interpretation to the practices and regulations within an institution. This leads to organization's institutional logics rapidly changing as new agents are added to the organization, or old one leaves or change position in the organization.

2.2.4 General deterrence theory

Another proposed theory that may explain the behavior of individuals and organizations is General Deterrence Theory (GDT). A theory that was originally proposed to explain criminal behavior (Siponen et al., 2022), deterrence theory is based upon the idea that actors are rational and will weigh the potential costs and benefits of their actions before deciding the most beneficial outcome (Moody, Siponen & Pahnila, 2018). In the context of information security, deterrence theory state that people will consider the potential consequences of engaging in malicious activities and thereby deter from committing a violation if the punishments outweigh the potential gains. The goal of deterrence is to create a so-called deterrent effect, a psychological effect that influences both employees, other actors in the system as well as malicious actors, by making them less likely to engage in activities that they know will be punished (Chen, Ramamurthy & Wen, 2012).

In previous research, deterrence theory seems to be successful for organizations who state examples of what happens when employees break the information security policy (Chen, Ramamurthy & Wen, 2012; Moody, Siponen & Pahnila, 2018), but Chen, Ramamurthy and Wen (2012) also note that this is a highly debated topic within information system security. Moreover moderate breaches against the information security policy may be mitigated with rewards, though this does not seem to be the case for severe breaches (Chen, Ramamurthy & Wen, 2012). On the other side of the coin too harsh punishments may lead to employees reacting negatively towards an organization's information security rules and additionally, it is important to have a strong and effective system for detecting and responding to cybercrime or other malicious activities (Moody, Siponen & Pahnila, 2018). This can include things like intrusion detection systems, firewalls, and other security technologies that can help to identify and prevent attacks. It can also include things like incident response plans, which outline the steps that should be taken in the event of a cyber attack. Though an overabundance of security processes and software may hamper employees productivity (Moody, Siponen & Pahnila, 2018).

Deterrence theory in information security is a strategy that is based on the idea that the threat of punishment can prevent individuals or organizations from engaging in dubious and/or malicious activities. By increasing the perceived costs of engaging in these activities, it is possible to create a deterrent effect that will help to keep individuals and organizations safe from harm.

2.2.5 The deterrence security model development

As mentioned earlier deterrence theory has been a fundamental part of several frameworks to deter individuals to stray from organizations policies. One pillar of the deterrence theory within information security has been the deterrence security model, which has iteratively been developed to deal with policy noncompliance.

Straub and Welke (1998) suggests that organizations implement a security model based upon deterrence theory to manage risks. The first part of Straub and Welke's model is to implement a deterrence feedback loop to deter, prevent, detect, and remedy abuse.

The second part is to implement an iterative security process with five phases.

1. Identify security problems or needs.
2. Preform a risk analysis, where threats are identified and prioritized.
3. Create new or alternative solutions.
4. Map solutions to the threat (countermeasures).
5. Incorporate the new solutions into the production lifecycle.

(Straub & Welke, 1998)

Baskerville (1993) studied and identified three generations of IS security design methods.

Briefly explained, the first generation of IS security design is a compiled list of checks for components and from there the best component is selected. The second generation expands the first generation with more sophisticated methods, incorporating functional requirements in a bottoms-up approach. The third generation tries to integrate security design into the general IS development life cycle.

Baskerville (1993) recommends organizations to implement a countermeasure matrix, containing security breaches and appropriate remedies.

Baskerville (1993) observed that organizations strive towards implementing the third generation of IS security design but lack the means to implement them.

Siponen (2005) expands Baskerville's three generations of security research into five, where the fourth generation includes involvement of the user and responsibility into the security model and the future fifth generation would incorporate responsibility and participation into practice. Which according to Siponen (2005) would reduce the need of deterrence and sanctions.

2.3 Further development of information security countermeasures

According to D'Arcy et al. (2009) the three countermeasures an organization can use to deter employee misuse of an IS are “Security, Education, Training, Awareness” (SETA) initiatives, security policy awareness and monitoring of IT resources.

2.3.1 Security, Education, Training, Awareness

SETA stems from the idea of GDT, where education, training and awareness is thought to remind users that any violation against the ISP is unlikely to go undetected and will be punished (D'Arcy et al., 2009).

Puhakainen and Siponen (2010) did an empirical study in Finland and noted that inclusion of the end-user in the development of information security processes and information security education had positive effects on the willingness to adhere to the ISP. Another interesting finding Siponen and Puhakainen (2010) did was that continuous IS security policy compliance communication is needed to maximize the user’s ISP compliance.

2.3.2 Security policy awareness

Bulgurcu et al. (2010) developed the Information Security Awareness model, consisting of ISP awareness and information security awareness and noted that this had a positive influence on the IS user complying with the ISP. Puhakainen and Siponen (2010) found that if there existed an information security champion at the executive level of the organization, it had a positive impact on the users to follow the ISP.

3 Method

3.1 Choice of method

Initially a sequential multimethod approach to gain deeper understanding of the research question was proposed. The study would stand on two qualitative strands to yield a sufficient answer to the research question. Though it quickly became apparent that the collection of empirical data in the form of qualitative interviews would become quite difficult. First because of a reluctance among potential respondents to participate, moreover it would also cause issues with the lack of validity, since a small sample of semi-structured interviews with staff from a few select universities would yield very little generalizable data. A qualitative multimethod approach would not be able to generate any generalizable data to the other universities in Sweden. Another issue that arose with a qualitative inquiry and the limited time scope is convenience sampling, while convenience sampling may seem tempting it is also frowned upon as it may introduce bias and may lead researchers to collect data just for the sake of data collection instead of purposeful data collection (Patton, 2014).

As noted previously, the use of a multimethod research approach seems to be insufficient when it comes to the proposed research questions. Particularly because of the lack of validity that a multimethod approach would yield in this case. Instead, a sequential mixed method research approach seemed to fit the research question better. The mixed method approach has been praised by many IS scholars as an important tool for researchers (Ågerfalk, 2013; Tashakkori & Creswell, 2007a, 2007b).

Several enrichments have been gained through using a mixed method approach in this study, and they should be highlighted.
First, the complimentary aspect. A sequential qualitative > quantitative mixed method allowed for an initial probing, using a qualitative analysis of universities information security policies. This analysis yielded great insights into what universities often neglected in their policies.

Secondly a mixed method research approach is an invaluable tool when it comes to compare what the regulations state should be done, and what employees observe is done, thereby providing a fuller and more diverse picture between practice and theory.

A thematic content analysis was chosen as the initial approach, the coding was done with MSBFS 2020:6 as the fundament. The advantages of a content analysis for this study are that it is a transparent and flexible method (Bryman, 2016). According to Bryman (2016) content analysis is useful when dealing with unstructured text, as is the case with various policy documents.

According to Oates et al. (2022) there are two different approaches to do a content analysis when it comes to documents. In the first approach you see the document as a vessel, which means that you see the document as carrier of information, this information is then used for analysis. In the second approach you see the documents as objects and can analyze their life span through metadata and how they are transferred within an organization (Oates et al., 2022). In this study, the documents will be used as vessels, as they contain the requirements, regulations, and guidelines.

When it comes to content analysis, where documents are used as vessels there exists a quantitative approach that for example can be used to analyze how many times a specific word occurs (Oates et al., 2022). There also exists a thematic approach, which is qualitative and that can be used to analyze the different topics within a selection of a document (Oates et al., 2022). In this case the latter was chosen to find out if the corresponding MSBFS 2020:6 regulations were contained within the universities ISP document.

The disadvantages with content analysis are that the quality of the content analysis is related to the quality and credibility of the document, further the coder must also interpret what the author intended (Bryman, 2016).
As the documents used for the analysis are the current documents used by the organizations the credibility is high, though it should be noted that much of the data in these documents is based upon the coder’s interpretation of both the original MSBFS 2020:6, from which the criteria were constructed and corresponding text in the documents gathered from the universities.

3.2 Qualitative data collection

A list of universities in Sweden was collected from Universitetskanslersämbetet (2022), only educational institutions under the category university or university college were selected, out of these 32 institutions, the Swedish Defence University (FHS) and the Swedish school of sport and health sciences (GIH) were excluded. FHS was excluded because of the heavy influence from the Swedish Armed Forces, even though it is a public university it is also a military university which makes it unique in a Swedish university context. Based upon the uniqueness of the university, the choice was made to exclude it from the potential list of samples. GIH on the other hand did an update of their website which made it unavailable during the time the data was collected.

A simple computer program was written in the programming language R, to choose 10 random universities from the list for further analysis. The program was written to prevent any potential bias in the selection of investigated institutions, the code required to replicate the selection process can be found in Appendix 3. From here each of the universities' public website was scrutinized, this included using the search function if the website had one. If no document was found on the website, a google search was done, containing the [university name] + information security guidelines, this was made in both Swedish and English. The data collection only searched for documents that were publicly available which limited the amount of data available.

3.2.1 Checklist

An initial checklist was developed to be able to compare the different university policies and requirements, the checklist is based upon the MSBFS 2020:6 Information security regulations for government agencies. This to gain an initial understanding of what parts of the ISP development was neglected. This checklist was used to evaluate each of the 10 universities

1. Yearly security follow up
2. Information continuity
    - 2.1. Identify needs
    - 2.2. Practice
3. Incidents and deviations
    - 3.1. Assess and discover
    - 3.2. Recover manipulated or lost data
    - 3.3. Assess if report is needed
4. Protection
    - 4.1. Prevent trespassing
    - 4.2. Technical alarm solutions
    - 4.3. Separation of physical zones
5. Personnel
    - 5.1. Background checks dependent on access level
    - 5.2. Inform about rules, regulations, work method and support
    - 5.3. Make sure Information security employees have sufficient competence
    - 5.4. Develop education programs, initiatives regarding Information security
6. External actor (EA)
    - 6.1. Other government actor
    - 6.1.1. Document which actor is responsible for what
    - 6.2. Other EA
    - 6.2.1. Understand and handle the risks involved in transfer of information

6.2.2. Have an agreement with requirements EA needs to follow
6.2.3. Have a plan to follow up EA follows requirements

7. Information classification
    7.1. Confidentiality, Integrity, Availability (CIA)
    7.2. Risk assessment
    7.3. Countermeasures
    7.4. Evaluate countermeasures and adapt

3.3 Quantitative data collection

The quantitative data was collected through an online survey. A link to the survey was emailed out, together with a short presentation and some general information about what the survey was about. The email also contained a short summary of the Swedish Research Councils ethical guidelines along with a link to the newest version of the Swedish Research Councils ethical guidelines, the ethical and moral implications of the study will be further discussed under 3.4 and 3.7. The email also encouraged the recipient to forward the email to colleagues within their department or organization that had information security policy work experience.

3.3.1 Sampling

The sampling used a mixed sampling strategy. First a purposive sampling (Oates et al. 2022, p. 103; Patton, 2014) was done, where the respondents were selected based upon their role in the university. The initial sample used data gathered from the previously compiled list of 30 Swedish universities and university colleges. With this list each individual university's website was visited and from each of them the public information and email addresses to managers within the IT-department was collected. One issue that arose was the plethora of different titles and roles that does exist in a modern IT infrastructure, along with the Swedish quite undescriptive naming conventions of titles within IT. This led to a focus on identifying the individuals at top managerial positions, contact them, and have them relay the survey to their subordinates, a so-called snowball sampling (Oates et al. 2022, p. 104). A total of 84 different individuals were identified with a managerial position such as Chief Digital Officer, Chief Information Officer, Chief Technical Officer, Data Protection Officer or equivalent.

3.3.2 Responses

Out of the 84 emailed individuals, two responded that they had forwarded the email to everyone who worked with information security within their organization.

One person responded that they were not in the target group.

One person responded with two questions, the first one where they wanted additional information regarding the purpose of the survey and second why section 5 in the survey would be excluded.

Further two autogenerated emails were received. One that stated that the person was no longer an employee at the institution, and the second one was on leave and that any questions should be emailed to the deputy [role]. The deputy was emailed with the same information and link and added to the list of emailed individuals.

3.3.3 Follow up email

Two reminders were emailed out, the first reminder was sent out one week after the initial email, the second one was emailed six days after the first reminder.

3.4 Survey construction

The initial survey contained 5 different sections, the different sections contained several closed questions and always ended with an open question, this to give the respondent the possibility to provide feedback on the questions, or if they wished to provide any additionally comments to what they had answered in the closed questions.

The first section contained two non-mandatory questions regarding the survey participants experience, which was measured in years and their title. This to give credibility to their survey and their participation. The participant also had the possibility to leave additional information if they so wished. The choice to make this section non mandatory was purely out of ethical considerations, and to allow full anonymity of the respondent. After considerations a better design would probably be to put this as the last section, this would allow respondents to take a more active role.

The second section focused upon the participants organization and how the information security affected the internal processes, whether other actors within the organization adhere to the information security policy or not. All in all, the second section contained 12 inquiries to begin with. At the end there was a text field that allowed participants to leave additional comments.

The third section was compiled of 16 questions of how the participant perceived that their organization’s work with the regulations provided by MSB, regarding information security. It should be noted that the first 15 questions are closely related to the 15 regulations provided by MSB, and the last question in the third section was a text field that allowed participants to write any additional comments.

The fourth section contains a total of 5 questions regarding the participant’s own view on the regulations. This section’s questions focused on if they believed that there are too many or too few regulations specified by MSB. If the regulations could be used as a fundament to further develop the information security processes or if the regulations have caused issues or hampered the organization when it came to their information security work. In the end there was a text field that allowed the participant to leave additional information or feedback.

The fifth and last section contained one question, and it was if the participant was interested in doing an interview and if so, they could fill in their contact details.

Oates et al. (2022) state that closed questions often can be criticized because there exists a potential in introducing bias with how the questions is formulated, and that survey respondents may not thoroughly think through their answer when provided with a limited number of answers. To counteract the introduction of potential bias, the initial version was emailed as a pilot study, to two different individuals, both with a PhD degree in information systems. One of them focus on security policy research, information security and noncompliance. The other one has a broader and interdisciplinary research field, this meant the first one could give expert feedback while the other could identify ambiguous, vague, or otherwise unclear questions as well as give feedback on for example the structure and the time required to complete the survey. The feedback provided in the pilot was very valuable, some minor spelling mistakes and changes were made, and a new question was added to the first section that allowed a respondent to select their different areas of expertise. To further deter bias and allow respondents to voice their opinions the last open survey item existed in all the sections except in section 5. The use of a pilot helps ensure the validity of a questionnaire (Oates et al., 2022, p. 236). Moreover Oates et al. (2022, p. 239) points out four disadvantages with surveys

1. Predefined answers may cause frustration and bias for the respondent.
2. Difficult to check disparity between answers as well as the truthfulness for the researcher
3. Researcher cannot correct misunderstandings, ask for more developed answers or provide the respondent with more information
4. Self-administered questionnaires may impose the respondent to have a high level of literacy and digital competency.

The first one has been addressed using an open survey question at the end of each section, this may not be the optimal solution, but the issue has been taken into consideration when designing the survey.

With the survey targeting a very specific group, and the sampling reducing the number of respondents, the potential of untruthful answers is reduced, though it does not eliminate the risks of untruthful answers.

With the use of a pilot, any potential misunderstandings have been reduced, this has been pointed out by Oates et al. (2022, p. 236) as well, though note that all potential misunderstandings are not eliminated.

With the target group being information security professionals and the survey used email as the channel through which it propagated, the criteria of digital competency should be eliminated, one potential issue though is the use of English in the survey, where participants may struggle. One potential solution here would be to translate the survey and have two different surveys, one in Swedish and one in English which in the end could be merged.

Below is a table of how every survey question relates to the different theories previously presented and how respondents were allowed to provide their answers.

Table 1 Survey

Question	Form type	Purpose/Theoretical background
Work title	Text field	Credibility
Years of work experience with information security	Radio button	Credibility
I work with	Checkbox	Credibility
Other information you wish to share	Text area	Credibility
I believe the department(s) that work with information security receive the resources they need within my organization	Radio button	Institutional theory (Smith et al., 2010)

I believe that executives are aware of the importance of information security within my organization	Radio button	Institutional theory (Smith et al., 2010)
I feel that I get the support I need from executives within my organization when it comes to work regarding the organization's information security policy	Radio button	Institutional theory (Smith et al., 2010; Puhakainen & Siponen 2010)
I believe that actors within my organization's information system(s) are aware of the organization's information security policy	Radio button	Institutional theory (Hu, Hart & Cooke, 2007)
I believe that disciplinary measures reduce misuse of my organization's information systems	Radio button	Deterrence theory
I believe that actors in my organization can follow the information security policy without experiencing any problems in their daily work routine	Radio button	Deterrence theory, Institutional logics
I believe that other departments within my organization understand the importance of the work my department does when it comes to information security	Radio button	Institutional theory (Hu, Hart & Cooke, 2007)
My department have the cross-functional capabilities to support other departments in their information security work	Radio button	Institutional theory
My department find it easy to recruit new competence	Radio button	Institutional logics (Thornton & Ocasio, 1999)
I feel that other departments within my organization appreciate the work my department does regarding information security	Radio button	Institutional theory (Hu, Hart & Cooke, 2007)
I trust the other departments in my organization to follow the information security policies	Radio button	Institutional theory (Hu, Hart & Cooke, 2007)
I believe my organization can implement changes in policies in a timely fashion	Radio button	General system theory
I believe the information security awareness within my organization is	Radio button	Awareness/Deterrence theory
I believe more security awareness is needed within my organization	Radio button	Awareness/Deterrence theory (Puhakainen & Siponen, 2010)
I believe that the information security work focuses on proactive measures	Radio button	General system theory

I believe that the information security work focuses on reactive measures	Radio button	General system theory
Additional comments	Text area	Credibility
My organization works systematically and risk based according to the ISO standards SS-EN ISO/IEC 27001:2017 and SS-EN ISO/IEC 27002:2017 or similar guidelines	Radio button	MSB Regulation
My organization's information security policy presents our information security strategy clearly	Radio button	MSB Regulation
My organization actively classifies information, based on Confidentiality, Integrity and Availability (CIA)	Radio button	MSB Regulation
My organization conduct follow up risk analysis, regarding information shared with external partners on a basis I find satisfactory	Radio button	MSB Regulation
My organization's internal work regarding information security education and awareness is satisfactory	Radio button	MSB Regulation
My organization's work regarding information security competence of external partners is satisfactory	Radio button	MSB Regulation
My organization continuously work to identify and assess potential physical security breaches (e.g. unauthorized access to server rooms)	Radio button	MSB Regulation
How often does your organization conduct information security follow ups?	Radio button	MSB Regulation
I believe the number of information security follow ups within my organisation are	Radio button	MSB Regulation
My organization's external threat analysis, is satisfactory regarding our information systems	Radio button	MSB Regulation
My organization's knowledge of what hardware and software exist in out information system(s) is	Radio button	MSB Regulation
My organization's competence regarding cyber security is	Radio button	MSB Regulation
My organization have satisfactory processes regarding back ups	Radio button	MSB Regulation
My organization quickly identifies information breaches.	Radio button	MSB Regulation
I believe my organization lives up to all of the regulations specified in MSBFS 2020:6	Radio button	MSB Regulation

To implement the regulations in MSBFS 2020:6 my organization had to do	Radio button	Institutional theory
Additional comments 2	Text area	Credibility
I believe following the regulations in MSBFS 2020:6 provides adequate security regarding information	Radio button	Institutional theory
I believe MSBFS 2020:6 supports my organization in developing new measures regarding information security	Radio button	General system theory
I believe the regulations in MSBFS 2020:6 are redundant for my organization	Radio button	General system theory
I believe that the number of regulations in MSBFS 2020:6 needs to be	Radio button	Institutional theory
I believe the regulations in MSBFS 2020:6 affected my organization's information security work	Radio button	Institutional theory
Additional comments 3	Text area	Credibility
Contact details	Text area	-

3.5 Collection and selection of academic literature

A large amount of literature was collected through google scholar and Lund University Library search (LUBsearch) using the search terms provided in the matrix in figure 3.1, the compiled list was reduced using LUBsearch’s possibility to only search for peer reviewed articles and articles published in the *basket of 8*.

Cyber	Information	System
Security	Governance	Risk
Policy	Managment	Requirements

Figure 3.1 search word matrix

The articles’ abstracts were read to see if they had any relevance to the research questions, if they did a thorough read through of the article’s full text was done. If the full text did not contain anything related to the subject it was excluded.

The remaining articles were then controlled against the Field Weighted Citation Impact (FWCI) score provided by Scopus, a FWCI score above 2 was needed in this first selection.

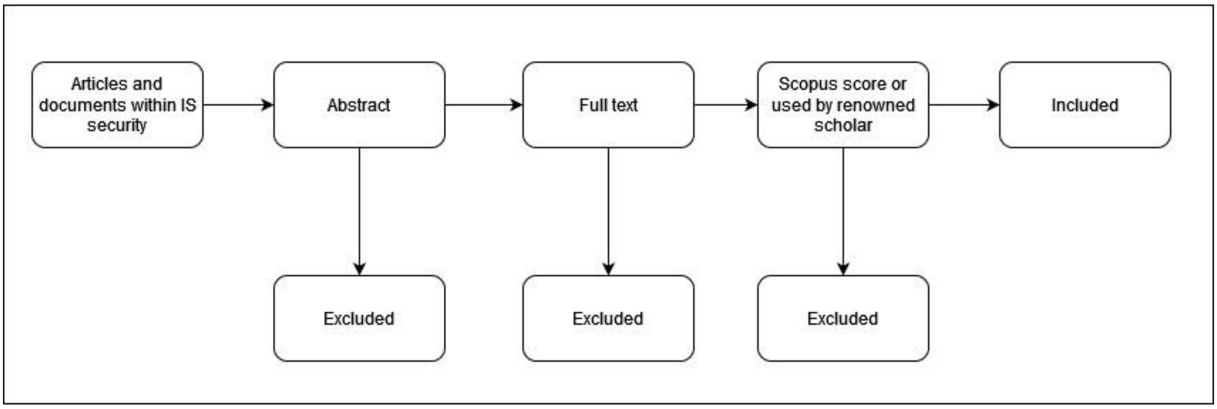

Articles and documents within IS security
Abstract
Full text
Scopus score or used by renowned scholar
Included
Excluded
Excluded
Excluded

Figure 3.2 selection process

From the articles that passed the first selection more documents were compiled into a new list that went through the same process, here the Scopus FWCI score was not deemed as important as the articles were used by renowned scholars within the field of IS security research.

3.6 Collection and selection of non-academic literature

A large part of the non-academic literature comes from government organizations and agencies within Sweden, who by law needs to live up to criteria such as availability, reliability and confidentiality which gives it credibility.

3.7 Ethical considerations

Within the thematic content analysis, the documents are freely distributed by the universities. One of the strengths with content analysis is that documents often do require less ethical considerations (Oates et al., 2022), as the documents are openly available.

As previously mentioned the Swedish Research Council (2017) ethical considerations were provided in the initial email, the survey also provided the respondent the opportunity of full anonymity, due to the fact no personal data was mandatory to provide. Oates et al. (2022) suggest the use of a webform to allow for full anonymity, further the only section that contained personal data is section 5 which will be excluded from the results, this to provide the respondents with full anonymity.

3.8 Validity

As the author has taken a clear interpretive approach to the study along with the limited number of survey respondents the external validity of the study is low, this is further impacted by the very limited scope of the study. With this said the sample group instead provides high trustworthiness and credibility, which is important for interpretivist research (Oates et al. 2022, p. 303). With the high credibility and trustworthiness that both the qualitative and quantitative parts have, this provides some internal validity as this investigates the ‘reality’ of information security employees at Swedish universities and university colleges. Further the use of having two PhD evaluate the survey further increases the validity of the survey.

3.9 Reliability

To statistically gain reliability from the survey the Cronbach’s α was used, Cronbach’s α is the most commonly used algorithm to determine reliability (Tavakol & Dennick, 2011). The approach to provide this statistical reliability was to use excel along with the add-in called Analysis ToolPak, which is used for data analysis. The scale used to calculate the sum follows

1. Strongly disagree
2. Disagree
3. Neutral/No opinion
4. Agree
5. Strongly agree

One of the answers included the answer “Unfortunately not all departments.”, this in regard to the item “My organization works systematically and risk based according to the ISO standards SS-EN ISO/IEC 27001:2017 and SS-EN ISO/IEC 27002:2017 or similar guidelines”, this answer was interpreted as the respondent disagreeing with the statement being applicable on all departments of the organization. Several of the items were problematic as the same scale was not consistently used. Further some questions also contained no quantifiable data, such as the additional comments where respondents freely could provide additional input as well as the fields where respondents could specify their title and ISP assignments, because of this they were left out of the analysis.

Table 2 Cronbach's α

Anova: Two-Factor Without Replication

SUMMARY	*Count*	*Sum*	*Average*	*Variance*
Row 1	30	95	3,166667	0,41954
Row 2	30	106	3,533333	0,878161
Row 3	30	77	2,566667	1,012644
Row 4	30	89	2,966667	0,929885
Row 5	30	100	3,333333	1,057471
Row 6	30	92	3,066667	0,891954
Row 7	30	92	3,066667	0,409195
Row 8	30	98	3,266667	0,754023
Column 1	8	18	2,25	0,5
Column 2	8	24	3	1,142857
Column 3	8	27	3,375	0,267857
Column 4	8	21	2,625	0,839286
Column 5	8	20	2,5	0,285714
Column 6	8	26	3,25	0,5
Column 7	8	23	2,875	1,553571
Column 8	8	28	3,5	1,714286
Column 9	8	17	2,125	0,410714
Column 10	8	27	3,375	1,125
Column 11	8	24	3	0,571429
Column 12	8	28	3,5	0,857143
Column 13	8	21	2,625	0,839286
Column 14	8	33	4,125	0,410714
Column 15	8	24	3	0,857143
Column 16	8	30	3,75	0,214286
Column 17	8	28	3,5	0,857143
Column 18	8	31	3,875	0,696429
Column 19	8	26	3,25	1,071429
Column 20	8	20	2,5	0,571429
Column 21	8	23	2,875	0,696429
Column 22	8	22	2,75	0,785714
Column 23	8	26	3,25	0,785714
Column 24	8	22	2,75	0,214286
Column 25	8	28	3,5	0,571429
Column 26	8	27	3,375	0,839286
Column 27	8	25	3,125	0,410714
Column 28	8	29	3,625	0,553571
Column 29	8	28	3,5	0,285714

Column 30	8	23	2,875	0,696429

ANOVA

Source of Variation	*SS*	*df*	*MS*	*F*	*P-value*	*F crit*
Rows	17,2625	7	2,466071	3,832807	0,000617	2,054908
Columns	53,62083	29	1,848994	2,873736	7,7E-06	1,523493
Error	130,6125	203	0,643411			
Total	201,4958	239				

Cronbach alpha	0,739095

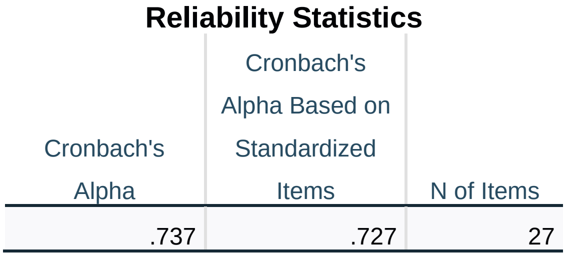
Overall, a Cronbach’s α of ~0,74 is seen as low but acceptable.

Several different levels of α have been suggested for different types of research, the majority of them range from between 0,7 up to 0,9 (Peterson, 1994). Peterson (1994) studied published scientific articles and found that among the 4286 α-coefficients investigated the mean value was 0,77 among published papers.

0,9 has been suggested as a maximum value of α, as values above 0,9 may indicate that there exist redundancies in the questionnaire (Tavakol & Dennick, 2011).

IBM SPSS was also used to calculate the Cronbach’s α, here the number of items were reduced to 27 items.

Table 3 SPSS Cronbach's α



Reliability Statistics

Cronbach's Alpha	Cronbach's Alpha Based on Standardized Items	N of Items
.737	.727	27

The reduction of items was because of design flaws that existed in the survey and difficulties of converting strings to integers, though the Cronbach’s α is still above 0,7 and close to the previously calculated α, this is in accordance with a reduction in the number questions yielding a lower α and increasing the number of questions increasing the α.

When it comes to the reliability of the content analysis the material that was selected has been analyzed twice, the weakness here stems from the same person interpreting the documents twice, although this was done sequentially. The second analysis was done 12 days after the initial analysis. No major updates in any of the documents were done during this period and the analysis provided the same result. Given the same documents and the same checklist to evaluate the documents with should result in a high reliability regarding the content analysis.

4 Results

A spreadsheet that contains each analyzed document's URL can be found in Appendix 2.

A complete table of the collected data from the content analysis can be found in Appendix 1.

4.1 Uppsala university (UU)

Uppsala university's information security management system is spread over several different documents.

The principal is responsible for the general security at Uppsala university.

The Chief of Security is responsible to coordinate security work and support the head of department or similar with the security.

The head of department or similar has the responsibility for security at the respective department.

The administrative director (intendent) is then responsible to support the head of department within their administrative area.

Every employee is responsible to help improve the security and to report any security vulnerabilities they encounter.

With the information found, UU does not live up to all the requirements in the checklist, since they lack two things; education and information of how often the security system guidelines should be revised and updated.

There seems to exist an initiative to educate personnel in information security, but no document that mentions this was found.

4.2 Lund university (LU)

Lund university does have an information security guideline document from 2017.

According to the information security guideline document at Lund university the principal is responsible for the executive decisions of how information security development should be conducted.

An IT-coordination team (SamIT) is responsible for handling general questions regarding acquisition, maintenance and dismantling IT resources.

Chief Information Security Officer is responsible that the organization lives up to the ISP and support system owners with security analysis of their systems.

The system owner is responsible that the system lives up to the requirements and has several subordinate roles that helps the system owner in managing the system.

Even though Lunds university has an older requirement document, it contains all the requirements listed in the checklist.

4.3 Linnéuniversitet (LNU)

Responsibility is delegated downstream.

LNU's information security requirement document contains all the requirements listed in the the checklist.

4.4 Gothenburg university (GU)

GU has several different roles

1. Principal is responsible for the general IT-security, responsibility follows the hierarchy downstream.
2. An *IT-maintainer* is nominated by the principal, who is responsible for the IT maintenance and security.
3. Each head of department is then responsible to nominate an *IT-maintainer* responsible for their department.

GU's requirement document contains very strict procedures but lacks information regarding how often the security documents should be revised and does not mention information security education among employees, based on the information found GU does not live up to all the criteria provided by the checklist.

4.5 Örebro University (ORU)

No public documents found.

4.6 Luleå university of Technology (LTU)

At LTU an ISP was found but no document that contain guidelines or requirements.

According to the ISP the principal of LTU is responsible for the agency and that the head of the different departments are responsible for the information security at their departments. The head of the department is also responsible to make sure all personnel at the department is aware of their responsibilities before they are allowed to use any of LTU's information systems.

As no guideline or requirement document was found it is difficult to evaluate whether LTU has an ISP that lives up to MSB's regulations.

4.7 Umeå university (UMU)

Under the principal there is a deputy who is responsible for the coordination of the information security at UMU. The principal designates an information security group that assists the deputy with information security. The deputy can delegate their role as responsible of information security to others.

The deputy or whoever is responsible for information security has the responsibility to plan, coordinate, follow up and control all the information security.

The information security group needs to contain representatives from IT-security, physical security, research, education, and administration. The principal is allowed to add representatives from other departments if it is deemed necessary.

The head of department or similar is responsible for planning, coordinating, follow up and control that the department does not violate the information security regulations.

UMU works with a Plan, Do, Check, Act cycle when it comes to information security.

UMU ISP contains all the selected touch points listed in MSBFS 2020:6.

4.8 Mid Sweden university (MIUN)

The information security at MIUN follows the whole organization, from executive level to operative.

At MIUN the department of infrastructure (INFRA) leads the information security work, they are responsible for decisions regarding guidelines, routines, and processes. INFRA are also tasked with supporting all the roles involved with strategic, tactical, and operative questions about information security.

INFRA reports their work with information security multiple times per year.

MIUN lives up to all the requirements in the checklist.

4.9 Karlstad university (KAU)

The guidelines and regulations found at KAU was directed at students for KAU and contained very little information about how KAU works with information security.

4.10 Malmö university (MAU)

The principal of MAU is responsible for the general security.

MAU has a Chief Information Officer (CIO) who is responsible for the IT-support.

System owners are responsible for their systems, except if a certain part of the system has been outsourced. The system owners have system maintainers that support them to maintain the system.

The CISO is responsible for the operative work regarding information security and is responsible for revisions of the information security rules and regulations when needed.

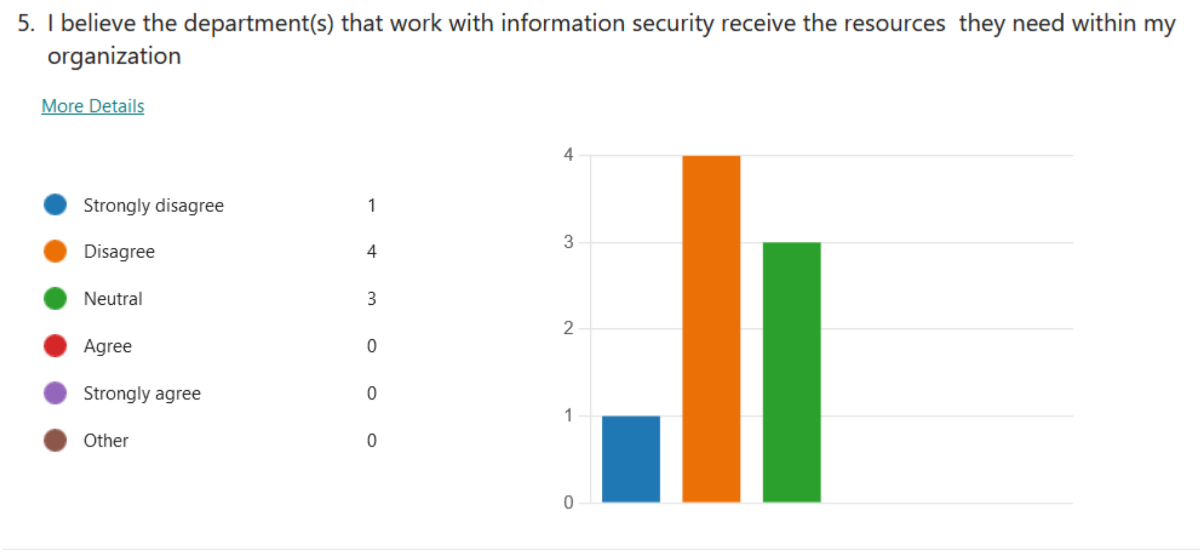
The CISO is responsible for the operative work with regards to IT-security and is responsible to establish guidelines and regulations, and that personnel are aware of established guidelines and regulations.

MAU has an information security Incident Response Team (IRT), which consists of the CISO and the university's legal advisor. The IRT is responsible for the development of emergency plans.

MAU fails to live up to two criteria of the MSBFS 2020:6, no regulation brings up education of personnel, and there is no explicit mention of when security and security documents should be revised.

4.11 Survey results

All the answers can be found in the table in Appendix 4

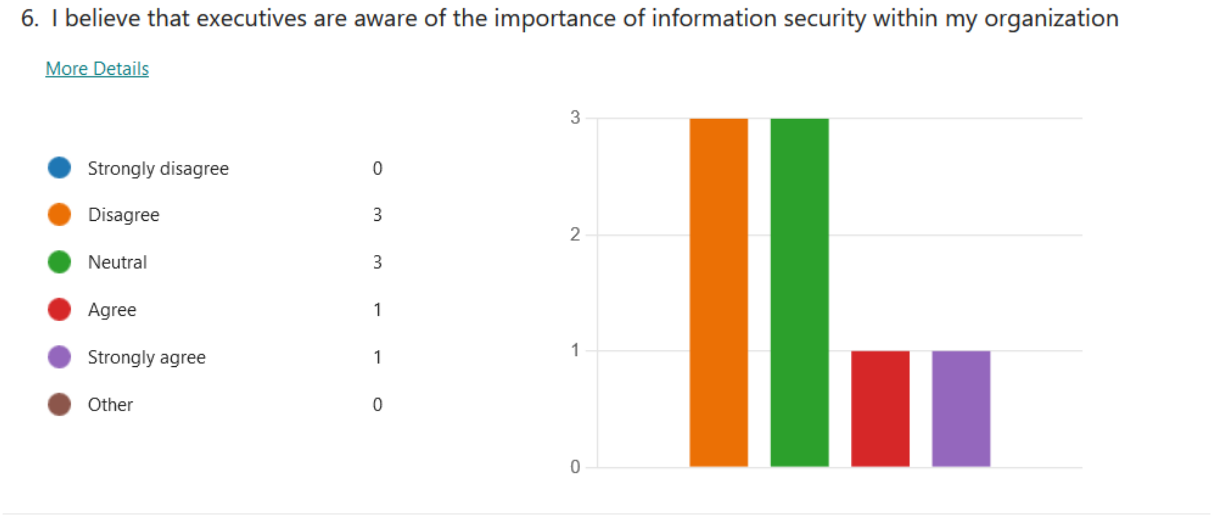


5. I believe the department(s) that work with information security receive the resources they need within my organization

More Details

●	Strongly disagree	1
●	Disagree	4
●	Neutral	3
●	Agree	0
●	Strongly agree	0
●	Other	0

Figure 4.1

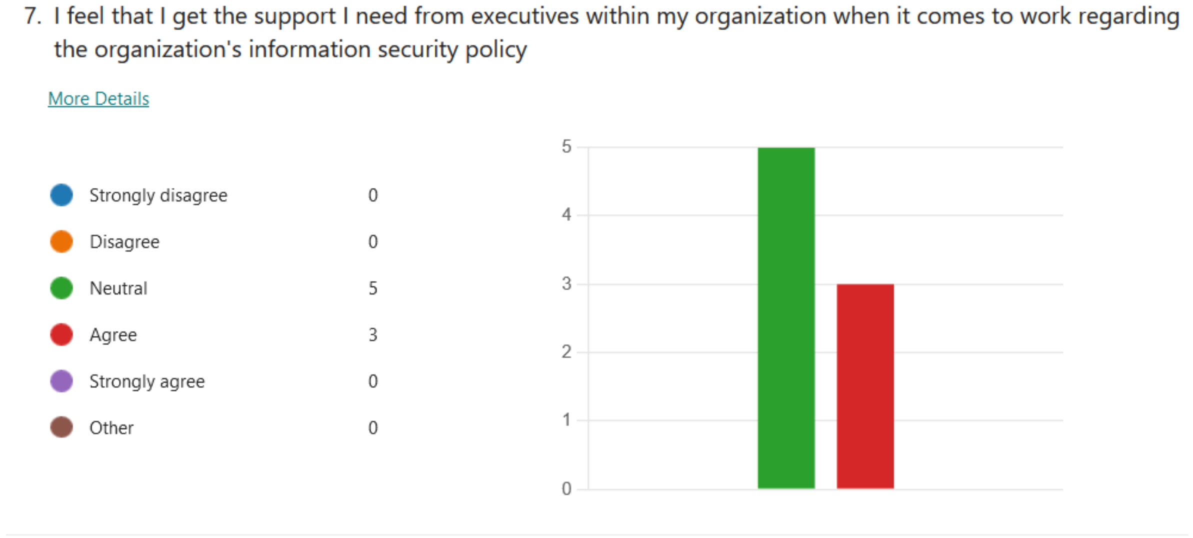


6. I believe that executives are aware of the importance of information security within my organization

More Details

●	Strongly disagree	0
●	Disagree	3
●	Neutral	3
●	Agree	1
●	Strongly agree	1
●	Other	0

Figure 4.2

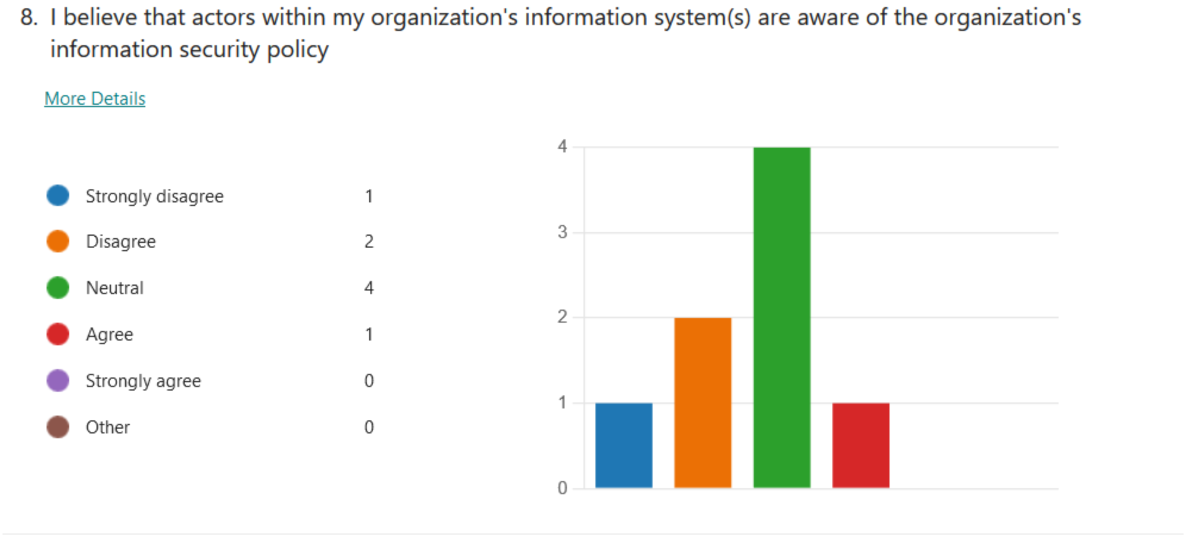


7. I feel that I get the support I need from executives within my organization when it comes to work regarding the organization's information security policy

More Details

●	Strongly disagree	0
●	Disagree	0
●	Neutral	5
●	Agree	3
●	Strongly agree	0
●	Other	0

Figure 4.3

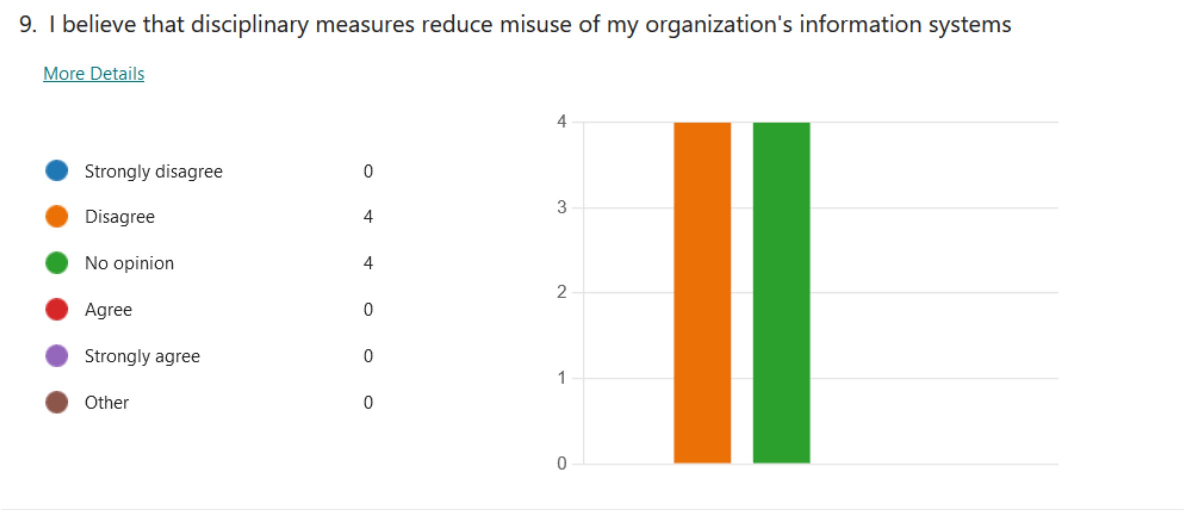


8. I believe that actors within my organization's information system(s) are aware of the organization's information security policy

More Details

●	Strongly disagree	1
●	Disagree	2
●	Neutral	4
●	Agree	1
●	Strongly agree	0
●	Other	0

Figure 4.4

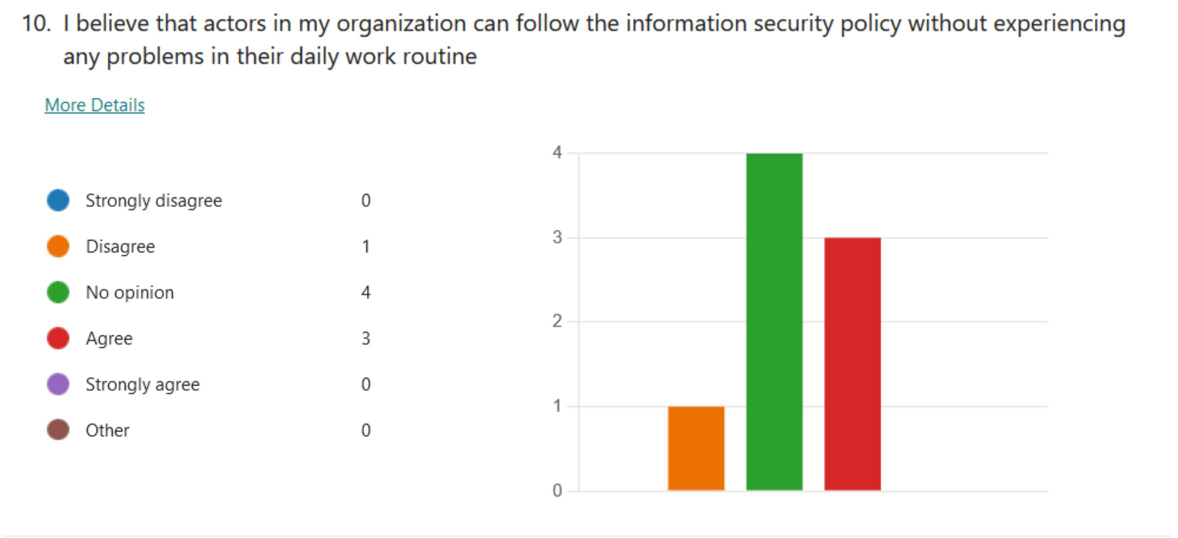


9. I believe that disciplinary measures reduce misuse of my organization's information systems

More Details

🔵 Strongly disagree	0
🟠 Disagree	4
🟢 No opinion	4
🔴 Agree	0
🟣 Strongly agree	0
🟤 Other	0

Figure 4.5

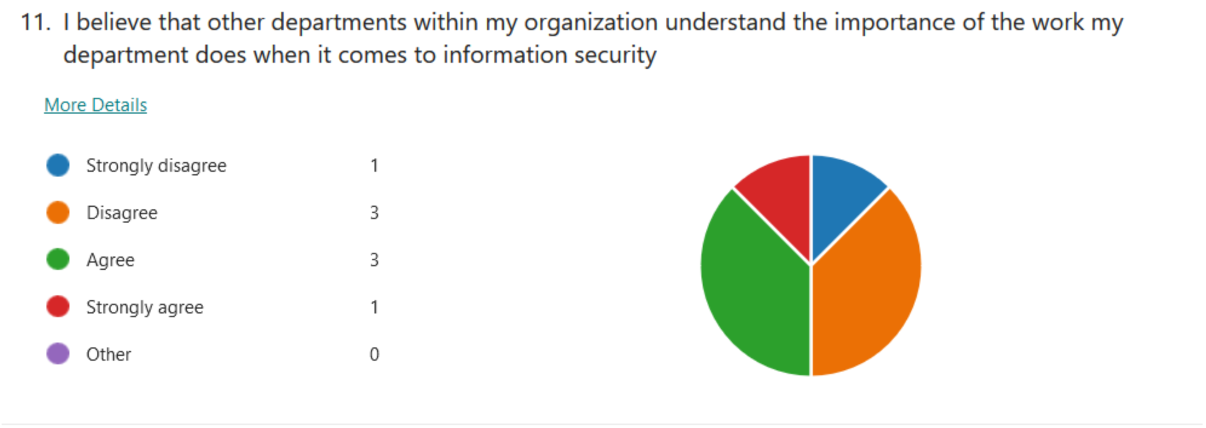


10. I believe that actors in my organization can follow the information security policy without experiencing any problems in their daily work routine

More Details

🔵 Strongly disagree	0
🟠 Disagree	1
🟢 No opinion	4
🔴 Agree	3
🟣 Strongly agree	0
🟤 Other	0

Figure 4.6

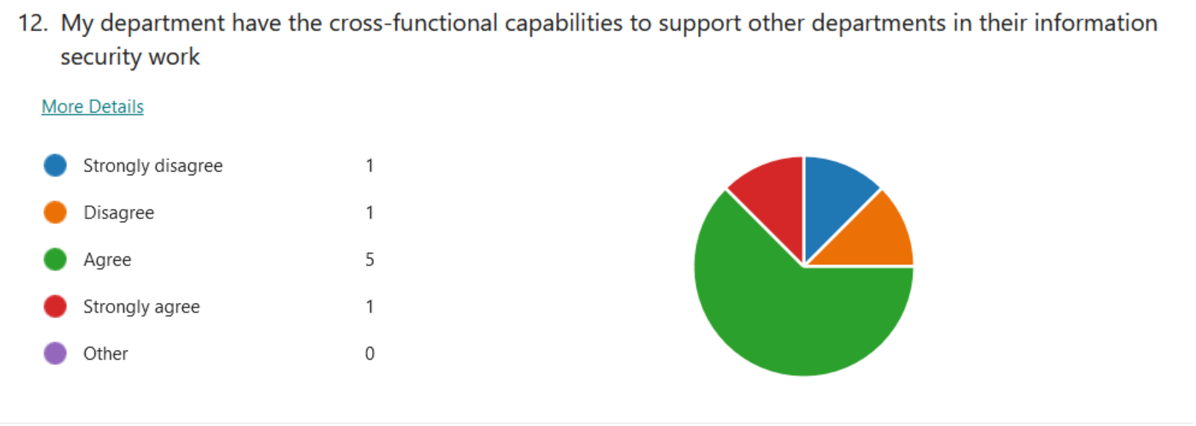


11. I believe that other departments within my organization understand the importance of the work my department does when it comes to information security

More Details

🔵 Strongly disagree	1
🟠 Disagree	3
🟢 Agree	3
🔴 Strongly agree	1
🟣 Other	0

Figure 4.7

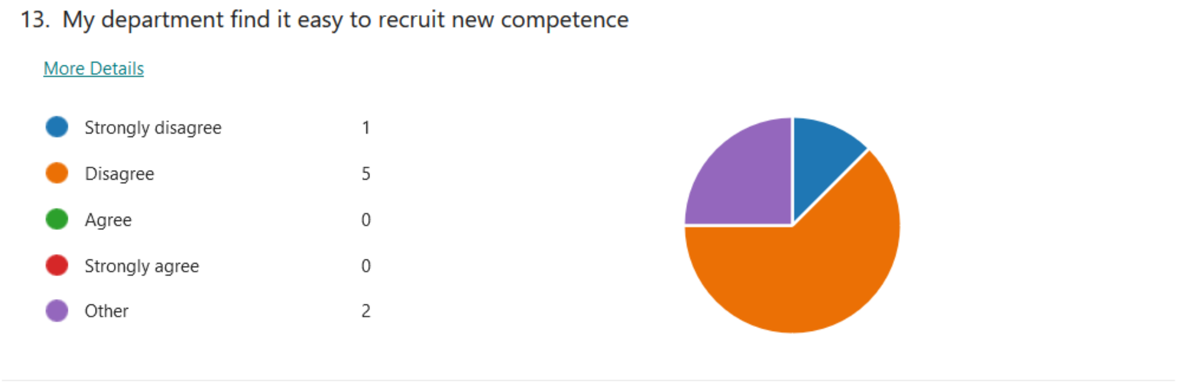


12. My department have the cross-functional capabilities to support other departments in their information security work

More Details

● Strongly disagree	1
● Disagree	1
● Agree	5
● Strongly agree	1
● Other	0

Figure 4.8



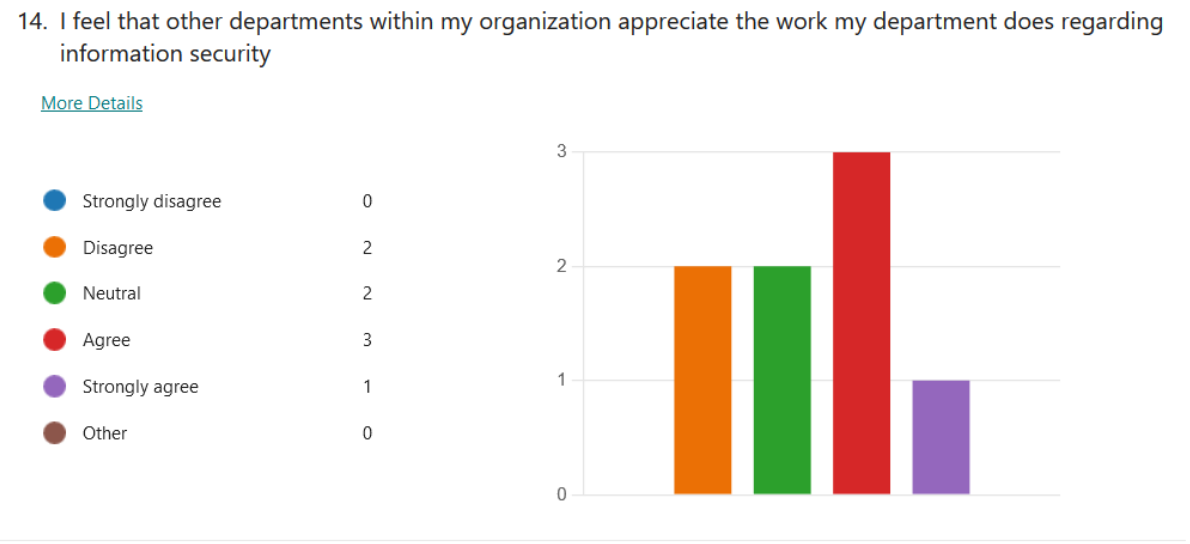
13. My department find it easy to recruit new competence

More Details

● Strongly disagree	1
● Disagree	5
● Agree	0
● Strongly agree	0
● Other	2

Figure 4.9

Here the answer “other” contained two customized answers, one answer stated that they had “No opinion”. The second stated that their department “hasn’t tried”.

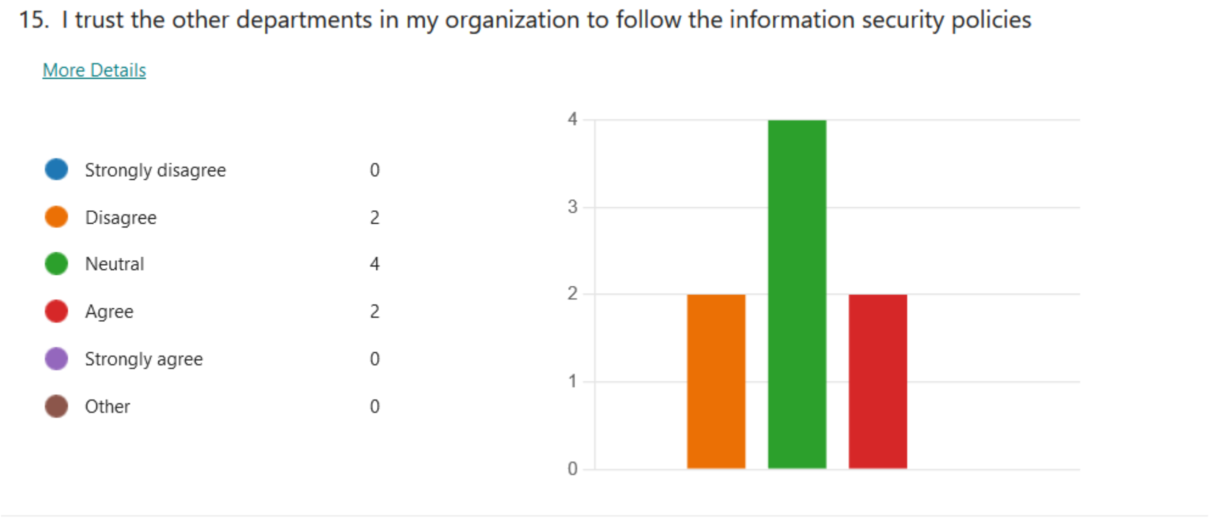


14. I feel that other departments within my organization appreciate the work my department does regarding information security

More Details

● Strongly disagree	0
● Disagree	2
● Neutral	2
● Agree	3
● Strongly agree	1
● Other	0

Figure 4.10

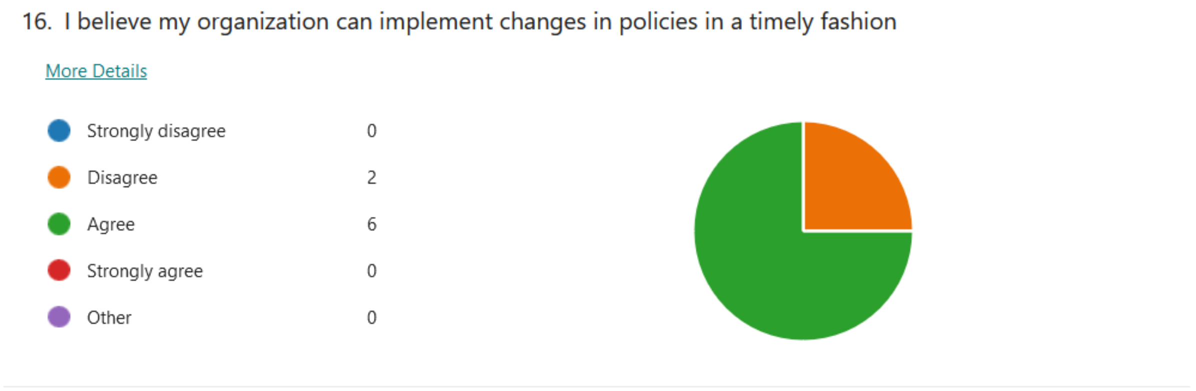


15. I trust the other departments in my organization to follow the information security policies

More Details

●	Strongly disagree	0
●	Disagree	2
●	Neutral	4
●	Agree	2
●	Strongly agree	0
●	Other	0

Figure 4.11

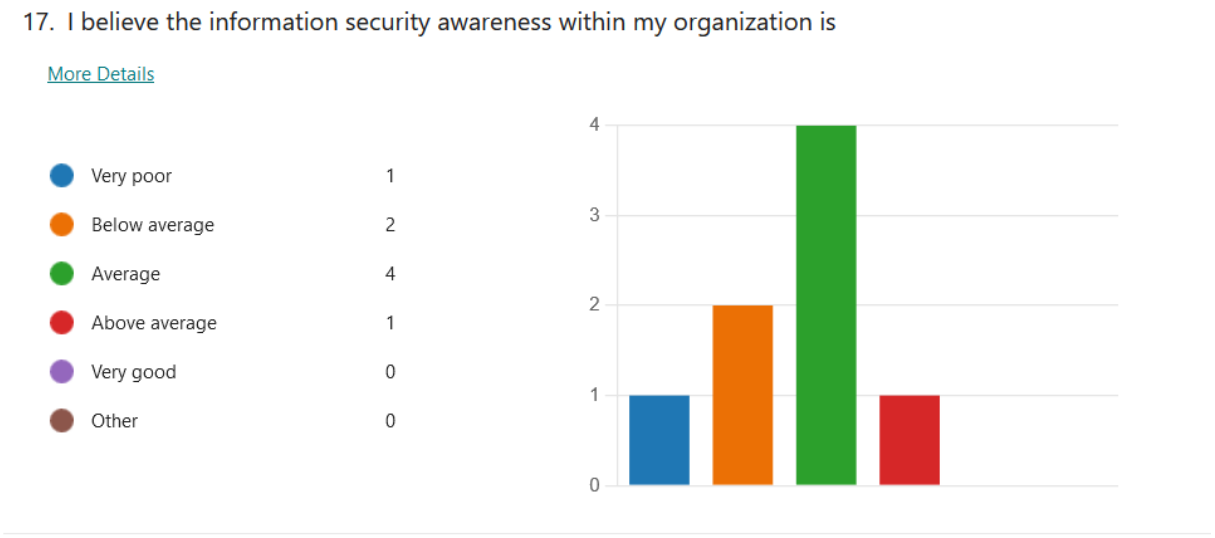


16. I believe my organization can implement changes in policies in a timely fashion

More Details

●	Strongly disagree	0
●	Disagree	2
●	Agree	6
●	Strongly agree	0
●	Other	0

Figure 4.12

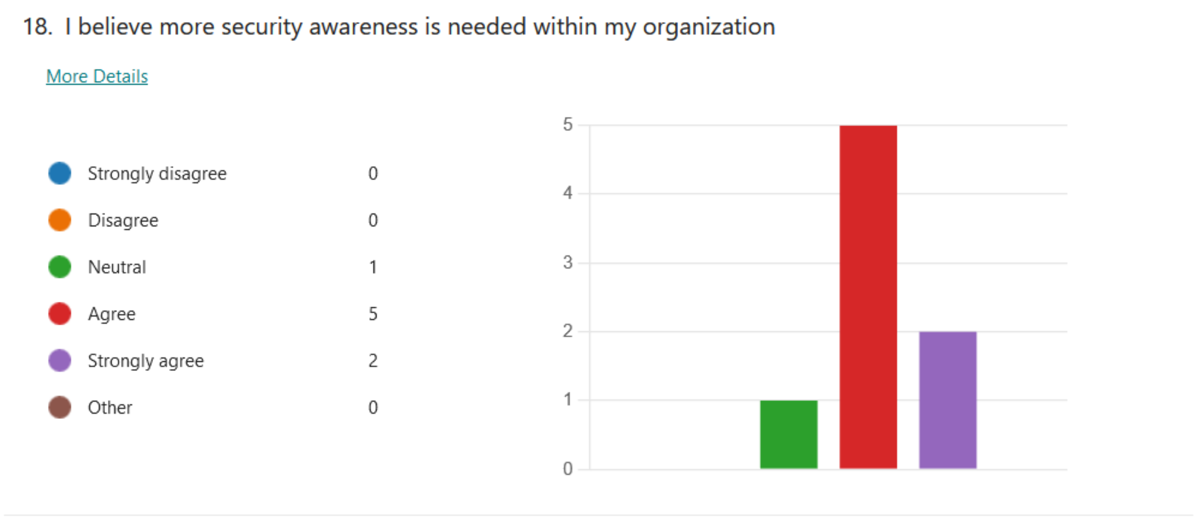


17. I believe the information security awareness within my organization is

More Details

●	Very poor	1
●	Below average	2
●	Average	4
●	Above average	1
●	Very good	0
●	Other	0

Figure 4.13

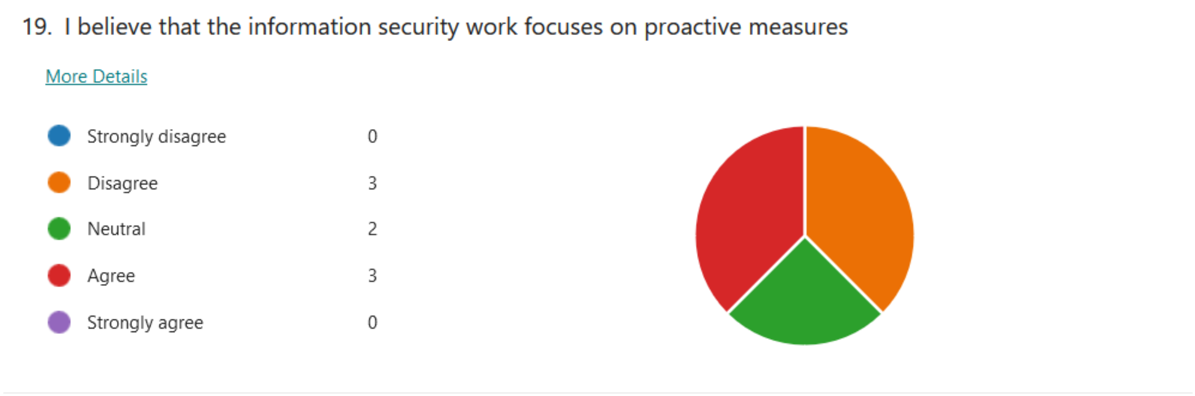


18. I believe more security awareness is needed within my organization

More Details

🔵	Strongly disagree	0
🟠	Disagree	0
🟢	Neutral	1
🔴	Agree	5
🟣	Strongly agree	2
🟤	Other	0

Figure 4.14

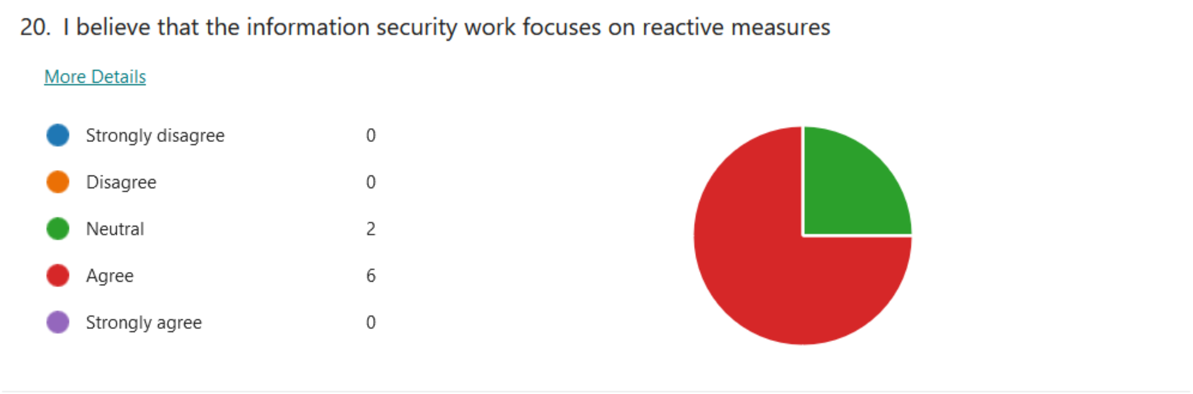


19. I believe that the information security work focuses on proactive measures

More Details

🔵	Strongly disagree	0
🟠	Disagree	3
🟢	Neutral	2
🔴	Agree	3
🟣	Strongly agree	0

Figure 4.15

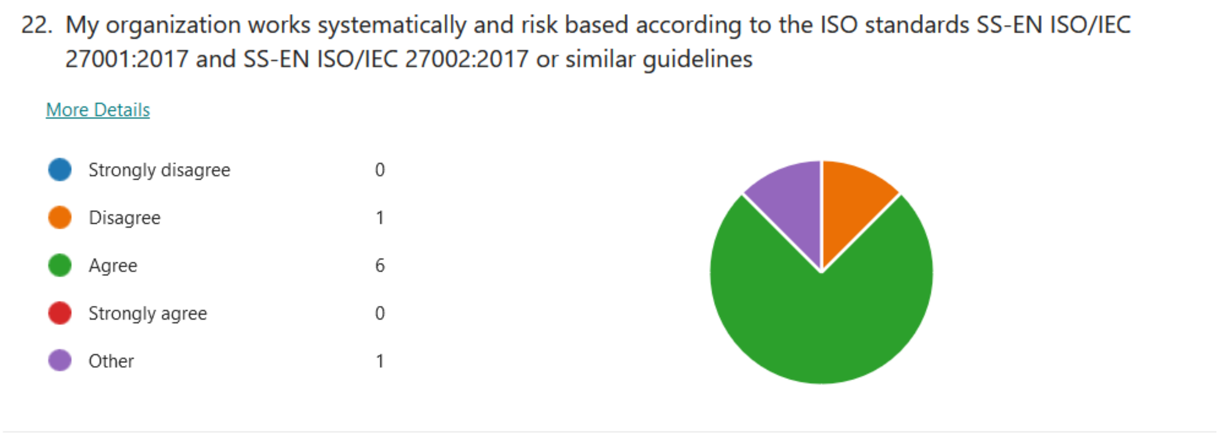


20. I believe that the information security work focuses on reactive measures

More Details

🔵	Strongly disagree	0
🟠	Disagree	0
🟢	Neutral	2
🔴	Agree	6
🟣	Strongly agree	0

Figure 4.16



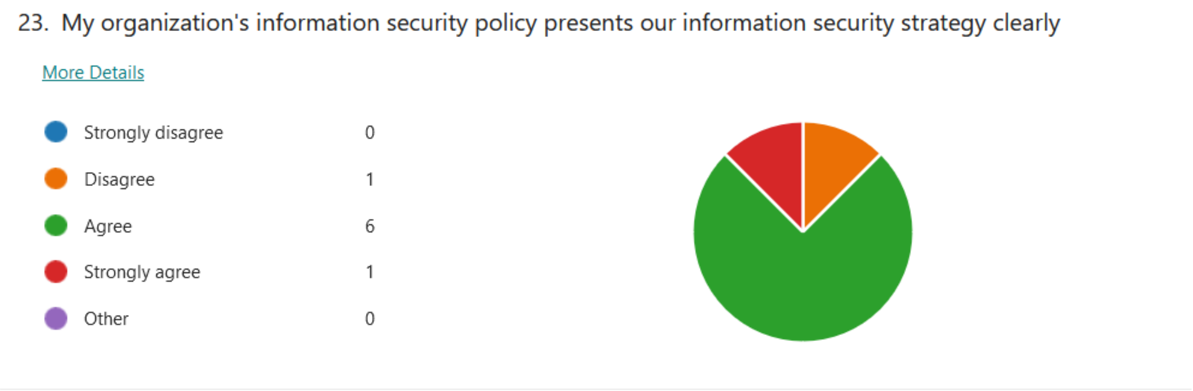
22. My organization works systematically and risk based according to the ISO standards SS-EN ISO/IEC 27001:2017 and SS-EN ISO/IEC 27002:2017 or similar guidelines

More Details

●	Strongly disagree	0
●	Disagree	1
●	Agree	6
●	Strongly agree	0
●	Other	1

Figure 4.17

As noted in the method section, one respondent commented that in their organization some departments worked with an information security standard, while others did not.

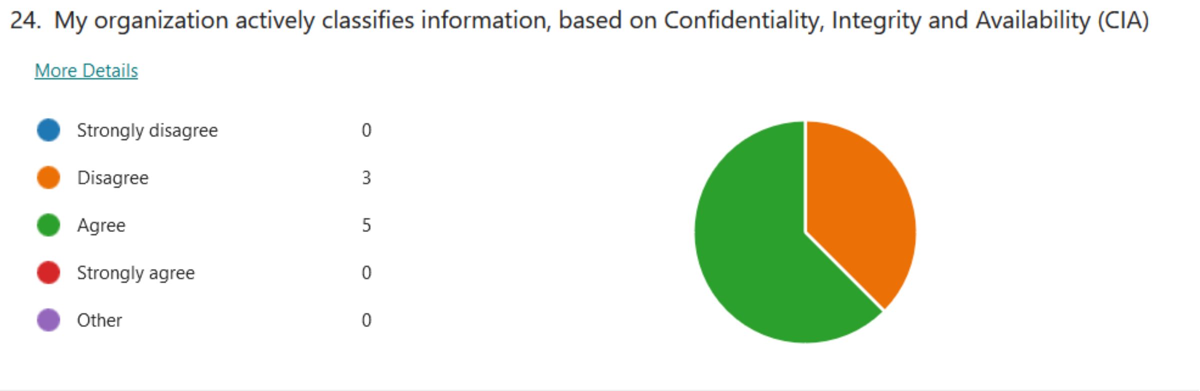


23. My organization's information security policy presents our information security strategy clearly

More Details

●	Strongly disagree	0
●	Disagree	1
●	Agree	6
●	Strongly agree	1
●	Other	0

Figure 4.18

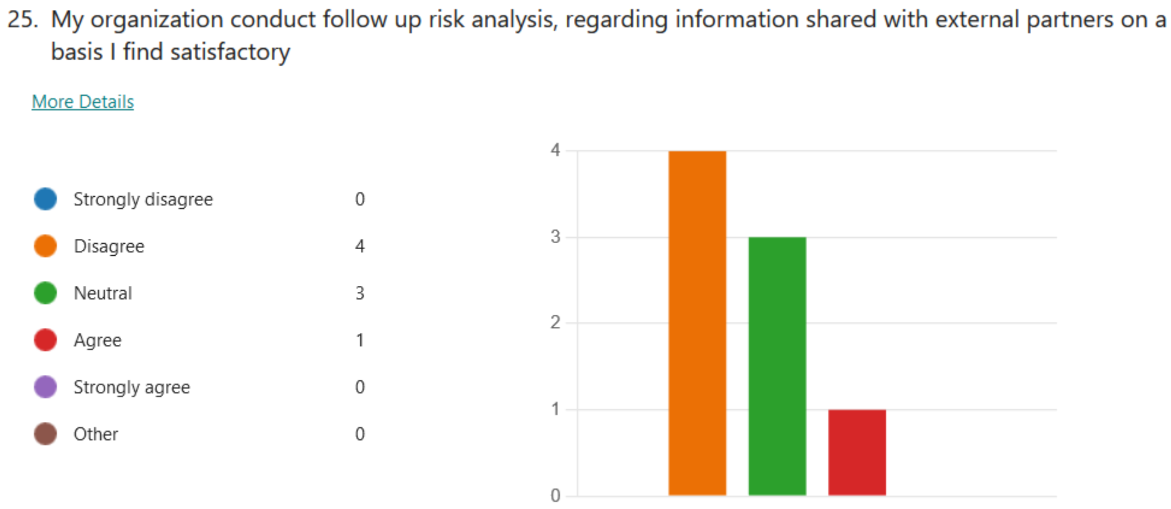


24. My organization actively classifies information, based on Confidentiality, Integrity and Availability (CIA)

More Details

●	Strongly disagree	0
●	Disagree	3
●	Agree	5
●	Strongly agree	0
●	Other	0

Figure 4.19

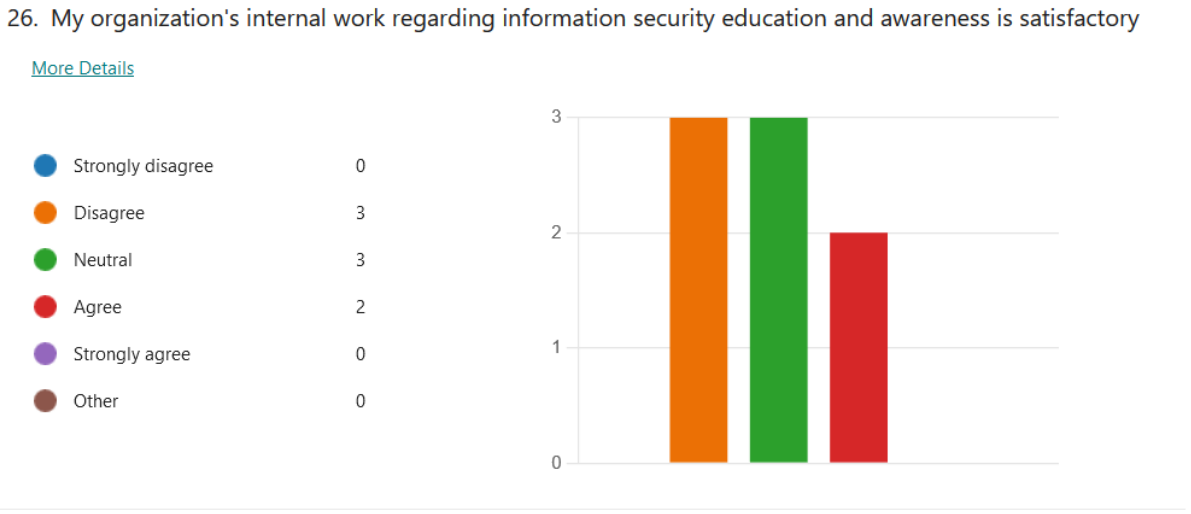


25. My organization conduct follow up risk analysis, regarding information shared with external partners on a basis I find satisfactory

More Details

● Strongly disagree	0
● Disagree	4
● Neutral	3
● Agree	1
● Strongly agree	0
● Other	0

Figure 4.20

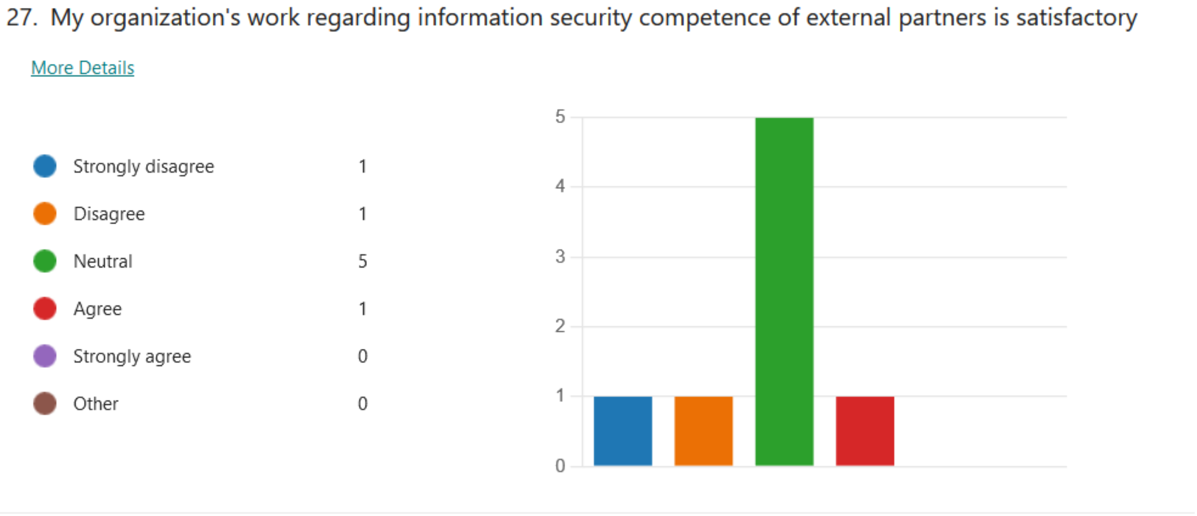


26. My organization's internal work regarding information security education and awareness is satisfactory

More Details

● Strongly disagree	0
● Disagree	3
● Neutral	3
● Agree	2
● Strongly agree	0
● Other	0

Figure 4.21

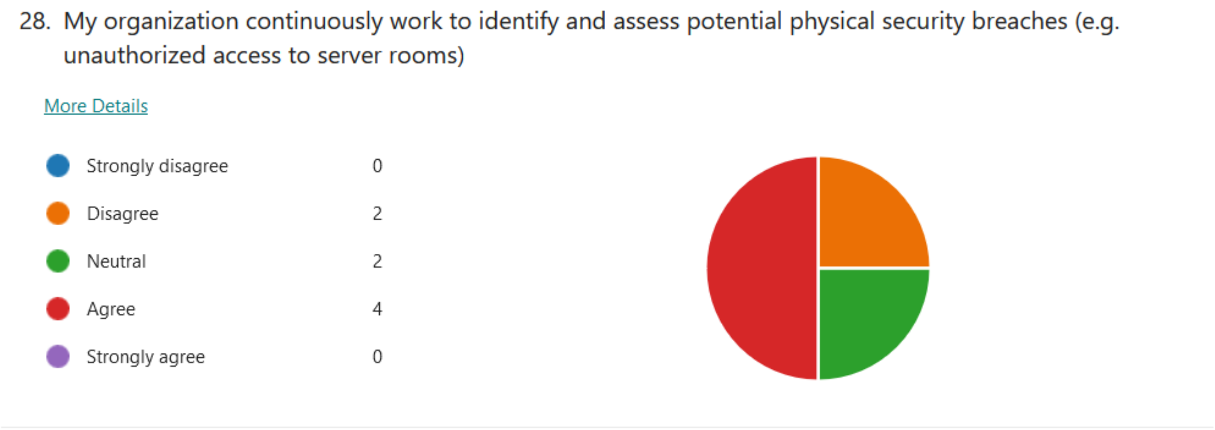


27. My organization's work regarding information security competence of external partners is satisfactory

More Details

● Strongly disagree	1
● Disagree	1
● Neutral	5
● Agree	1
● Strongly agree	0
● Other	0

Figure 4.22

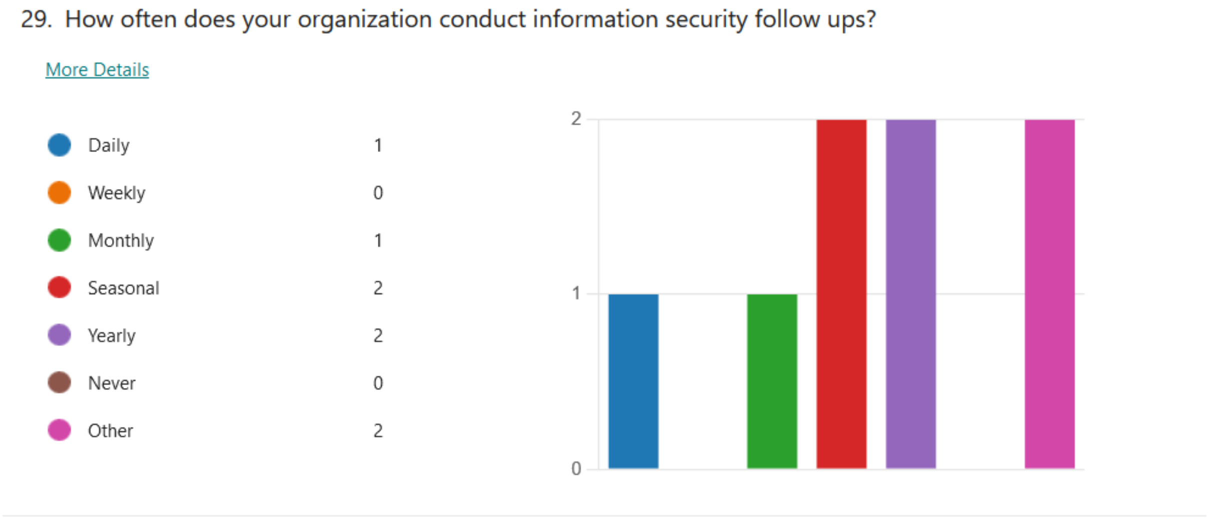


28. My organization continuously work to identify and assess potential physical security breaches (e.g. unauthorized access to server rooms)

More Details

●	Strongly disagree	0
●	Disagree	2
●	Neutral	2
●	Agree	4
●	Strongly agree	0

Figure 4.23



29. How often does your organization conduct information security follow ups?

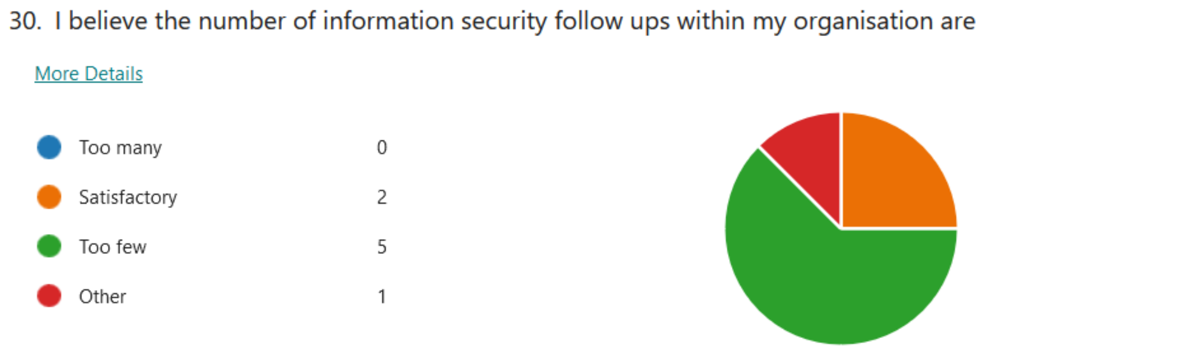
More Details

●	Daily	1
●	Weekly	0
●	Monthly	1
●	Seasonal	2
●	Yearly	2
●	Never	0
●	Other	2

Figure 4.24

Here two respondents wrote it was dependent on what type of follow up it was "It depends on what it is. For example, information classification is supposed to be followed up yearly."

While the other one wrote "Sometimes yearly and sometimes more seldom."



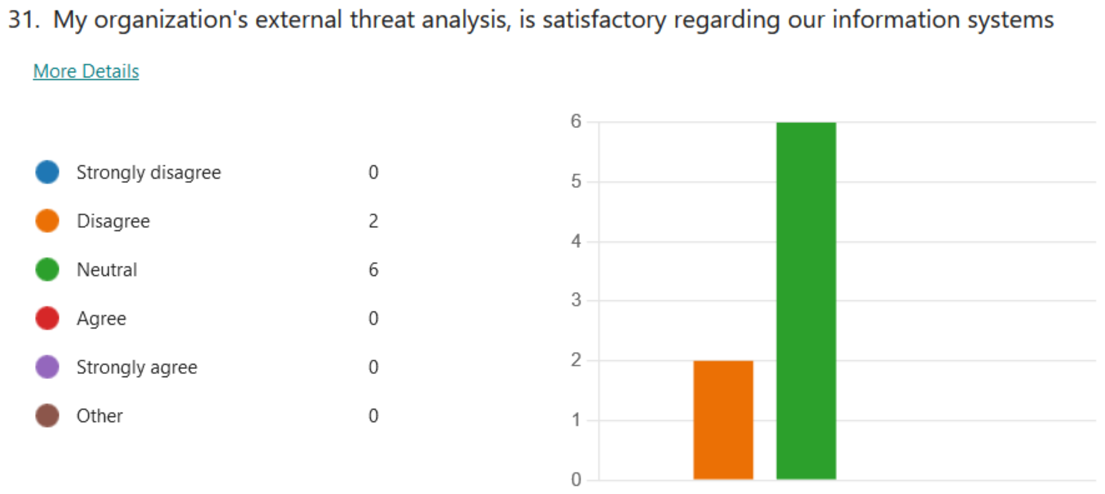
30. I believe the number of information security follow ups within my organisation are

More Details

●	Too many	0
●	Satisfactory	2
●	Too few	5
●	Other	1

Figure 4.25

Here one respondent wrote that they did not understand the question.

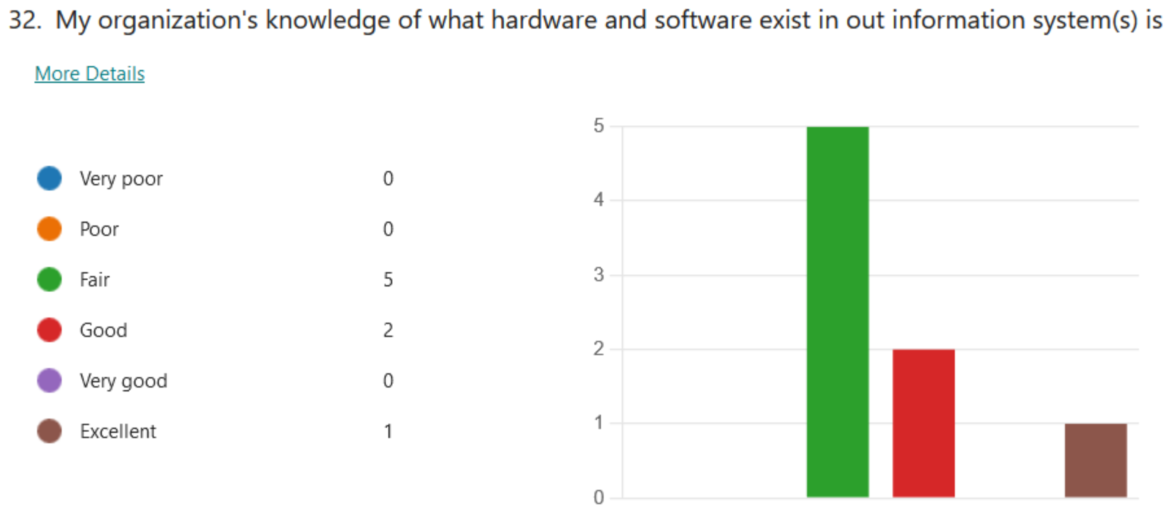


31. My organization's external threat analysis, is satisfactory regarding our information systems

More Details

🔵	Strongly disagree	0
🟠	Disagree	2
🟢	Neutral	6
🔴	Agree	0
🟣	Strongly agree	0
🟤	Other	0

Figure 4.26

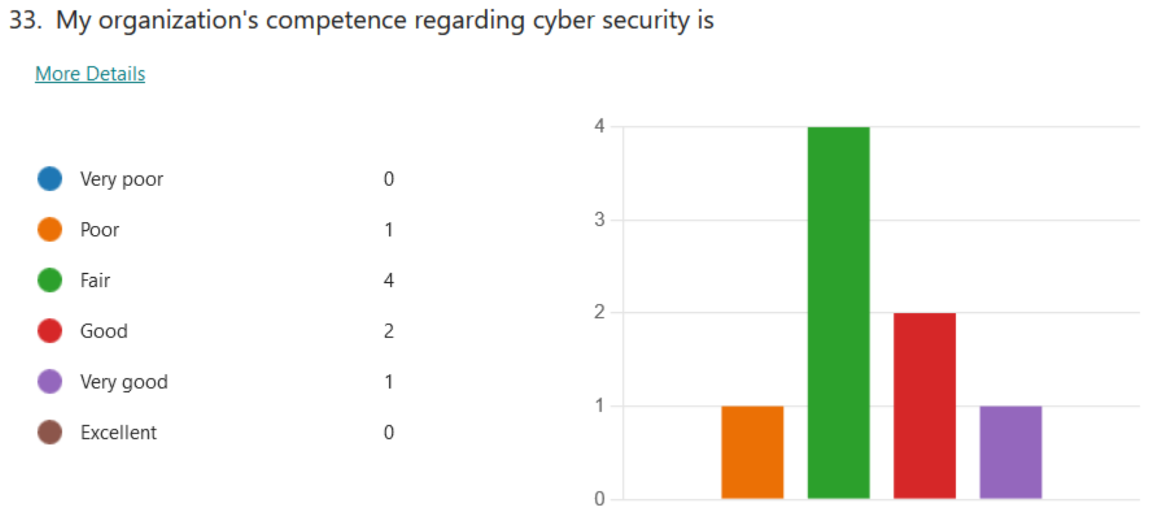


32. My organization's knowledge of what hardware and software exist in out information system(s) is

More Details

🔵	Very poor	0
🟠	Poor	0
🟢	Fair	5
🔴	Good	2
🟣	Very good	0
🟤	Excellent	1

Figure 4.27

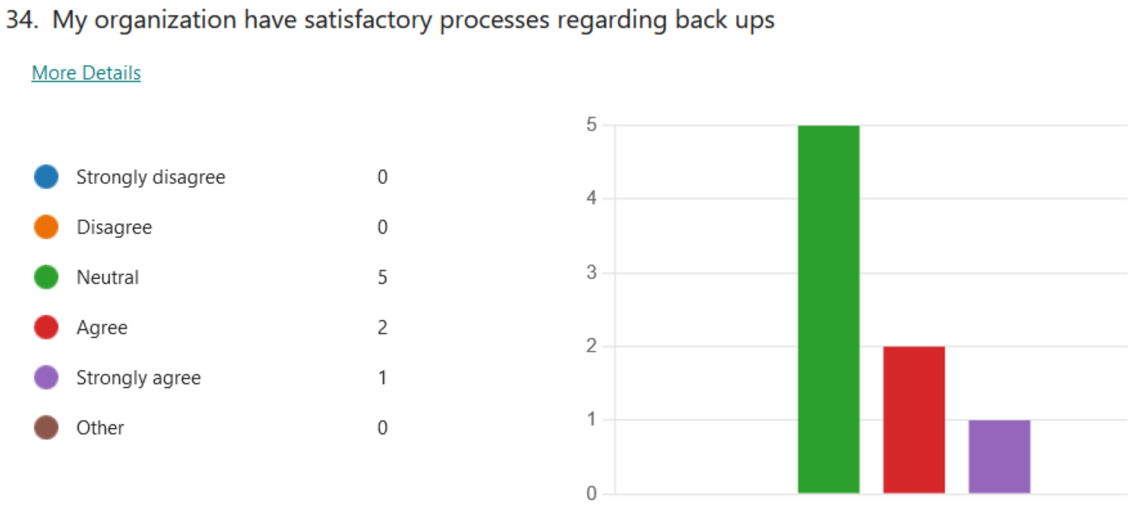


33. My organization's competence regarding cyber security is

More Details

🔵	Very poor	0
🟠	Poor	1
🟢	Fair	4
🔴	Good	2
🟣	Very good	1
🟤	Excellent	0

Figure 4.28

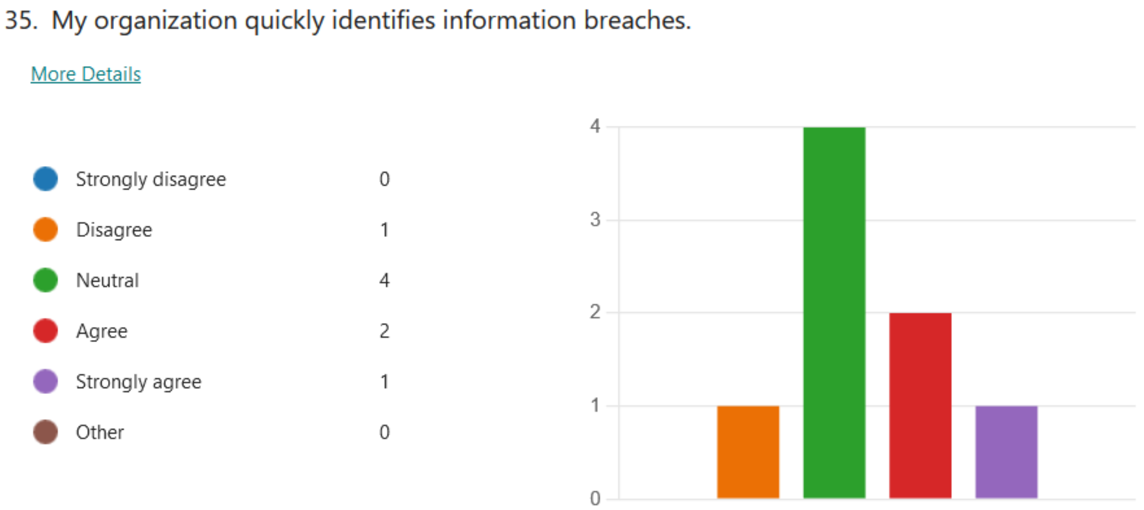


34. My organization have satisfactory processes regarding back ups

More Details

●	Strongly disagree	0
●	Disagree	0
●	Neutral	5
●	Agree	2
●	Strongly agree	1
●	Other	0

Figure 4.29

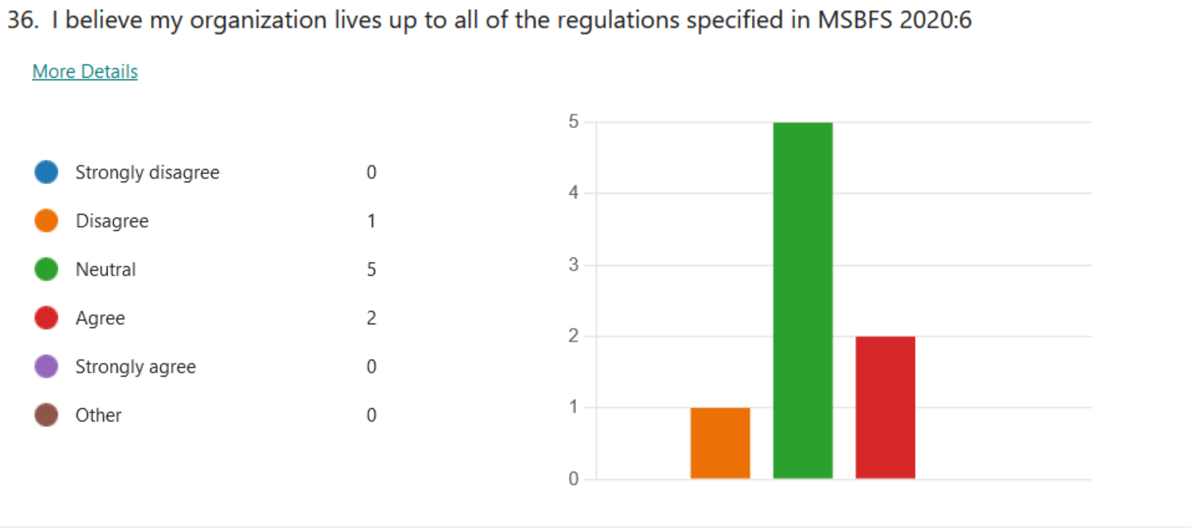


35. My organization quickly identifies information breaches.

More Details

●	Strongly disagree	0
●	Disagree	1
●	Neutral	4
●	Agree	2
●	Strongly agree	1
●	Other	0

Figure 4.30

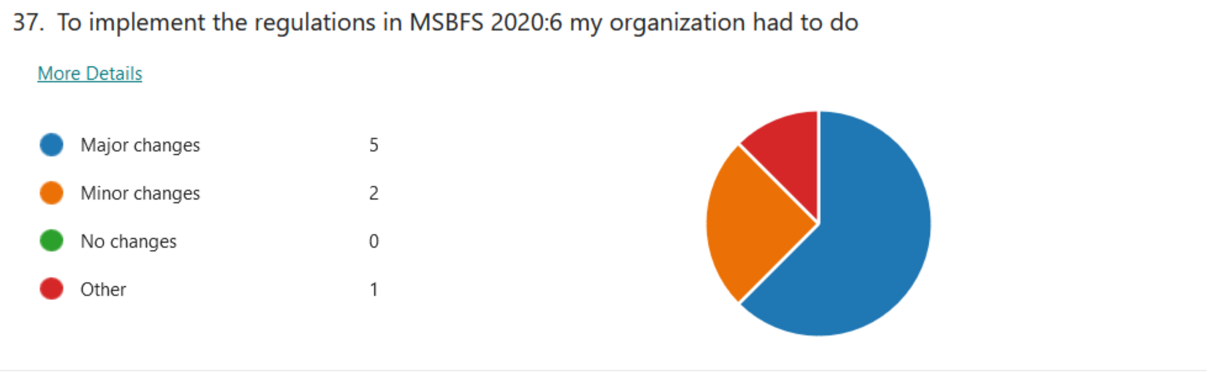


36. I believe my organization lives up to all of the regulations specified in MSBFS 2020:6

More Details

●	Strongly disagree	0
●	Disagree	1
●	Neutral	5
●	Agree	2
●	Strongly agree	0
●	Other	0

Figure 4.31

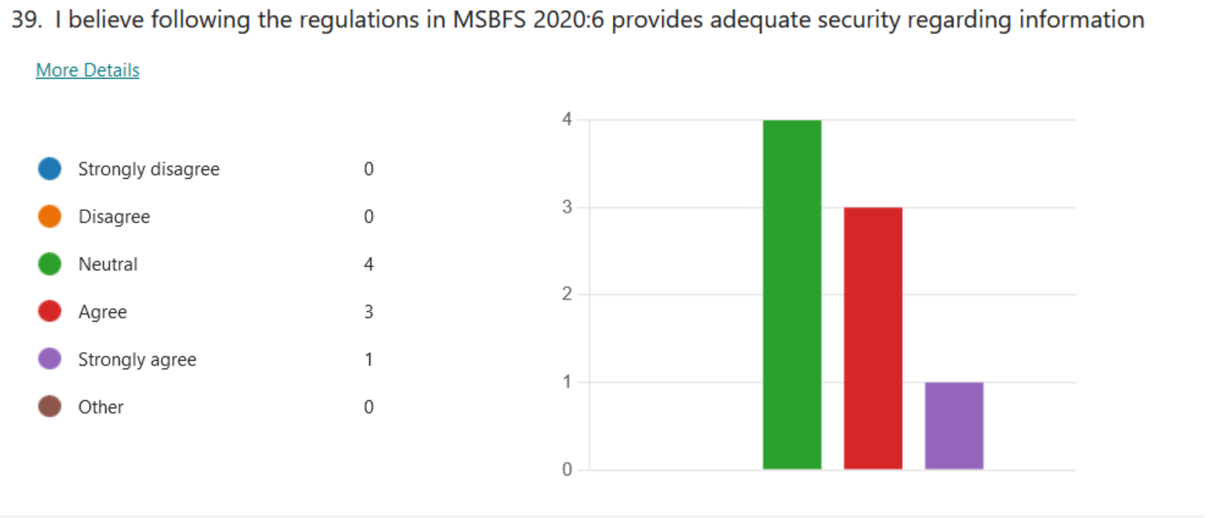


37. To implement the regulations in MSBFS 2020:6 my organization had to do

More Details

●	Major changes	5
●	Minor changes	2
●	No changes	0
●	Other	1

Figure 4.32

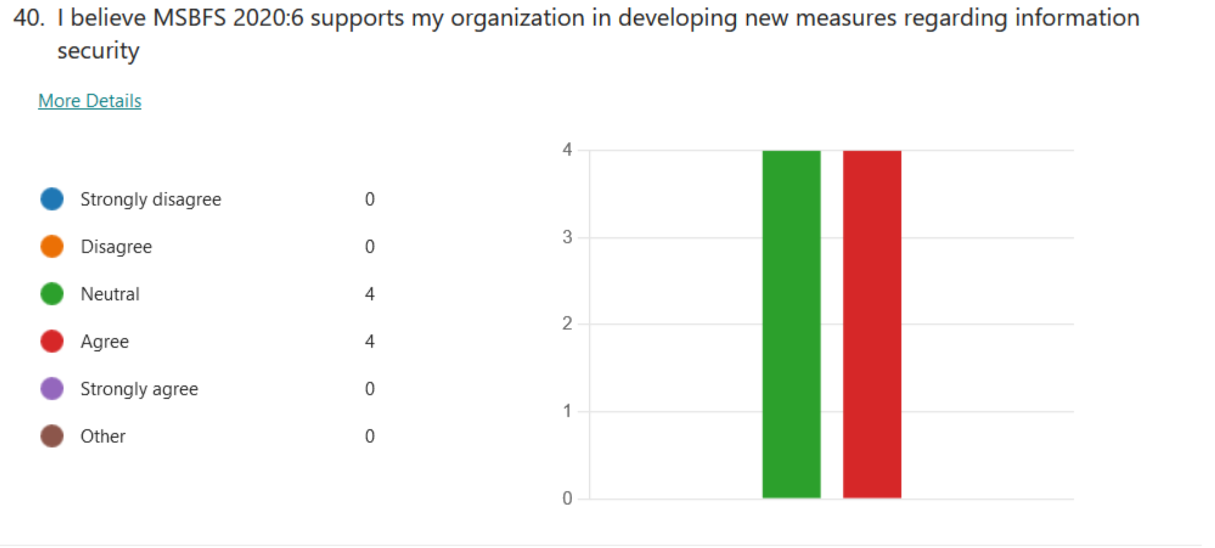


39. I believe following the regulations in MSBFS 2020:6 provides adequate security regarding information

More Details

●	Strongly disagree	0
●	Disagree	0
●	Neutral	4
●	Agree	3
●	Strongly agree	1
●	Other	0

Figure 4.33

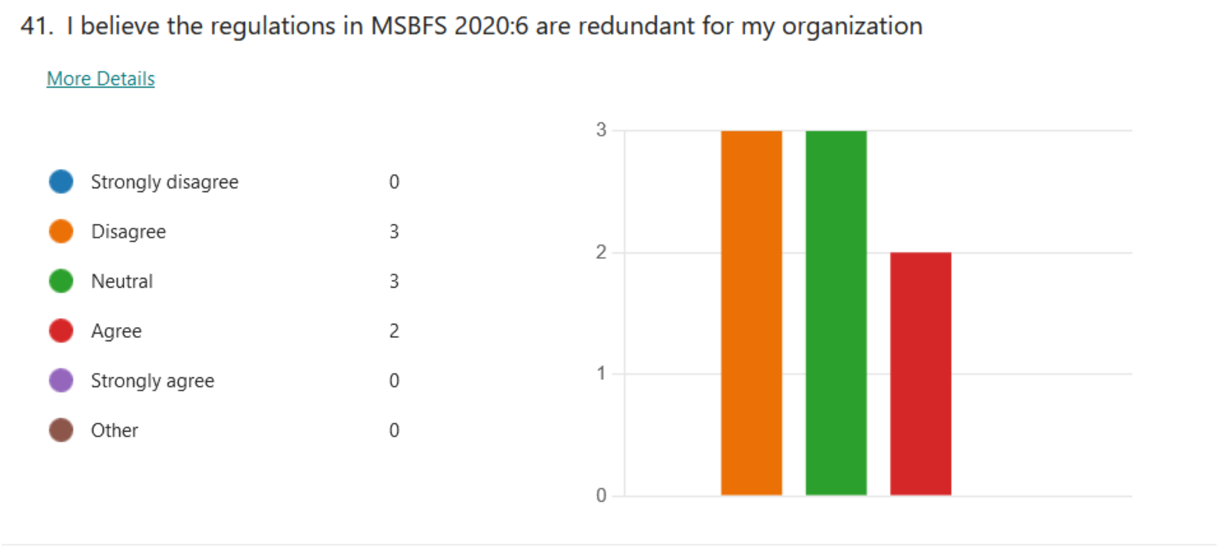


40. I believe MSBFS 2020:6 supports my organization in developing new measures regarding information security

More Details

●	Strongly disagree	0
●	Disagree	0
●	Neutral	4
●	Agree	4
●	Strongly agree	0
●	Other	0

Figure 4.34



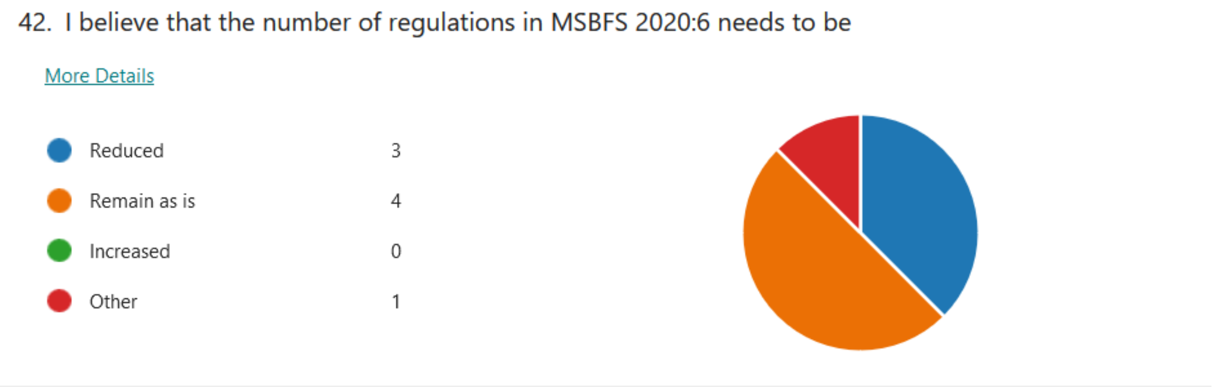
41. I believe the regulations in MSBFS 2020:6 are redundant for my organization

More Details

● Strongly disagree	0
● Disagree	3
● Neutral	3
● Agree	2
● Strongly agree	0
● Other	0

Figure 4.35

In the following two questions one respondent answered with “-“.

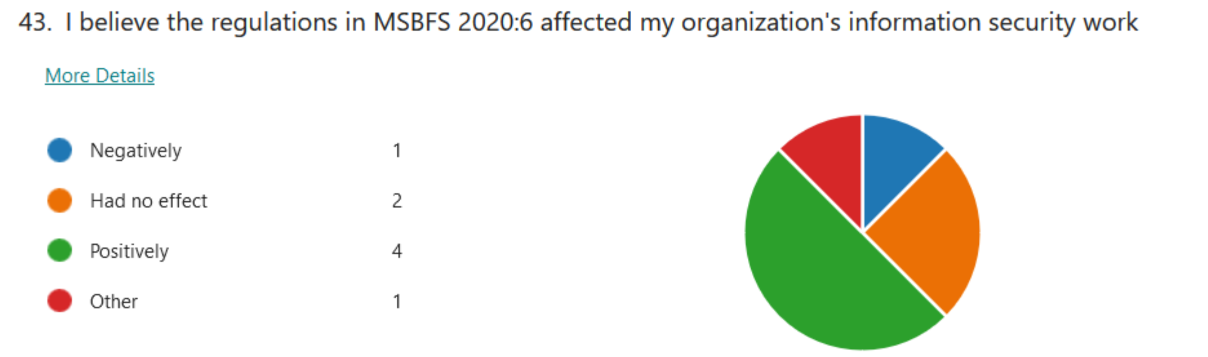


42. I believe that the number of regulations in MSBFS 2020:6 needs to be

More Details

● Reduced	3
● Remain as is	4
● Increased	0
● Other	1

Figure 4.36



43. I believe the regulations in MSBFS 2020:6 affected my organization's information security work

More Details

● Negatively	1
● Had no effect	2
● Positively	4
● Other	1

Figure 4.37

4.11.1 Summary

5 out of 8 do not believe that the departments who work with information security get the resources that they need. There seems to exist a lack of support from executives regarding information security, though respondents also feel supported by executives when it comes to work with the ISP. Moreover, respondents do seem to feel that other departments do not take

information security seriously, this while respondents believe they have the capability to support other departments with information security competence. Competence also seems to be a struggle for many information security departments.

There seems to exist an information security unawareness among university employees, and most of the respondents believe more ISA is needed within their organization. Regarding the responses concerning how the different departments work, the information security maturity seems to differ between organizations, some employees do believe it works well, others do not, though most agree on that they believe more information security awareness is needed within the organization.

The majority of the respondents believe that information security focuses on reactive measures, in other words the focus is to amend and repair potential damage when an incident occurs, this while only three believe the same is true for proactive measures, where activities such as staff education and training often is placed.

Further analyzing the MSBFS 2020:6 regulations and how respondents believe their organization reach the goals only one disagree and two agree with this statement, this even though many of them are not satisfied with how their organization handles certain segments of the regulations.

Overall, there seems to exist support for MSBFS 2020:6 among the respondents, though three answer that they would like to see the number of regulations reduced.

5 Discussion

The structure of the investigated organizations has properties common with each other. All the investigated organizations can be viewed as an echelon like ontological hierarchy, where the operative works at a department, who is led by the head of department, who is led by the principal or corresponding. Yet all investigated organizations have had different approaches when interpreting the MSBFS 2020:6 requirements and how they have chosen to deal with information security.

MIUN has one of the more unorthodox implementations, where the infrastructure department (INFRA) are responsible for anything related to information security. This allows INFRA to become a network node within the university, and work as a channel for both internal and external communication. This specialist department can therefor work as a mediator for the rest of the organization, which leads to an adaptability that none of the other investigated groups have, in case the organization needs to reorganize.

The choice that every department is responsible for their own information and IT security requires personnel with competence. This will increase the need for competent employees required to securely maintain information systems. This organizational responsibility model and the universities lack of information security awareness and education initiatives may cause serious issues in the future. First and foremost, the respondents answer that they find it difficult to recruit new competence. Moreover, the majority of the respondents in the survey state that there exists a demand for more information security awareness. Some respondents also believe that information security is a reactive process, this is a contradiction as most researchers sees awareness as a proactive measure.

One of Puhakainen and Siponen’s (2010) findings, is the importance of the involvement of the whole organization when it comes to develop good information security practices. Yet out of the 83 (total of 85, 1 no longer employed at the institution, 1 not in the target group) emailed IT-managers only 8 responded, which shows that either information security is a neglected area that IT-professionals are not aware of, or that it only involves a few select within the university IT-departments.

An interesting finding is that while many researchers propose that there needs to exist a requirement of balance between security and efficiency (Dhillon & Backhouse, 2001; Whitman et al., 2001; Siponen, 2005; Siponen, 2006; Hedström et al., 2011), only one respondent believes that following the ISP will inhibit the productivity of employees.

There also seems to exist a confusion around the regulations in MSBFS 2020:6, while two respondents state that they agree that their organization lives up to the regulations, only one disagree and the remaining five state that they neither agree nor disagree with the statement. At the same time four of the answers to the question; “My organization conduct follow up risk analysis, regarding information shared with external partners on a basis I find satisfactory”, state that they disagree with this statement, even though this is one of regulations in MSBFS 2020:6.

The LU information security guideline document refers to an ISP, five years after the decision of implementing the guideline document, the ISP still has not been signed and approved by the principal, this makes one reflect upon why important decisions take such long time?

Among the ten further investigated universities, only seven information security policies were found as public documents. Further some of the universities had split their policies into several different documents, resulting in the important policies and regulation documents within the management information system difficult to find. This correlates with what NAO reported in 2016, during their information security audit, that many employees were unaware of where to find the specific documents (Riksrevisionen, 2016).

From the perspective of Baskerville (1993) and Siponen (2005) who sees the evolution of information security methods divided into different generations, the contemporary use of information security seems to have stagnated and settled in the fifth generation. This may stem from the lack of empirical research done regarding the implementation and iterative development of information security as noted by for example Cram et al. (2017).

As noted by Aurigemma and Mattson (2019) there exists a lack of research regarding contingency theory within information security research, the results presented in this study shows that organizations have different procedures even though their mission and structure are similar, even though the universal models may yield valuable insights. Moreover, information system security research has focused on theory development and whether the individual employee have been burdened by regulations or not and seems to have disregarded the observations done by the security experts.

Further the key success factors when implementing an information security standard, identified by Smith et al. (2010), were adequate funding, support from management and buy-ins, in comparison the responses implies that IT Security-departments are underfunded and receive varying levels of support from executives.

6 Conclusion

This study contributes with qualitative and quantitative empirical data. As well as an analysis of information security in the context of Swedish universities.

Regarding the first research question, the study has a limited scope but the results from the content analysis shows that Swedish universities lives up to a high degree of the regulations set by MSB, but some institutions do not live up to all the regulations even though they are obliged to do so. Three of the further investigated universities seem to completely neglect education of personnel or at least do not state anything about this in their ISP document. This is supported by the findings in the survey where everyone except one answered that they believed that more information security awareness is needed. Further only two agreed that their organization’s internal information security education and awareness programs were satisfactory.

Analyzing the data from the quantitative part, the information security staff that have responded to the survey seems to struggle with funding and support, both from executives and other departments. Though they generally perceive the regulations as good guidelines. It is of utmost importance to be aware of the fact that none of the respondents believed the number of regulations should be increased, rather the opposite as three of them thought there were too many rules and regulations, and actually believed the number of regulations should be reduced. Further research is needed to understand this phenomenon. With the increase of regulations and different standards such as the information security standard ISO/IEC 27001, has too much complexity been introduced into the management system for employees to fully understand the system?

Education is according to D’Arcy et al. (2009) as well as Puhakainen and Siponen (2010) one of the most important organizational tools to counteract noncompliance. If the number and types of attacks aimed at the educational institutions in the Educational Institutions Findings Annex - Cyber Security Breaches Survey 2022 (2022) are accurate, the most cost efficient countermeasure is education and awareness programs. As stated, before these education and awareness programs have been neglected by the Swedish universities, this is further supported by the findings by previous scholars that state human errors often lead to data breaches (D'Arcy et al., 2014; Kajtazi et al., 2021; Hedström et al., 2011). The massive number of social engineered attacks also points towards this type of attack being the vector with the highest return of investment, which further demonstrate the importance of aware employees.

Further none of the respondents agree with the statement that punishments deter actors from misusing the information systems, this may indicate a metamorphosis of deterrence theory in the context of information security from sovereign power towards disciplinary power. This can also be a result of a higher engagement from employees reducing the need for sanctions as predicted by Siponen (2005).

The results in this study provide indicators that information security awareness and education programs are still needed within many of the Swedish institutions of higher education. While many may have a basic SETA program, this does not seem to be enough to prevent a future information security crisis.

Appendix 1

Regulation	UU	LU	LNU	GU	ORU	LTU	UMU	MIUN	KAU	MAU
Yearly follow up	n	y	y	y	N/A	N/A	y	y	N/A	n
- information continuity										
identify needs	y	y	y	y	N/A	N/A	y	y	N/A	y
practice	y	y	y	y	N/A	N/A	y	y	N/A	y
- Incidents and deviations										
assess and discover	y	y	y	y	N/A	N/A	y	y	N/A	y
recover manipulated or lost data	y	y	y	y	N/A	N/A	y	y	N/A	y
assess if report is needed	y	y	y	y	N/A	N/A	y	y	N/A	y
- Protection										
prevent trespassing	y	y	y	y	N/A	N/A	y	y	N/A	y
technical alarm solutions	y	y	y	y	N/A	N/A	y	y	N/A	y
separation of physical zones	y	y	y	y	N/A	N/A	y	y	N/A	y
- Personnel										
background checks dependant on access level	y	y	y	y	N/A	N/A	y	y	N/A	y
inform about rules, regulations, work method and support	y	y	y	y	N/A	N/A	y	y	N/A	y
make sure InfoSec employees have sufficient competence	y	y	y	y	N/A	N/A	y	y	N/A	y
develop education programs, initiatives regarding InfoSec	n	y	y	n	N/A	N/A	y	y	N/A	n
- External actor										
other government actor										
document what actor is responsible for what	y	y	y	y	N/A	N/A	y	y	N/A	y
other external actor (EA)										
handle the risks involved in information transfer	y	y	y	y	N/A	N/A	y	y	N/A	y
have an agreement with requirements EA needs to follow	y	y	y	y	N/A	N/A	y	y	N/A	y
Plan to follow up EA follows requirements	y	y	y	y	N/A	N/A	y	y	N/A	y
- Information classification										
Confidentiality, Integrity, Availability (CIA)	y	y	y	y	N/A	N/A	y	y	N/A	y
Risk assessment	y	y	y	y	N/A	N/A	y	y	N/A	y
Countermeasures	y	y	y	y	N/A	N/A	y	y	N/A	y
Evaluate countermeasures and adapt if needed	y	y	y	y	N/A	N/A	y	y	N/A	y

y = yes, n = no, N/A = Not available

Appendix 2

UU	https://regler.uu.se/digitalAssets/704/c_704260-l_3-k_ufv2018-668-sakerinformationshantering20180815.pdf https://regler.uu.se/digitalAssets/33/c_33861-l_3-k_rktlinjer-for-sakerhetsarbetet.pdf https://regler.uu.se/digitalAssets/41/c_41950-l_1-k_ufv2017-93-informationsecurity.pdf	
LNU	https://lnu.se/globalassets/dokument---gemensamma/universitetsledningenskansli/organisationsplan-for-informationssakerhet.pdfhttps://lnu.se/medarbetare/anstalld-vid-lnu/kris-ochsakerhet/sakerhet/informationssakerhet/	
LU	https://www.medarbetarwebben.lu.se/sites/medarbetarwebben.lu.se/files/riktlinjerfor-informationssakerhet-vid-lunds-universitet.pdf	
GU	https://medarbetarportalen.gu.se/digitalAssets/1516/1516608_it-s--kerhetsregler_revidering20150212.pdf https://medarbetarportalen.gu.se/styrdokument/sakerhet/ https://medarbetarportalen.gu.se/digitalAssets/1504/1504073_policy-f--r-it-s--kerhetm-f--rsb141124.pdf	
LTU	https://www.ltu.se/cms_fs/1.164013!/file/Informationss%C3%A4kerhetspolicy%28238761%29%20%280%29_TMP.pdf	
UMU	https://www.umu.se/globalassets/fristaende-webbar/regelverk/beslutsstrukturdelegation-och-organisation/21---informationssakerhetspolicy-for-umea-universitet-fs-1.1.1-998-17.pdf https://www.umu.se/globalassets/fristaende-webbar/regelverk/lokaler-it-och-miljo/fs-1.1-807-22-regel.pdfhttps://www.umu.se/globalassets/fristaende-webbar/regelverk/lokaler-it-och-miljo/74---100-3305-10_itsakerhetsplan.pdf	
MIUN	https://www.miun.se/medarbetare/universitetet/informationssakerhet/a-o/	
KAU	https://www.kau.se/files/2017-09/allm%C3%A4nna_regler_f%C3%B6r_informationss%C3%A4kerhet_vid_kau_15241.pdf	
MAU	https://mau.app.box.com/s/yiqqizuaze7d9cd0na70	

Appendix 3

```
#read xlsx
df <- openxlsx::read.xlsx(‘SwedishUniversities.xlsx’)
#replace = FALSE does not allow for duplicates
rand_rows <- df[sample(nrow(df), 10, replace = FALSE),]

print(rand_rows)
```

Appendix 4

ID	1	2	3	4	5	6	7	8
Work title	Dataskyddsombud	Information Security Officer	IT administrator	[Redacted] & dataskyddsombud	Informationssäkerhetssamordnare	CIO	IT-chef	Information security advisor
Years of work experience with information security	10+ years	10+ years	6-10 years	1-5 year(s)	1-5 year(s)	10+ years	10+ years	10+ years
I work with	Information security risk managment;	Information security policy development;Information security awareness;Information security risk managment;	Information security policy development;Information security awareness;Information security risk managment;	Information security awareness;Developing information security related processes;Information security risk	Information security policy development;Information system audits;Developing information security related processes;Information security risk managment;Informatio	Information security policy development;Information security awareness;	IT-chef;	Information security policy development;Information security awareness;Information assurance;Information security risk managm

				managment;	n security awareness;			ent;Developing information security education programs;
Other information you wish to share								
I believe the department(s) that work with information security receive the resources they need within my organization	Disagree	Disagree	Strongly disagree	Disagree	Disagree	Neutral	Neutral	Neutral
I believe that executives are aware of the	Neutral	Strongly agree	Disagree	Disagree	Disagree	Agree	Neutral	Neutral

importance of information security within my organization								
I feel that I get the support I need from executives within my organization when it comes to work regarding the organization's information security policy	Neutral	Agree	Neutral	Neutral	Neutral	Agree	Agree	Neutral

I believe that actors within my organization's information system(s) are aware of the organization's information security policy	Neutral	Agree	Strongly disagree	Neutral	Neutral	Disagree	Neutral	Disagree
I believe that disciplinary measures reduce misuse of my organization's infor	No opinion	Disagree	No opinion	No opinion	Disagree	Disagree	No opinion	Disagree

mation systems								
I believe that actors in my organization can follow the information security policy without experiencing any problems in their daily work routine	No opinion	Agree	No opinion	Disagree	Agree	No opinion	No opinion	Agree
I believe that other departments within my	Agree	Agree	Strongly disagree	Disagree	Disagree	Strongly agree	Agree	Disagree

organization understand the importance of the work my department does when it comes to information security								
My department have the cross-functional capabilities to support other departments in their information	Strongly disagree	Agree	Agree	Agree	Agree	Strongly agree	Disagree	Agree

security work								
My department find it easy to recruit new competence	No opinion	Disagree	Hasn't tried	Disagree	Disagree	Strongly disagree	Disagree	Disagree
I feel that other departments within my organization appreciate the work my department does regarding information security	Agree	Neutral	Disagree	Neutral	Strongly agree	Agree	Disagree	Agree
I trust the other	Neutral	Agree	Disagree	Neutral	Agree	Neutral	Neutral	Disagree

departments in my organization to follow the information security policies								
I believe my organization can implement changes in policies in a timely fashion	Agree	Agree	Agree	Disagree	Agree	Agree	Disagree	Agree
I believe the information security awareness	Average	Average	Below average	Very poor	Below average	Average	Above average	Average

within my organization is								
I believe more security awareness is needed within my organization	Neutral	Agree	Agree	Strongly agree	Strongly agree	Agree	Agree	Agree
I believe that the information security work focuses on proactive measures	Agree	Disagree	Disagree	Agree	Agree	Disagree	Neutral	Neutral
I believe that the information secur	Agree	Agree	Neutral	Agree	Agree	Agree	Neutral	Agree

ity work focuses on reactive measures								
Additional comments								
My organization works systematically and risk based according to the ISO standards SS-EN ISO/IEC 27001:2017 and SS-EN ISO/IEC 27002:2017 or similar guidelines	Agree	Agree	Disagree	Unfortunately not all departments.	Agree	Agree	Agree	Agree

My organization's information security policy presents our information security strategy clearly	Agree	Agree	Agree	Agree	Strongly agree	Agree	Agree	Disagree
My organization actively classifies information, based on Confidentiality, Integrity and Availability (CIA)	Agree	Agree	Disagree	Agree	Disagree	Disagree	Agree	Agree

My organization conduct follow up risk analysis, regarding information shared with external partners on a basis I find satisfactory	Neutral	Disagree	Disagree	Disagree	Neutral	Disagree	Neutral	Agree
My organization's internal work regarding information security education and awareness	Neutral	Disagree	Agree	Neutral	Disagree	Disagree	Neutral	Agree

is satisfactory								
My organization's work regarding information security competence of external partners is satisfactory	Neutral	Neutral	Strongly disagree	Neutral	Neutral	Disagree	Neutral	Agree
My organization continuously work to identify and assess potential physical security breaches	Neutral	Agree	Disagree	Agree	Agree	Disagree	Neutral	Agree

(e.g. unauthorized access to server rooms)								
How often does your organization conduct information security follow ups?	Daily	Seasonal	Yearly	It depends on what it is. For example, information classification is supposed to be followed up yearly.	Yearly	Monthly	Seasonal	Sometimes yearly and sometimes more seldom.
I believe the number of information security follow ups within my organisati	Satisfactory	Too few	Satisfactory	Too few	don't understand the question	Too few	Too few	Too few

on are								
My organization's external threat analysis, is satisfactory regarding our information systems	Neutral	Neutral	Disagree	Neutral	Disagree	Neutral	Neutral	Neutral
My organization's knowledge of what hardware and software are exist in out information system(s) is	Fair	Excellent	Fair	Good	Good	Fair	Fair	Fair
My orga	Good	Very good	Fair	Good	Fair	Fair	Fair	Poor

nization's competence regarding cyber security is								
My organization have satisfactory processes regarding back ups	Neutral	Strongly agree	Neutral	Agree	Agree	Neutral	Neutral	Neutral
My organization quickly identifies information breaches.	Neutral	Strongly agree	Disagree	Neutral	Agree	Agree	Neutral	Neutral
I believe my organization lives up to all of	Neutral	Agree	Neutral	Disagree	Agree	Neutral	Neutral	Neutral

the regulations specified in MSBFS 2020:6								
To implement the regulations in MSBFS 2020:6 my organization had to do	-	Minor changes	Major changes	Major changes	Minor changes	Major changes	Major changes	Major changes
Additional comments 2								
I believe following the regulations in MSBFS 2020:6 provides adequate	Neutral	Agree	Agree	Agree	Neutral	Neutral	Neutral	Strongly agree

security regarding information								
I believe MSBFS 2020:6 supports my organization in developing new measures regarding information security	Neutral	Neutral	Agree	Agree	Agree	Neutral	Neutral	Agree
I believe the regulations in MSBFS 2020:6 are redundant for my	Neutral	Agree	Disagree	Disagree	Agree	Neutral	Neutral	Disagree

organization								
I believe that the number of regulations in MSBFS 2020:6 needs to be	-	Remain as is	Reduced	Remain as is	Remain as is	Reduced	Reduced	Remain as is
I believe the regulations in MSBFS 2020:6 affected my organization's information security work	-	Positively	Positively	Positively	Had no effect	Negatively	Had no effect	Positively
Additional comments 3								

References

Aurigemma, S. & Mattson, T. (2019). Generally Speaking, Context Matters: Making the Case for a Change from Universal to Particular Isp Research, *Journal of the Association for Information Systems,* vol. 20, no. 12**,** pp 1700-1742

Baskerville, R. (1993). Information-Systems Security Design Methods - Implications for Information-Systems Development, *Computing Surveys,* vol. 25, no. 4**,** pp 375-414

Boulding, K. E. (1956). General Systems Theory-the Skeleton of Science, *Management Science,* vol. 2, no. 3**,** pp 197-208

Bryman, A. (2016). Social Research Methods, 5th: Oxford university press.

Bulgurcu, B., Cavusoglu, H. & Benbasat, I. (2010). Information Security Policy Compliance: An Empirical Study of Rationality-Based Beliefs and Information Security Awareness, *MIS Quarterly,* vol. 34, no. 3**,** pp 523-548

Chen, H. & Li, W. (2014). Understanding Organization Employees Information Security Omission Behavior: An Integrated Model of Social Norm and Deterrence, vol. no.

Cram, W. A., Proudfoot, J. G. & D'Arcy, J. (2017). Organizational Information Security Policies: A Review and Research Framework, *European Journal of Information Systems,* vol. 26, no. 6**,** pp 605-641

D'Arcy, J., Herath, T. & Shoss, M. K. (2014). Understanding Employee Responses to Stressful

Information Security Requirements: A Coping Perspective, *Journal of Management Information Systems,* vol. 31, no. 2**,** pp 285-318

D'Arcy, J., Hovav, A. & Galletta, D. (2009). User Awareness of Security Countermeasures and Its Impact on Information Systems Misuse: A Deterrence Approach, *Information systems research,* vol. 20, no. 1**,** pp 79-98

Dhillon, G. & Backhouse, J. (2001). Current Directions in Is Security Research: Towards Socio-Organizational Perspectives, *Information Systems Journal,* vol. 11, no. 2**,** pp 127-153

Dhillon, G., Smith, K. & Dissanayaka, I. (2021).Information Systems Security Research Agenda: Exploring the Gap between Research and Practice, *Journal of Strategic Information Systems,* vol. 30, no. 4**,** pp 101693

Flowerday, S. V. & Tuyikeze, T. (2016). Information Security Policy Development and Implementation: The What, How and Who, *Computers & Security,* vol. 61, no. 169183

Forrester, J. W. (1958). Industrial Dynamics, *Harvard Business Review,* vol. 36, no. 4**,** pp 3766

Forrester, J. W. (1968). Industrial Dynamics—after the First Decade, *Management science,* vol. 14, no. 7**,** pp 398-415

Hedström, K., Kolkowska, E., Karlsson, F. & Allen, J. P. (2011). Value Conflicts for Information Security Management, *Journal of Strategic Information Systems,* vol. 20, no. 4**,** pp 373-384

Kajtazi, M., Holmberg, N., Sarker, S., Keller, C., Johansson, B. & Tona, O. (2021). Toward a Unified Model of Information Security Policy Compliance: A Conceptual Replication Study, *AIS Transactions on Replication Research,* vol. 7, no. 1**,** pp 2

Kalix.se. (2022). *Så Klarade Vi It-Attacken!* [Online]. Available online: https://www.kalix.se/Aktuellt/Omsorg-ochraddning/krisinformation/driftstorningarna-till-foljd-av-it-attacken/sa-klarade-vi-itattacken/ [Accessed 2022-07-12].

Klaić, A. & Hadjina, N. (2011) Published. Methods and Tools for the Development of Information Security Policy — a Comparative Literature Review. 2011 Proceedings of the 34th International Convention MIPRO, 23-27 May 2011. 1532-1537.

Lodge, M., Page, E. C., Balla, S. J. & Whitford, A. B. (2016). Oliver E. Williamson, Markets and Hierarchies: Analysis and Antitrust Implications: Oxford University Press.

Malone, T. W., Yates, J. & Benjamin, R. I. (1987). Electronic Markets and Electronic Hierarchies [It Effects], *Communications of the ACM,* vol. 30, no. 6**,** pp 484-497

MSB, M. f. s. o. b. (2022). En Inblick I Sveriges Cybersäkerhet Årsrapport It-Incidentrapportering 2021, (MSB), M. f. s. o. b.

Oates, B. J., Griffiths, M. & McLean, R. (2022). Researching Information Systems and Computing: Sage.

Paananen, H., Lapke, M. & Siponen, M. (2020). State of the Art in Information Security Policy Development, *Computers & Security,* vol. 88, no. 101608

Puhakainen, P. & Siponen, M. (2010). Improving Employees' Compliance through Information Systems Security Training: An Action Research Study, *MIS Quarterly,* vol. 34, no. 4**,** pp 767-A4

Riksrevisionen. (2014). Informationssäkerheten I Den Civila Statsförvaltningen.

Simon, H. A. (1988). The Science of Design: Creating the Artificial, *Design Issues,* vol. 4, no. 1/2**,** pp 67-82

Siponen, M. (2006). Six Design Theories for Is Security Policies and Guidelines, *Journal of the Association for Information systems,* vol. 7, no. 1**,** pp 19

Siponen, M., Soliman, W. & Vance, A. (2022). Common Misunderstandings of Deterrence Theory in Information Systems Research and Future Research Directions, *DATA BASE FOR ADVANCES IN INFORMATION SYSTEMS,* vol. 53, no. 1**,** pp 25-60

Siponen, M. & Willison, R. (2007). A Critical Assessment of Is Security Research between 1990-2004, vol. no.

Siponen, M. T. (Year) Published. Policies for Construction of Information Systems' Security Guidelines. IFIP International Information Security Conference, 2000. Springer, 111120.

Siponen, M. T. (2005). Analysis of Modern Is Security Development Approaches: Towards the Next Generation of Social and Adaptable Iss Methods, *Information and organization,* vol. 15, no. 4**,** pp 339-375

Straub, D. W. & Welke, R. J. (1998). Coping with Systems Risk: Security Planning Models for Management Decision Making, *Mis Quarterly,* vol. 22, no. 4**,** pp 441-469

Whitman, M. E., Townsend, A. M. & Aalberts, R. J. (2001). Information Systems Security and the Need for Policy. *Information Security Management: Global Challenges in the New Millennium.* IGI Global pp 9-18.

Bertalanffy, L. V. (1950). AN OUTLINE OF GENERAL SYSTEM THEORY, *The British Journal for the Philosophy of Science,* vol. Volume 1, no. Number 2

Chen, Y., Ramamurthy, K. & Wen, K.-W. (2012). Organizations' Information Security Policy Compliance: Stick or Carrot Approach?, *Journal of Management Information Systems,* vol. 29, no. 3, pp.157–188

Dimaggio, P. J. & Powell, W. W. (1983). THE IRON CAGE REVISITED: INSTITUTIONAL ISOMORPfflSM AND COLLECTIVE RATIONALITY IN ORGANIZATIONAL EIELDS, *AMERICAN SOCIOLOGICAL REVIEW*

Ebers, M. & Oerlemans, L. (2016). The Variety of Governance Structures Beyond Market and Hierarchy, *Journal of Management*, vol. 42, no. 6, pp.1491–1529

Educational Institutions Findings Annex - Cyber Security Breaches Survey 2022. (2022). *GOV.UK*, Available Online: https://www.gov.uk/government/statistics/cyber-security-breaches-survey-2022/educational-institutions-findings-annex-cyber-security-breaches-survey-2022 [Accessed 18 December 2022]

Holmström, M. (2022). Regeringen kräver skärpt it-säkerhet på högskolor, *DN*, 21 December, Available Online: https://www.dn.se/sverige/regeringen-kraver-skarpt-it-sakerhet-pa-hogskolor/ [Accessed 24 December 2022]

Hu, Q., Hart, P. & Cooke, D. (2007). The Role of External and Internal Influences on Information Systems Security – a Neo-Institutional Perspective, *The Journal of Strategic Information Systems*, vol. 16, no. 2, pp.153–172

Kast, F. E. & Rosenzweig, J. E. (1972). General Systems Theory: Applications for Organization and Management, *Academy of Management Journal*, vol. 15, no. No. 4

Lounsbury, M. & Boxenbaum, E. (2013). Institutional Logics in Action, in M. Lounsbury & E. Boxenbaum (eds), *Institutional Logics in Action, Part A*, Vol. 39 Part A, [e-book] Emerald Group Publishing Limited, pp.3–22, Available Online: https://doi.org/10.1108/S0733-558X(2013)0039AB004 [Accessed 31 December 2022]

Moody, G. D., Siponen, M. & Pahnila, S. (2018). TOWARD A UNIFIED MODEL OF INFORMATION SECURITY POLICY COMPLIANCE., *MIS Quarterly*, vol. 42, no. 1, pp.285-A22

Myndigheten för samhällsskydd och beredskap MSB. (2021). Årsrapport it-incidentrapportering 2021

Patton, M. Q. (2014). Qualitative Research & Evaluation Methods: Integrating Theory and Practice, Sage publications

Peterson, R. A. (1994). A Meta-Analysis of Cronbach's Coefficient Alpha, *Journal of Consumer Research*, vol. 21, no. 2, p.381

Smith, Winchester, Bunker, & Jamieson. (2010). Circuits of Power: A Study of Mandated Compliance to an Information Systems Security 'De Jure' Standard in a Government Organization, *MIS Quarterly*, vol. 34, no. 3, p.463

Tavakol, M. & Dennick, R. (2011). Making Sense of Cronbach's Alpha, *International Journal of Medical Education*, vol. 2, pp.53–55

Thornton, P. H. & Ocasio, W. (1999). Institutional Logics and the Historical Contingency of Power in Organizations: Executive Succession in the Higher Education Publishing Industry, 1958– 1990, *American Journal of Sociology*, vol. 105, no. 3, pp.801–843

Vetenskapsrådet. (2017). God forskningssed

Ågerfalk, P. J. (2013). Embracing Diversity through Mixed Methods Research, *European Journal of Information Systems*, vol. 22, no. 3, pp.251–256

Universitetskanslersämbetet. (2022). *Lista Över Universitet, Högskolor Och Enskilda Utbildningsanordnare* [Online]. Available online: https://www.uka.se/fakta-omhogskolan/universitet-och-hogskolor/lista-over-universitet-hogskolor-och-enskildautbildningsanordnare.html.

Oates, B. J., Griffiths, M. & McLean, R. (2022). Researching Information Systems and Computing: Sage.