YRKESHÖGSKOLAN
NOVIA

CISSP certification – accreditation value for employees and recruiters

Tommi Äijälä

Master's Thesis in Business and Administration,

The degree programme in Leadership and Service Design

Turku, Finland 2018

MASTER'S THESIS

Author: Tommi Äijälä
Degree Programme and place: Leadership and Service Design, Turku

Supervisor: Thomas Finne

Title: CISSP certification – accreditation value for employees and recruiters

---

Date: 28.5.2018 Number of pages: 54 Appendices: 6

Abstract

There is an increasing need to hire skilled IT security professionals but organisations worldwide have a hard time to fill their vacant IT security positions. The constant demand for new IT security professionals and increased requirements in their skillset raises the need for know-how also among professional recruiters. These recruiters must find ways to identify and verify IT security recruits skillset during the recruitment process.

To uphold the IT security standards, organisations must make sure they use the best practices concerning IT security by hiring qualified persons. Many IT security certifications have been developed to help organisations to verify that the persons they hire have the needed IT security qualifications. This is why security certificates such as CISSP (Certified Information Systems Security Professional) are becoming increasingly important for IT professionals and recruiters. Certification provides a way to get validation of a person's IT security qualifications.

CISSP is a well-reputed IT security certificate; becoming a CISSP certificate person likely provides credibility on a resume when marketing IT security consultant or management services to organisations. This thesis studies the value, for both companies and employees, of the CISSP certificate developed by International Information Systems Security Certification Consortium (ISC)². The thesis sets out to investigate if there is value or benefits in acquiring CISSP certificate from two perspectives, the certificate holder's perspective and the recruiter's perspective.

The thesis also researches the contents of the CISSP certificate. It provides details on the CISSP certification content and covers the knowledge that must be learned to pass the

CISSP certification exam.

The thesis includes insights on the requirements and contents to be learned for the CISSP certificate. The thesis covers the CISSP certificate requirements for all eight different IT security knowledge domains defined by CISSP certification standards. In addition, as part of my empirical research, I participate in the CISSP certificate exam, try to become, a CISSP certificate holder.

Language: English Key words: Certificates, CISSP, Leadership, IT security

---

TABLE OF CONTENTS

APPENDICES

1 INTRODUCTION

Information is a key resource for most businesses today. Handling of data and keeping information secure is essential for growth, success and survival in almost any business (Doom 2010; 7). Many businesses and services are provided, to some extent, through the Internet; some businesses depend solely on the Internet to survive. Almost all aspects of any business are nowadays handled with computers connected to the Internet. Organisations are becoming more global, mobile, connected and dependent on information. This makes secure handling of information within an organisation more important than ever. Data and information in organisations around the globe have a lot of value and this value must be protected.

Over the last decades with the increased usage of IT systems, many IT security standards and best practices have been developed by various organisations to protect information from being intentionally or unintentionally exposed, leaked, stolen or destroyed. To uphold the IT security standards, organisations must make sure they use the best practices concerning IT security by hiring qualified persons. Many IT security certifications have been developed to help organisations to verify that the persons they hire have the needed IT security qualifications.

CISSP (Certified Information Systems Security Professional) is a security certification, which was developed by International Information Systems Security Certification Consortium, abbreviated as (ISC)² or ISC². The ISC² CISSP certification has become the de-facto standard for individuals pursuing a management role in information security. The CISSP certificate is a step for security professionals and managers, who are working towards a career in of security leadership, which is well received by organisations. Security positions such as Chief security officer (CSO), Chief information security officer (CISO) or Chief technology officer (CTO) are likely expected to have CISSP certification. (IT Governance Ltd 2016)

CISSP certification is often listed as a preference in many senior security positions for organisations and companies around the world. Security certification might even be required to fulfil government or organisation requirements for an information security mandate. (ISC², 2016). This especially applies to management positions. There has been some criticism, in the information security industry, that CISSP certificate does not really tell if a person is good at specific IT security tasks or not (Porup 2016). However,

commonly it has been accepted as a certificate with a high-standard of requirements. The CISSP certificates requirements, an extensive exam on IT security and risk management provide confirmation that a person has wide knowledge concerning IT security, which is a valuable asset for individuals in management and leadership positions.

1.1 Aim and research questions for the thesis

Organisations worldwide have a hard time to fill their vacant IT security positions. The technology company *Cisco Systems* estimates that there are 1 million IT security positions unfilled worldwide and demand of competent IT security personnel is growing (IEEE Cyber Security 2017). At the same time, IT security threats are getting more sophisticated every year, as more services are digitalized and automated at an increasing pace.

The aim of this thesis is to research the CISSP certification value for both IT security professionals and recruiters. The thesis will research CISSP certificate attractiveness, appreciation and value by CISSP holders and professional recruiters. The thesis sets out to investigate if there are values or benefits in acquiring CISSP certificate from two perspectives, the certificate holder's perspective and the recruiter's perspective.

The thesis will try to answer if CISSP accreditation adds value to IT security employees with the following research questions:

- Do IT security professionals and CISSP certificate holders feel that the certificate provides better job opportunities and salary?

- Do recruiters believe that CISSP certificates and/or IT certificates, in general, make potential recruitment candidates more attractive on the job market?

The target group for the thesis research, professional recruiters and another target group is CISSP certificate holders. This is to provide insights about certificate value from both a recruiter's and an employee's point of view. The *Figure 1: frame of reference* of this thesis, displays how CISSP certificate is tied to organisations and employees.

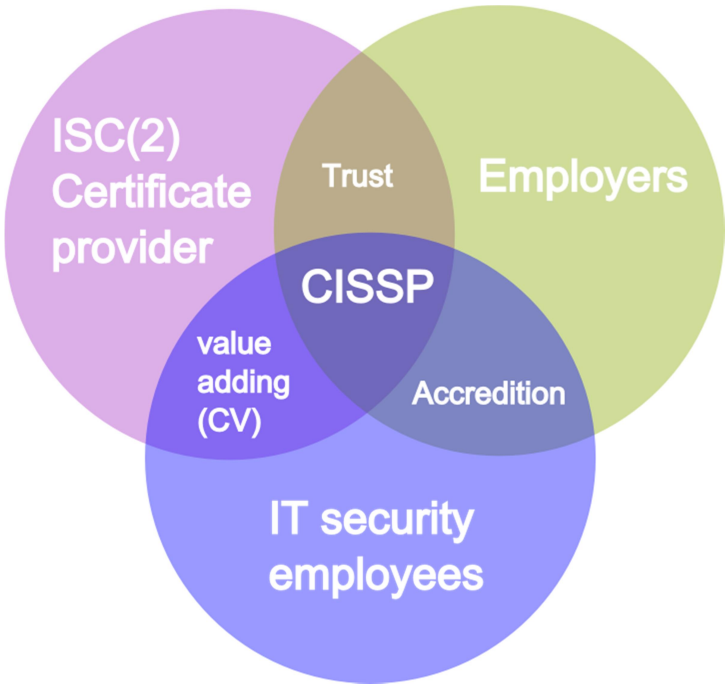

Figure 1: CISSP frame of reference

The thesis includes information about IT security industry practices and why cyber security is today more important than ever. The thesis includes a detailed description of the contents of a CISSP certificate in detail; the eight domains of CISSP Common Body of Knowledge (CBK). The CISSP CBKs are Security and risk management, Asset security, Security engineering, Communication and network security, Identity and access management, Security assessment and testing, Security operations and Software development security.

As part of the thesis, I will pursue a CISSP certification as required by my employer, a cybersecurity company. This thesis will describe the requirements and path to the certification in detail. I will participate in the CISSP certification exam and document the process. My employer pays the CISSP certification study materials and certification exam fee; however, this thesis itself is not commissioned.

1.2 Research methods and process

The main research methods are surveys among CISSP stakeholders and professional recruiters, with additional more in-depth interviews with the recruiters. The interviews

include both qualitative and quantitative questions about the attractiveness, appreciation and value of certifications for certificate holders as well as hiring organisations.

Research process:

1) Customer journey: CISSP self-studies, participating in the CISSP certification exam.
2) Study CISSP and IT security history and phenomena.
3) Gather target group contact details.
4) Prepare the CISSP and recruitment survey questions.
5) Distribute surveys.
6) Prepare in-depth-interview questions.
7) Interview some professional recruiters.
8) Analyse CISSP survey results.
9) Analyse recruiters' survey results.
10) Analyse data based on interviews.
11) Provide conclusion to this thesis based on findings.

1.3 Restrictions

This thesis focuses on CISSP certificate holders and its attractiveness to organisations. The ISC² organisation provides many other security certificates, which will not be covered in detail in this thesis. There will be some comparison with other management IT security certificates by other organisation than ISC² but the focus is on CISSP certification.

The thesis does not include information about other IT security certificates, such as Offensive Security Certified Professional (OSCP) or platform specific certificates such as Cisco Certified Network Associate (CCNA) Security certificate.

2 IT SECURITY MANAGEMENT AND LEADERSHIP

"Many executives are declaring cyber as the risk that will define our generation," according to Dennis Chesley, PricewaterhouseCoopers Global Risk Consulting Leader (PricewaterhouseCoopers 2016, 3).

Technology is constantly changing the way companies operate. These new technologies disrupt organisations and change the way a company creates value at an increasing pace. New IT, such as cloud computing makes company systems interconnected digital ecosystems more spread out than ever before. There are new challenges and threats emerging from all this interconnected technology according to PricewaterhouseCoopers (PwC), who follow up IT security issues on a yearly basis with their 'The Global State of Information Security'-report. PwC has noticed that cyber attacks against organisations continue to increase every year in frequency and severity. Unfortunately, most prevention and detection methods have proven to be ineffective against these attacks because organisation likely does not have the skills or resources to combat skilled cybercriminals (PricewaterhouseCoopers 2016, 2-3.)

According to PwC 'The Global State of Information Security Survey 2016' report, any IT security program must start with a strategy and a foundation. This is also the recommended way according to CISSP security and risk management domain, where it is emphasized that IT security should be led by a top-down model; where management drives the security program instead of the less effective way, bottom-up method, where staff members try to develop a security program by themselves (Harris 2016, 40.)

In an organisation, the most important information security officer is usually the Chief Information Security Officer (CISO) or Chief Security Officer (CSO). Requirements for the positions today require not only expertise in IT security but also knowledge in risk management, corporate governance and overall business objectives. He or she should have access to provide business risk insight directly to key executives of the organisation (PricewaterhouseCoopers 2016, 18.)

"Today's security leader is a general manager with expertise in communications, presentation and business—in short, all the skills you would expect of a COO," according to James Shira, Global CISO for PwC (PricewaterhouseCoopers 2016, 18.)

Figure 2: Skill and competencies of security leaders (PriceWaterhouseCoopers 2016)

As can be seen in figure 2 by PriceWaterhouseCoopers. only 43 percent of security leaders approach IT security as part of organisations risk management and communicate the IT risks directly to the executive leaders and only 35% update the organisation board frequently about the IT security.

The CISO and CSO are accountable to set IT security standards across the organisation and evaluate potential risks. This responsibility means that IT security risks should be reported to a leader that has a wide overview of both strategy and risk, such as the CEO (PricewaterhouseCoopers 2016, 18-19.)

PwC *'The Global State of Information Security Survey 2016'* reports that more Boards of Directors have started to address possible risks-oversights (e.g. strategic and financial risks) involving IT security. According to the survey, Board participation in IT security has helped improve security practices and increased the IT security budget for the organisations (PricewaterhouseCoopers 2016, 19.)

Based on the results, PwC has gathered from the survey; the amount of IT security threats has risen every year in the last decade. On the bright side, organisations have "woken up" to the risks it involves. Organisation managements have started to realise that they need to be more and more involved in managing IT security. This increases the demand for IT security management expertise, which can be verified for individuals with IT security certifications.

2.1 A short history of IT security

Today everyone in the world is using computers that are connected to each other over the Internet. The rise of communications technology has also "given birth" to computer-related risks and security issues. IT security is about securing your computing assets from malicious threats and risk and process management.

This chapter describes a brief history of technical IT security, describing how various techniques were developed over time to take advantage of networked IT systems without the owner's consent. These techniques fuelled the development of IT security countermeasures and it has been a "cat-and-mouse" game ever since, with one "side", a malicious threat actor, trying to take advantage of IT systems and security process weaknesses of an organisation or a user's systems. The other "side" is the system owner, trying to prevent systems from being compromised.

2.1.1 The rise of digital communication

During the 1970s and the invention of digital communication methods, there were cases of users trying and succeeding to circumvent the phone communication billing systems to be able to do phone calls for free. This is called known as *phreaking*. These are some of the first known IT system security threats.

Next decade, in the 1980s, home computers were starting to get a foot in some households and computer clubs were created around the world. In 1986, the first known computer virus, Brain, was created. The virus was non-destructive and harmless, but it started a new era of security measures. There were also some notable cases in individuals hacking telephone networks, using the phone lines to their advantage in further system cracking attempts (SC Media 2009.)

2.1.2 Modern IT security era

The 1990s was the dawn of modern IT security industry, boosted by the rise of the Internet and the World Wide Web in 1995. Computer viruses and malware were spreading faster than ever before. Internet worms and other methods for spreading viruses over the internet

forced new IT security companies to form. New technologies were created and implemented to protect companies and individual assets. New technologies, such as firewalls, anti-virus protection, regular patching of software and other protection methods were introduced to the world of IT security (SC Media 2009.)

At the shift of the millennium, IT security became more crucial than ever. As many services, both private and governmental switched to make their IT services available through the Internet. Internet services provided easy access and convenient service for users, but also opened the systems up for potential abuse over the network. Together with the rise of internet advertisement, it helped the rise of cybercriminals, trying to make money in many ways by taking advantage of Internet users and companies providing services over the internet. Major criminal enterprises try to make money by abusing technology flaws online. They can use extortion of user and companies of their IT asset, defrauding advertisements for click-through's, which earn them money from legitimate advertisers among other techniques. Because the profits that criminals can make are big, they have become a big challenge for IT security companies to help protect organisations from cyber attacks (SC Media 2009.)

2.1.3 The present and the future

Today IT security measures and IT security threats are part of our everyday lives. There are ransomware attacks, holding users computers for ransom. Cryptocurrency attacks, using users' computers resources for mining Cryptocurrency such as Bitcoin, without users consent. There are various botnets on the internet, a collection of internet users devices unknowingly under control of a malicious actor. The malicious botnet owners can use millions of computers under control their control to extort organisations and companies for money, by threating to cause a Denial-of-service attack (DDOS) on the businesses that are depending on online functions, such as banks and the gaming industry (Akamai 2017.)

Another threat on the rise (or at least the awareness of it) are governmental interest in, monitoring (or spying) on internet traffic of other nations, do politically motivated cyber attacks and trying to control internet connection points in case of cyber warfare. "Nation-state attackers typically go after political targets: the Democratic National Committee, government agencies, critical infrastructure, and defence contractors. It's become

increasingly clear that any company, in any industry, could be affected, either as a result of being a deliberate target or as collateral damage in a wider attack" (CSO online 2018.)

What the future of IT security holds is, of course, uncertain, but the risks are not going away. On the contrary, every day more devices connect to the internet, and more devices connected are affecting our everyday lives. IoT (Internet of Things) devices are smart devices controlling many functions in the household; cars are getting smarter in navigation and autonomy of driving. All these are systems that are potentially open to abuse by malicious attackers. Abusing these systems might put humans at risk in real-life, e.g. if house thermostats and security systems are tempered with, without consent. Due to this IT security industry is calling out for IoT security standards (CSO online 2017.)

Today security threats are so advanced that many organisations have a separate Security Operations Centre (SOC) that monitors and acts on security threats. The SOC continuously monitors organisations assets, trying to find abnormalities in network traffic or system logs, which they investigate and classify. Many parts of this monitoring are automated using a Security Information and Event Management system (SIEM) to highlight events using pre-defined, continuously developed, offence rules (Vijayan, 2018.)

This infrastructure is also spreading more rapidly outside an organisations' borders, with the rapid adaption of cloud services; services providing infrastructure over the internet to provide global flexibility for services, this is in contrast to a traditional organisation using self-owned datacentre services. All this new technology put more demand on IT security controls. The need for risk management and IT security is seen to be more important than ever before, as IT systems are controlling most of the world's infrastructure at an increasing pace (CSO online 2017.)

2.2 IT security fundamentals

The main objective of IT security is to provide availability, integrity and confidentiality protection to important organisation assets. This is referred to as the AIC triad (or CIA triad) in CISSP study materials. AIC is often accepted as the de-facto security principles of IT security. As every security objective (asset), an organisation has its own security requirements and requires different levels of protection, the protection is provided using mechanisms, safeguards and security controls for all areas of AIC triad. Any security risks,

vulnerabilities and threats are measured for their capability to compromise one or many of the AIC principles to evaluate their potential danger (Harris 2015, 3.)

Availability ensures that the assets' resources are available and possible to access when needed without unnecessary delays in a predictable manner. The assets should be able to recover quickly from any disruptions so that productivity is not affected (Harris 2015, 3-4.)

Integrity is an assurance that the information and platform are provided without any unauthorised modification. Integrity means that the users can be assured that the asset the system is providing is free of any deliberate on un-deliberate unauthorised modification (Harris 2015, 4.)

Confidentiality provides assurance that the information remains undisclosed for unauthorised individuals. The level of secrecy should apply during the whole life cycle of the data even if it is stored, moved or archived. As longs as the classification of the data status has not changed, the level of exposure should not either (Harris 2015, 5.)

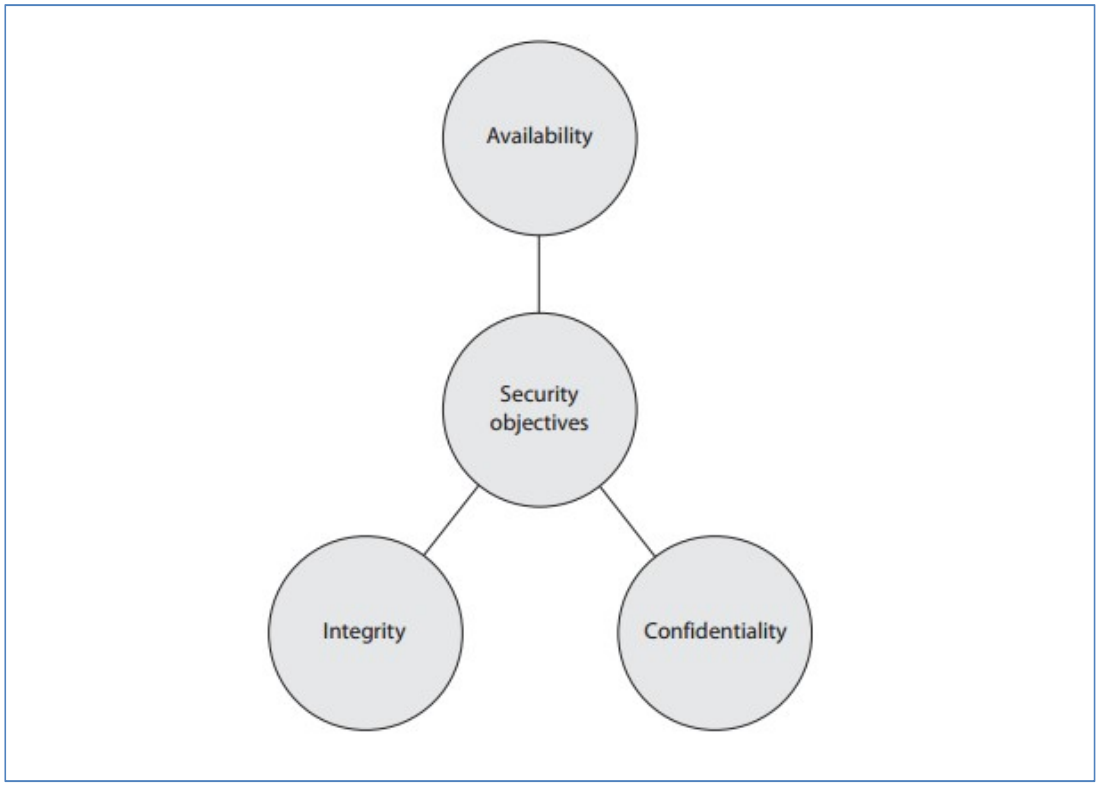

Figure 3: AIC triad diagram (Harris 2015, 3)

AIC is not the only security principles to follow in IT security. There are other security-related principles to be considered when creating a security policy or security plan (ISC² 2015, 51, 53.)

One widely used security principle is the principle of IAAA (Identification, Authentication, Authorization, Auditing and Accounting). IAAA principle defines the baseline for identifying individuals and makes sure they are how they claim to be, have the proper rights administered. The claim is validated through auditing and the individual's trace is non-repudiated. This process is abbreviated as either three letters: AAA or four letters: IAAA, but the principle actually consists of five elements: Identification, Authentication, Authorization, Auditing and Accounting. IAAA is a five-step process where the step must be validated in correct order for the process to be able to proceed as seen in Figure 3 (ISC² 2015, 51-53.)

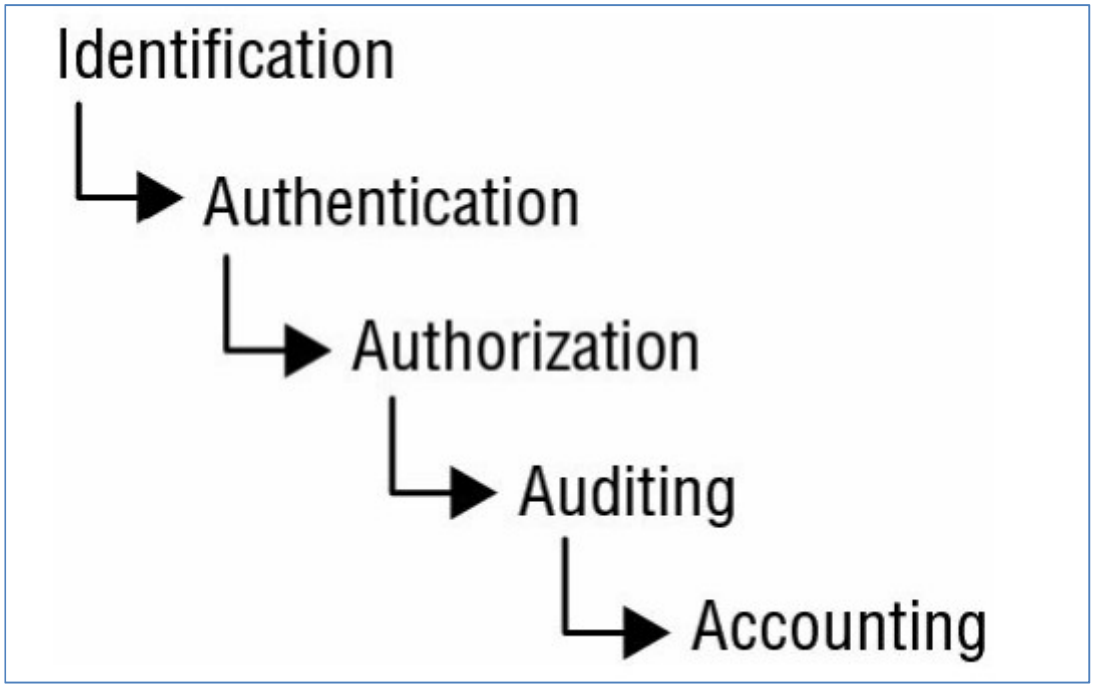

Figure 4: The five elements of IAAA services (ISC² 2015, 51)

Identification is the first step a subject must follow to identify itself, and it is the start of the Authentication, Authorization and Auditing process. Identification can be provided in many ways; it can be a login to a system using a username and password or it can be an individual showing his/her organisation security badge to a security guard. The credentials the subject is using to identify itself provided with the required resource for that specific situation (ISC² 2015, 51-52.)

Authentication verifies if the subject is who it claims to be and the identification is valid. This happens for example when a password is validated by a system during login process or when a security guard verifies that the security badge picture matches the individual presenting it. It must be considered that if others can obtain and/or counterfeit the authentication factor relatively easy, then the authentication process is insecure. Identification and authentication always form together a two-step process; first, the subject provides identification and secondly the authorization is verified. Should any of these two steps fail, the individual should not gain access to proceed further (ISC² 2015, 52.)

Authorization can be provided once the subject has gone through the identification-authentication process. The authorization process ensures that the subject has the proper rights and privileges to assigned resources in place. The identification-authentication process is an all-or-nothing concept where the subject is granted either access or not, the authorization process is resource based. For example, the authorization process might classify the subject so that it can only access a specific set of folders in a system or the individual might have gained access to the whole building except the financial department (ISC² 2015, 53.)

Auditing means that a subject's actions are monitored, recorded and analysed to maintain the environment and all its resources in operation. Everything a subject is doing in an environment should be recorded and attached to the identification. This creates an audit trail where the environment owners can follow-up subjects and their actions. These audit trail logs can then be used to improve the system or find anomalies that will help then environment operators to improve the system stability and security. For example, if an individual tries to log in to a system (whether it fails or succeeds) or a system crashes for any reason, the system should produce logs of everything that has happened. Also, physical controls, such as CCTV video surveillance systems recordings can be used as an audit trail to follow a subject (ISC² 2015, 54.)

Accountability must be maintained if an organisation wants to be able to enforce their security policies. Security can only be maintained if an individual can be held accountable for their actions. Linking an individual’s actions and identity through security mechanism of IAAA is a way to achieve accountability. However, accountability is heavily dependent on the authentication process; if the authentication measure is weak, the accountability of the individual will be in doubt. Nonrepudiation is essential for accountability. The result of the completed IAAA process is to ensure that the individual cannot deny that their

performed action took place. An individual that can repudiate the claim of their participation in an event, because of "holes" in the security measures, cannot be held accountable for the action (ISC² 2015, 54-55.)

2.3 Organisation security program

Every organisation exists for a specific reason, a business' purpose is to make a profit for the owner, a publicly traded company's goals is to increase shareholder value, a non-profit organisation goal is to further the causes of what it supports and government organisation provide services for their citizens. Security can therefore not stand in the way of the organisation business processes, but should be implemented to make them better (Harris 2015, 30.)

Security management planning ensures that the security functions are aligned with the organisation strategy, goals and objectives. This is achieved by including creation, implementation and enforcement of the security policy planning. A business case is needed to justify an investment, especially if the project is related to security. Security is essential in long-term for any organisation but can be expensive to uphold. Organisations have limited resources, people, technology and money; therefore, it is important to find a balance between costs and benefits. The business case for security measures can be calculated using organisation risk management tools covered in one of the CISSP domain: Security and risk management (ISC² 2015, 57-58.)

In any organisation, all core businesses must be integrated into a standards-based security model with specified risk tolerance criteria. Risk tolerance is the balance between functionality and security, e.g. allowing personnel to work from home saves office space, but opens up some risk when opening up connections from home office to the company network. Here the potential risk is calculated in comparison to the benefit of the new working method. Security should help the organisation become more effective by enabling the organisation to do new things safely (Harris 2015, 31.)

The top-down model is the preferred security program approach. Top-down means that the initiative, direction and support of a security program should come from organisation leadership and go through all management layers down to the staff members. A bottom-up

method, where staff members initiate the security programs, is usually less effective because it is rarely broad enough to consider all security risks (Harris 2015, 40.)

Defining security roles, selecting the responsible for organisation security, planning how security is managed and tested, creating security policies, doing risk analysis and making sure the organisation staff is trained in security are the essentials of security management. Most of this, however, is useless without senior management approval. Ultimately, senior management is responsible for the overall security of an organisation. Security is considered a business operations issue, not an IT administrative issue. The team or department responsible for security should be led by a CSO that reports directly to company leadership. The security team should be an autonomous part of the organisation (ISC² 2015, 58.)

2.4 Organisational security policy

Security policies are general statements created by an organisations' senior management or alternatively by a policy committee or policy board. The organisational security policy provides direction and scope for every security-related activity within the organisation. In an organisational security policy, the organisation leaders establish how the organisation security program will be set up. The policy establishes the security program's goals, displays the strategic value of IT security, assign responsibilities and define how the program should be enforced. The organisational security policy should include how to satisfy local related laws, regulations and liability issues. It should also include a description of how much risk the leadership is willing to take (Harris 2016, 86.)

Important characteristics of an organisational security policy are that business should drive the implementation of the policy, business goals come first. The policy should be developed in an easily understandable format so that it integrates security into all business functions of the organisation. The policy should be reviewed regularly and changed as the organisation changes. It should also support all possibly required legislation and regulations required by authorities. The organisational security policy and any additional security policy defined within an organisation should be implemented with the help of standards, guidelines and procedures (Harris 2016, 87-93.)

Standards are defined as mandatory activities and rules that must be enforced to be effective. A standard could be a rule that e.g. require all members to wear their ID badge visibly when at the organisation office (Harris 2016, 87-93.)

Guidelines are recommended actions, operational guides and a general approach for members when a specific standard does not apply. A member of an organisation and refer to a guideline for guidance when dealing with undefined "grey areas" or unforeseen circumstances (Harris 2016, 87-93.)

Procedures are well-defined tasks with systematic instructions to achieve a certain goal. Procedures instruct how the policies, standards and guidelines are implemented into the organisations operating environment (Harris 2016, 87-93.)

2.5 IT security certificate providers

There are many organisations, companies and associations providing IT security certifications, this section list some globally known IT security certification and education providers.

2.5.1 SANS Institute

The SANS Institute (officially named the Escal Institute of Advanced Technologies) is a private U.S. for-profit company founded in 1989. SANS Institute specializes in information security and cybersecurity training. SANS Institute has a certification program called *Global Information Assurance Certification* (GIAC), this is an information security certification entity that specialises in technical and practical certifications in security administration, audit, management, software, forensics, and legal domains. As of writing this thesis, SANS Institute has 27 different active certificates available in their programs. (GIAC 2017)

2.5.2 ISACA

ISACA founded in 1969, is an association also known as the *Information Systems Audit and Control Association.* The association is known for major publications about audits, IT risk and IT security procedures and best practices (ISACA 2017.)

ISACA provide following certificates:

- Certified Information Systems Auditor (CISA)
- Certified Information Security Manager (CISM)
- Certified in the Governance of Enterprise IT (CGEIT)
- Control Objectives for Information and Related Technology (COBIT)
- Certified in Risk and Information Systems Control (CRISC)
- Cybersecurity Nexus Practitioner (CSX-P)

2.5.3 EITCI institute

EITCI (European Information Technologies Certification Institute) is an international non-profit organisation founded in 2008. The organisation has many IT certification programmes under their brand EITCA (European Information Technologies Certification Academy). There are many different EITCA certification programs, each focusing on a different IT area. EITCA/IS (EITCA Information Technologies Security Academy) is the certification program providing IT security certificates (EITCI 2017.)

2.5.4 ISC²

Founded in 1988, the International Information System Security Certification Consortium also known as ISC² is a non-profit organisation. ISC² specialises in IT security certificates and education. The organisation provides a wide range of IT security certificates; including CISSP certificate, which is one of the most known IT security certificates and the focus of this thesis when researching its value to the individual certificate holder (ISC² 2017.)

ISC² provide following certifications:

- Certified Information Systems Security Professional (CISSP), including additions:
    - Information Systems Security Architecture Professional (CISSP-ISSAP)
    - Information Systems Security Engineering Professional (CISSP-ISSEP)
    - Information Systems Security Management Professional (CISSP-ISSMP)
- Certified Secure Software Lifecycle Professional (CSSLP)
- Certified Authorization Professional (CAP)
- Certified Cloud Security Professional (CCSP)
- Systems Security Certified Practitioner (SSCP)
- HealthCare Information Security and Privacy Practitioner (HCISPP)
- Certified Cyber Forensics Professional (CCFP)

3 CISSP CERTIFICATE

This chapter describes the contents of CISSP certificate studies and contents of the eight domains of CISSP certificates. CISSP certification accreditation sub-chapter describes the additional requirements of CISSP certification, how the CISSP certificate exam is structured and how to upkeep the certificate once the certificate was successfully acquired. It also gives an insight into study materials available for the certification exam. A detailed content list of the CISSP certificate exam with domain weight (proportion percentage of CISSP domains in certificate exam evaluation), is presented in appendix 6.

3.1 CISSP domains

The CISSP certificate domains (also known as CISSP CBKs) are: ‘Security and risk management’, ’Asset security’, ‘Security engineering’, ‘Communication and network

security', 'Identity and access management', 'Security assessment and testing', 'Security operations' and 'Software development security'. This is the core of the certificate and a person must have knowledge of all domains to pass the certification exam.

3.1.1 Security and risk management

CISSP security and risk management domain is the foundation for a proactive risk and security program for any organisation. The domain explains policies, frameworks, principles, concepts, standards and structures in managing an organisation's risks and security. It also explains the link between business objectives and information technology, which is becoming more important than ever in today's society, as information is the most important asset a company has. The security and risk management domain teaches how to upkeep IT security with administrative, technical or physical security controls to protect integrity, availability and confidentiality (AIC), of organisation assets. This is done with help of policies, procedures, standards, baselines and guides, to establish threat modelling, best practices, compliance and security awareness in an organisation (Gordon 2015, 29.)

The domains' risk management part encompasses security reviews, risk analysis, cost-benefit analysis, management decision making, on-going review and safeguards evaluation, analysis and implementation. Understanding justice systems and different laws is a big part of security management. Risk management is a tool for organisation leadership to make informed decisions using risk-managing principles of risk avoidance, risk transfer, risk mitigation and risk acceptance. CISSP security and risk management domain provide insight into enterprise-wide business continuity (BC) and risk management areas such as operational risk management, physical security, financial risk management, audits and compliance with laws and regulations (Gordon 2015, 30.)

3.1.2 Asset security

The asset security domain is about monitoring and securing organisation assets using security principles, concepts, standards and structures to upkeep availability, integrity and confidentiality (AIC). This should be done in line with the risk and security controls

described in the security and risk management chapter. Asset security focuses on control and protection the organisation assets such as personnel, information and tangible assets (Gordon 2015, 268.)

The domain describes how to classify information and how data should be managed and "owned" correctly. The domain explains methods to protect organisation assets and how to handle important data during the assets life cycle (Gordon 2015, 269-270.)

3.1.3 Security engineering

The security engineering domain provides knowledge about IT security design principles, fundamental concepts in IT security models, controls and countermeasures based on security standards and how to assess, mitigate vulnerabilities in security architectures and design. It also helps understanding principles cryptography, (physical) facilities design and site protection (Gordon 2015, 354.)

The domain focuses on systems at both individual IT system level protection and enterprise security architecture (ESA). It explains all phases of a computing system, and how to keep the computing system secure through its life cycle by identifying the modern system building blocks and characteristics that distinguish systems from each other (Gordon 2015, 355-356.)

3.1.4 Communication and network security

Communication and network security domain provide information on how to upkeep availability, integrity and confidentiality of public and private communication channels and media. The network is one of the most important assets in IT security and the domain covers network security measures, structures, transmission methods and formats. The domain explains how to proactively build security controls and countermeasures to keep communication channels safe in an organisation (Gordon 2015, 612.)

The Communication and network security domain cover IT networking in detail, including all layers the Open System Interconnect (OSI) model and the most commonly used transmission protocols such as Transmission Control Protocol/Internet Protocol (TCP/IP).

The domain also focuses on securing resources and controlling risks with monitoring network performance and security. It covers common network attacks and methods to prevent them from occurring (Gordon 2015, 613.)

3.1.5 Identity and access management

Access control mechanisms, processes and techniques help protect the assets of an organisation. The identity and access management domain cover all types of access management on all levels in an organisation. Including access and identity control knowledge about personnel, facilities, support and information systems. This domain covers how to:

- Specify which users can access a system or facility.
- Specify what resources those users can access.
- Specify what operations those users can perform.
- Enforce accountability for those users' actions.

(Gordon 2015, 836-837)

Managing both physical and electronic access, together with the user identification, is essential to keep the organisation secure and its assets safe. Proper identity and access management protect availability, integrity and confidentiality of the company assets in a way so that the protected asset is only available to those with proper rights when needed, all access can be audited and it is ensured that the asset has remained unchanged and undamaged by unauthorized entities (Gordon 2015, 836-838.)

3.1.6 Security assessment and testing

"Security Assessment and Testing cover a broad range of ongoing and point-of-time based testing methods used to determine vulnerabilities and associated risk. Mature system development life cycles include security testing and assessment as part of the development, operations, and disposition phases of a system's life" (Gordon 2015, 968.)

The security assessment and testing domain provides knowledge for system development lifecycles and managing the security risk when developing and maintaining IT systems using different testing and evaluation methods. These testing and evaluation methods are used to secure and improve the systems by helping to find flaws and taking quick corrective actions when needed during the systems life cycle. This domain covers a wide area of methods to improve security, including vulnerability and penetration testing, log reviews, misuse cases, and code review methods. This helps to identify critical capabilities so that the risks the flaws pose can be identified, managed or mitigated. The security assessment and testing domain provides knowledge how to gather data and Key Performance Indicators (KPIs) for security reviews, processing and auditing. The domain also describes how to use the gathered data to improve security awareness, improve disaster recovery and business continuity in an organisation (Gordon 2015, 969-971.)

3.1.7 Security operations

The security operations domain covers a wide area of security. It handles crime scenes, evidence collection, handling, investigation, forensic techniques, incident response, and resource protection techniques. It outlines the foundational security operations concepts together with change management, business continuity planning, and disaster recovery strategies. The security operations domain includes both physical site security and information security (Gordon 2015, 1028-1029.)

The security operations domain helps to prepare for any threats and disasters that can occur in an organisation, both physical and non-physical. Security operations handle daily routine tasks to keep an organisation and its services running. A primary goal of security operations is to protect the organisation's critical assets and have a plan for any operational anomalies that might occur. Well designed and maintained security operations, gets an organisation restored to normal after an incident or disaster in a timely manner (Gordon 2015, 1028.)

3.1.8 Software development security

Many security vulnerabilities today are found in software running an organisations systems and services. Many security measures are focused on system-level protection and access

control. Today software development security plays a bigger role than ever before in software development (Gordon 2015, 1244.)

The software development security domain covers all part of secure software development, including, development life cycle, maturity models, maintenance, operation and change control. It outlines the used security controls for software development tools and goes through best practices for software development auditing, reviews, risk analysis, risk mitigation and acceptance testing. The domain also includes the process of software acquisition and review in a secure manner (Gordon 2015, 1246.)

3.2 CISSP certification accreditation

This subsection outlines the needed requirements for CISSP certificate, ways of studying for the exam, the exam outlines and once the certificate has been acquired, and how one can maintain an active CISSP certificate status.

3.2.1 Certificate requirements and the exam

Becoming an active CISSP certificate holder requires more than passing the certification exam. There are four distinct phases to becoming a CISSP certificate holder:

- You must meet the education or work experience requirements.
- You must pass the exam.
- An active CISSP certificate holder must endorse you.
- You should be prepared for an audit of these requirements.

(Warner 2010)

To qualify for education or work experience, a CISSP certificate applicant must have five years of work experience in at least two different CISSP domains (CBKs). Four years of work experience is enough if you have a relevant four-year college degree or other approved credits from ISC^2 (the CISSP certificate provider) (ISC² II 2017.)

The CISSP exam fee as of writing this thesis is 599,00 US dollars, this must be paid to attend the exam and the participant must pay the fee each time they try to make the CISSP certification exam. The CISSP certificate exam is passed if the participant scores 700 out of 1000 points. The exam has 250 questions and includes a mix of *multiple-choice*, *drag-and-drop* and *hotspot questions* (Tittel 2016.)

In *multiple-choice* questions, the exam taker selects the right answers out of usually four answers. Only one answer is correct, and the answer options might be very similar with subtle differences. Usually, the correct answer is not providing technical solutions but a more high-level IT security answer. In the exam, the participant should consider them in a security advisor role with more high-level advice (Tittel 2016.)

Drag-and-drop questions require an exam participant to match different topics and answers together or arrange lists in right order, e.g. re-arranging stages of a security model in correct order. Here you must move all correct answers to the right side to pass the question as shown in figure 5.

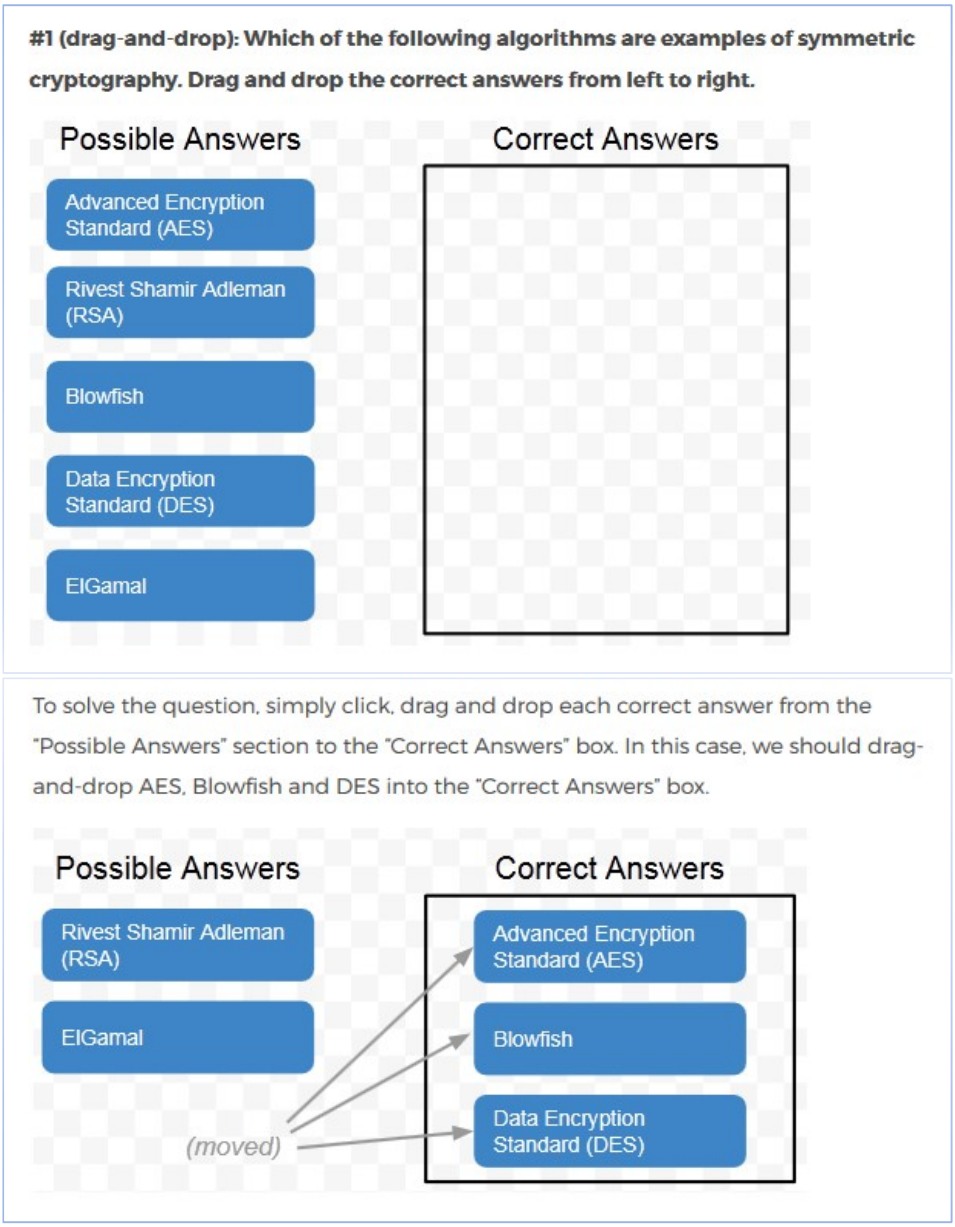

Figure 5: A CISSP exam drag-and-drop question example. (Infosec Institute, 2017)

Hotspot questions display one or more pictures together with a description, in these questions the exam participant must select with the computer mouse and mark the correct area of the picture based on the description text of the question, as shown in figure 6.

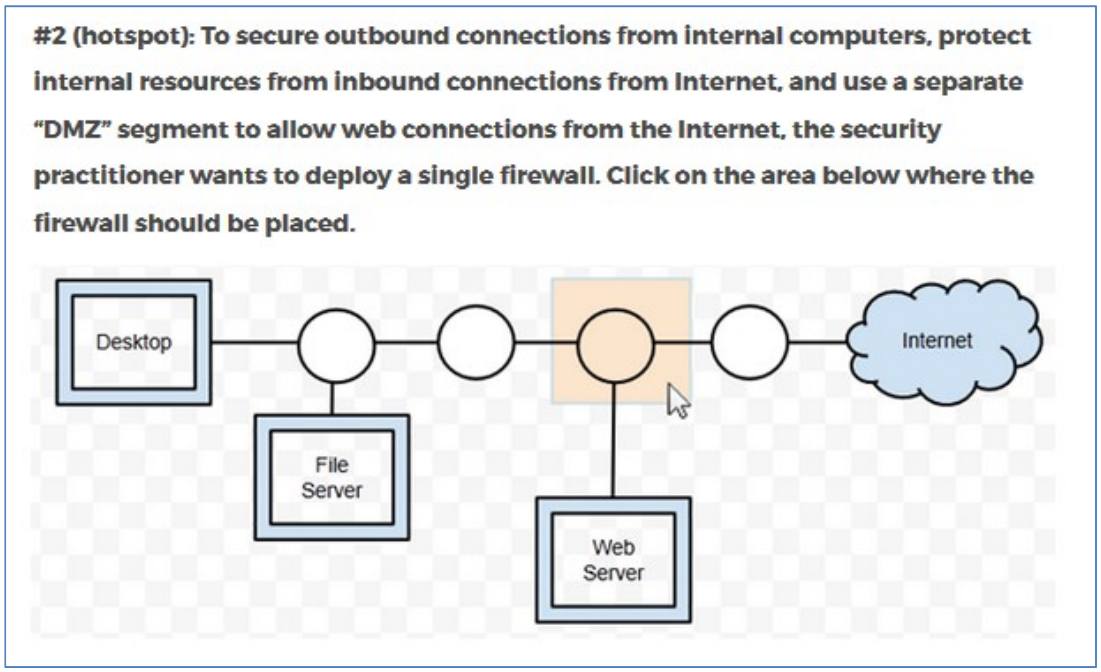

Figure 6: A CISSP exam hotspot question example. (Infosec Institute 2017)

Out of 250 questions, 25 of the exam questions are control questions not providing any points. Control questions are presumably used by the certificate provider to verify that a participant knows the subjects and is not relying on luck (or cheating). Exam points are not equally distributed among the questions, some questions give more points than others are, the values of the questions are not displayed in the exam (Tittel 2016.)

Information on how CISSP exam questions are weighted between different CISSP domains is public information and can be found in ISC^2 institute website (appendix 6). Security and risk management is the most important domain in the exam with a weight of 15% of the exam questions, while the rest of the exam domains have a weight between 10-14 percentages (ISC² IV 2017.)

The exam is taken in a controlled environment, using a computer in an ISC^2 institute partner site. A participant has six hours to complete the exam, on-site breaks are allowed but leaving the exam area is not allowed during the exam. In addition, exam time is not paused during the break time used, the six hours includes and breaks the participant might take.

Once (or if) the exam is passed and experience requirements are met, the participant can apply for a CISSP certificate, however, the application must include an endorsement from an active CISSP certificate holder. If this is included together with the rest of the

requirements, the participant will get active CISSP certificate status. ISC², the CISSP certificate provider organisation, randomly selects CISSP applicants for audits, when applying for a CISSP certificate; each applicant must be prepared to provide additional data supporting their application (Warner 2010.)

3.2.2 Studying and preparing for the CISSP certificate exam

There are multiple ways to prepare for the CISSP certificate exam. ISC² institute provides a detailed outline of the certificate content (appendix 6) and there are multiple official (provided by ISC² institute) and unofficial books designed for exam studies, as well as both computer and mobile applications with mock-up CISSP exam tests to practice one's abilities before a real CISSP certificate exam.

There are many organisations providing CISSP certification training courses, both live classroom courses and online courses. Usually, the classroom courses come with a high price compared to the online courses or self-study CISSP study material and exam costs (Tittel 2016.)

I created a customer journey map (figure 7) to visualise the journey to CISSP certification from a user's perspective.

- *Green/red boxes* are the numbered touchpoints,
- *blue clouds* the user's thoughts during the touchpoint,
- *grey arrows* describe the path,
- *yellow boxes* are the tools, services or environment encountered by the users.

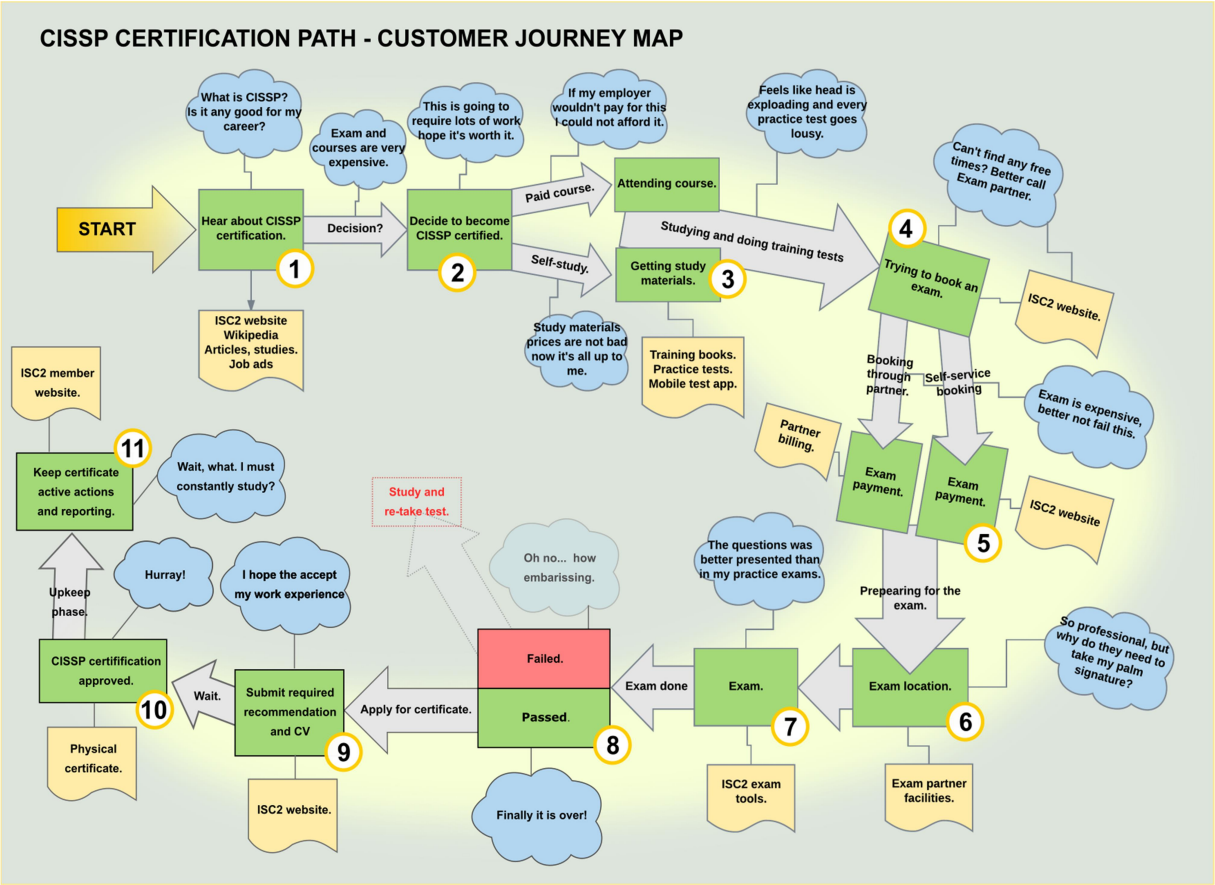

Figure 7: A customer journey map to CISSP certification.

There are 11 identified touchpoints in the CISSP certification customer journey map:

1) Hearing about CISSP certification.
2) Decide to persuade CISSP certification.
3) Starting to study; either as self-learning or through a course.
4) Booking exam to CISSP certification test.
5) Pay CISSP certification exam fee.
6) Arriving at exam location.
7) Take CISSP certification exam.
8) Exam result: passed or failed.

9) If exam passed and all certification requirements are met, apply for certification.

10) Receive CISSP certification approval.

11) Maintaining the CISSP certification active by reporting activities to ISC^2.

This *customer journey map* was built on my own experience when I passed the certification exam and full-filled the rest of needed qualifications to get CISSP certificated. I managed to get the CISSP certificate in May 2017. The customer journey was improved and revised using information received from other CISSP certificate holders through interviews.

3.2.3 Keeping the certificate active

Once CISSP certificate is acquired, it has a three-year lifespan. During the three-year period, a certificate holder must collect at least 120 continuing professional education (CPE) credits (40 CPEs / year). There are two types of CPE credits:

- Type A, security and CISSP CBK related.
- Type B, development of other professional skills.

(Warner 2010)

These CPEs are earned by attending seminars, fairs, reading security books, white papers, articles and publications. Listening to web- or podcasts, taking training or academic courses will also count for CPE credits. All activity is self-reported through ISC² member website and the CPE credit reports can randomly be selected for auditing by ISC² organisation (ISC² III 2017.)

Additionally, to collecting CPEs, there is a yearly fee for keeping the CISSP certificate active, as of writing this thesis the yearly fee is 85,00 US dollars each year, excluding the first year the exam was taken (ISC² III 2017.)

4 RESEARCH: CISSP VALUE AND RECOGNITION

This section describes the CISSP certificate value and recognition research methods and results. It explains the theory behind the research and tries to display results in an objective but visual manner. This section displays individual results from individual methods. The combined research results and conclusions in this thesis are later presented in the separate conclusion chapter.

4.1 Target groups

One target group for this research are CISSP holders and IT security professionals, the other target group is recruiting professionals and people involved in organisations recruitment process. Target group CISSP holders and IT security professionals represent the employees' perspective and the research focus on how they individually experience IT certifications and specifically CISSP value and recognition among companies or organisations.

The other target group, recruiting professionals and other people involved recruiting processes to represent the employer's point-of-view regarding IT security certifications and certifications in general.

4.2 Research methods theory

This section describes the research methods used in this thesis and the theory behind them. The research methods for this thesis are interviews, surveys and a CISSP certification path customer journeys.

4.2.1 Surveys

Surveys are used to do market and social research for respondents' opinions and experiences. It is a common way to gather insights on almost any subject. Surveys gather

data from respondents; the data is analysed to draw a conclusion or to support further research. Getting valid data from surveys requires reduction of four distinct types of errors. The types of errors are *coverage error, sampling error, non-response* error and *measurement error* (Boussalis 2012, 2.)

Coverage error happens when a survey group included differs too much from rest of the population the survey is trying to inference. This can be avoided by making sure that the survey sample group is part of the focus group defined, the survey is available for all participants and unit duplication is taken into consideration to avoid double counting of opinions (Boussalis 2012, 5.)

Sampling error happens when the size of the sample is not in proportion to the sampled population. This lack of proper sample increases the margin of error in the results (Boussalis 2012, 6.)

Non-response error can arise if there is a specific target group selected for the survey and not large enough sample answers the survey. This might cause that, those who answered have a different opinion than those that decided not to participate. Motivating respondents to answer is a good way to reduce non-response error (Boussalis 2012, 7.)

Measurement error can happen because of inaccurate answers due to poor survey questions or design. Question format is an important factor limiting measurement errors (Boussalis 2012, 8.)

Survey questions can be divided into the following groups: *Open-ended, close-ended* and *partially closed*. Open-ended questions give the respondents a chance to freely write an answer. Open-ended questions are harder to make statistics of but enable respondents more freedom to be creative. Close-ended questions give respondents different choices but no room for creativity. These types of questions are easier to analyse statistically. Partially closed questions, provide pre-defined answers but also give the respondent a possibility to add one's own answer to the question. As with open-ended questions, this makes it harder for the survey creator to analyse and compare the results (Boussalis 2012, 8-11.)

There are many ways of distributing surveys, but they can be divided into two distinct categories: physical and electronic (online).

The physical distribution methods would be:

- Physical on-site delivery/interview.
- Through postal mail delivery.
- Feedback “boxes” with physical papers at events, conferences and fairs.

The disadvantages of a physical delivery are higher costs, more work and limited delivery methods. Providing a physically printed survey will likely cost more to produce (e.g. photocopying) compared providing one through the internet because the results are written on a paper it requires more work to digitalize the results for analysing on a computer. In addition, there are more geographical restrictions on providing a physical survey than an electronic one (Hohwü 2013.)

If the surveys are delivered personally on paper or are conducted through an interview, the respondents might take this physical survey more seriously than an electronic one. Today, especially in social media, people are constantly “bombarded” with online surveys; this makes people numb to them and they are likely unwilling to participate in any. Physical survey forms might also be easier to fill in with a pen at events such as conferences while listening to the event when you have the paper in front of you; compared to trying to remember to go to a website the do the survey “when you have time” during the event.

While the above chapter’s statements about surveys are based on my own experience in arranging and participating in surveys, they are just my personal experience and opinion. A recent study called, ‘*Web-Based Versus Traditional Paper Questionnaires: A Mixed-Mode Survey With a Nordic Perspective’,* has concluded that both traditional physical paper surveys and online surveys have comparable participation results (Hohwü 2013.)

The electronic methods would be surveys delivered:

- Online (internet)
- Survey kiosks

There are many advantages of online surveys compared to physical surveys. They are usually cheap to set up. The results are instantly stored in a digital format. Results can be quickly analysed and spread through various methods such as social media, e-mails, websites and online advertisements. You can easily spread the questionnaire over a worldwide area. As the Lena Hohwü et al. study shows, the web-based questionnaires

could replace traditional paper questionnaires, because they have comparable response rates and lower costs compared to traditional physical surveys.

Survey kiosks is an electronic method but a hybrid version. While kiosks provide the ease of data gathering and analyses. They require physical access and are an effective method for respondents to answer surveys at events that respondents are attending physically. Survey kiosks are highly visible and easy to use, encouraging respondents to share their opinions. They have an advantage in capturing in-the-moment feedback at events of an on-site target group (Pilon 2017.)

4.2.2 Interviews: structured, unstructured and one-to-one

Interviews are a common research method. An interview is a conversation, with one or many persons, where questions are asked to retrieve information about a subject of study.

Interviews are a method to:

- collect respondents' point of view of a subject,
- understand likes and dislikes,
- collecting stories and insights on a subject.

Using the interview method requires the respondent's permission to store and/or record the information, this requires usually to make a confidentiality agreement with the respondent and e.g. agree to anonymize the answers before publication (Curedale 2013, 174.)

Structured interviews follow a prepared script with a set of pre-defined questions, while unstructured interviews can modify questions during the interview. Structured interviews make it easier to analyse the results and suit well for quantitative research. However, it might be harder to get the respondent to discuss sensitive topics and structured interviews give no possibility to answer context related follow-up questions as it's important for the researcher to follow the script exactly and keep a consistent behaviour for each respondent (Curedale 2013, 188-189.)

Unstructured interviews provide the researcher with more options to modify the structure and questions of the interview. It is the preferred interview method to discuss sensitive

topics with the respondent, as it gives the researcher the possibility to react to received answers with follow-up questions and emotional response. Using unstructured interviews make it impossible for a researcher to stay completely unbiased (Curedale 2013, 188-189.)

An interview, between one researcher and one respondent in a face-to-face situation, is called a *one-to-one interview*. This is the best method for researching personal information and opinions about sensitive subjects. It is also a good opportunity to observe and listen to the respondent with better focus than in a group interview. It is important that one-to-one interviews are done at a location where the respondent feels relaxed and safe. One-to-one method results can be challenging to combine with group interviews, should such be done on the same subject (Curedale 2013, 186.)

4.2.3 Customer journey map

A customer journey map draws a visual map of the user's experience when interacting with a service. It uses touchpoints to create a path, called a journey. Following this customer journey, the reader gets an insight into the user experience and the emotions the participant felt during the whole service process, in an easy to read visual manner (Stickdorn & Schneider 2011, 158.)

A customer journey map is built from the user interaction touchpoints with the service. There are different methods of identifying service touchpoints and insight on the user experience of a service. Interviews are a common well-working method, but user diary keeping and self-mapping can be a good way also. Once touchpoints are identified, the researcher constructs a connected customer journey map of the whole experience. The map is a high-level overview of factors affecting the whole journey user experience built up from a user's experience. The map also helps highlight problem areas in the journey, might add perspectives and room for innovation in different stages on the map. This method also gives the opportunity to compare multiple user customer journeys in a quick and easy way. Assuming the customer journey maps are created using the same visual "language" for all customers (Stickdorn & Schneider 2011, 158-159.)

4.3 Research results

This section of the thesis describes the individual results of my research. I used three different research methods for two different target groups. The target groups were recruitment professionals and IT security professionals. The methods used for research were surveys, interviews and customer journey map.

I created a customer journey map of my own CISSP certification experience, which is presented earlier in chapter *3.2.2 Studying and preparing for the CISSP certificate exam*. The customer journey map is mainly based on my own experience getting a CISSP certificate and insights as an IT security professional with more than 15 years of work experience in IT field. While the customer journey gives insight on the path to become CISSP certificate holder, I decided to leave it out of this research results chapter. The research results chapter is focused on answering the research questions presented at the introduction of this thesis.

4.3.1 Survey one: CISSP certificate value survey

The CISSP certificate value survey was distributed online using Google forms online service. The survey questions can be read in *Appendix 1* of this thesis. The survey was distributed among IT security professional the popular social media site called Facebook (facebook.com) in CISSP specific interest groups and through reddit.com forum site sub-sections ("sub-reddits") such as "*reddit.com/r/cissp*". The survey had the potential reach to thousands of people. It is impossible to say how many saw the survey in the news streams, but approx. 100 CISSP certificate engaged users answered the survey.

The goal of this survey was to gather insights into how IT security professionals and current CISSP certificate holders, appreciate the CISSP certificate using the *close-ended* questions, but also gives room for general insights about the CISSP certificate value through *partially open* and *open-ended* questions.

The survey got 101 responses and 47,5 percent of the respondents where aged 29-39 years old. However, every question was provided with an option to skip answering, so some comparisons done later in this chapter might contain a lower number of responses to specific questions in the survey.

Many respondents that answered the survey were IT security professionals, the survey profession field included plenty of professions in IT security industry. Professions such as *Security Operations Center (SOC) analyst, Network security engineer, Information Security Professional, Army Officer, Director of IT, Network Security Administrator, SOC Engineer, Information Systems Security Manager, Information Security Officer, Penetration Tester, IT Executive* and *Information Security Analyst*.

As displayed in *Figure 8*, most of the respondents were from the United States of America with over 74 percentage, next biggest country of respondents was Finland with 8,9 percent. India and United Kingdom each represented 5 percent of the respondents and 6,9 percent of the respondents came from various countries around the world, such as the Netherlands, Argentina, Hungary, Saudi Arabia and Macedonia.

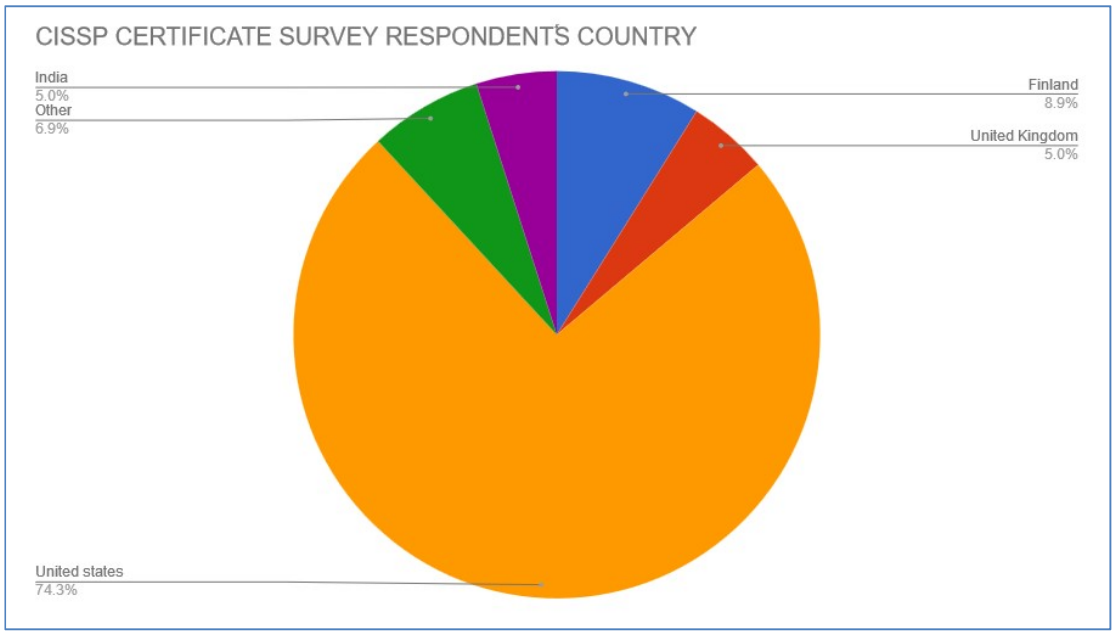

Figure 8: CISSP certificate survey respondent's country Figure.

As the survey was distributed to IT security professionals and CISSP focus groups, almost 50 percent of the responders had achieved CISSP certification. As *Figure 9* displays, only 11 out of 101 respondents did not plan to get CISSP certificated in the near future; in contrast, 38 responders that were not yet CISSP certified are planning on getting CISSP certified in the near future.

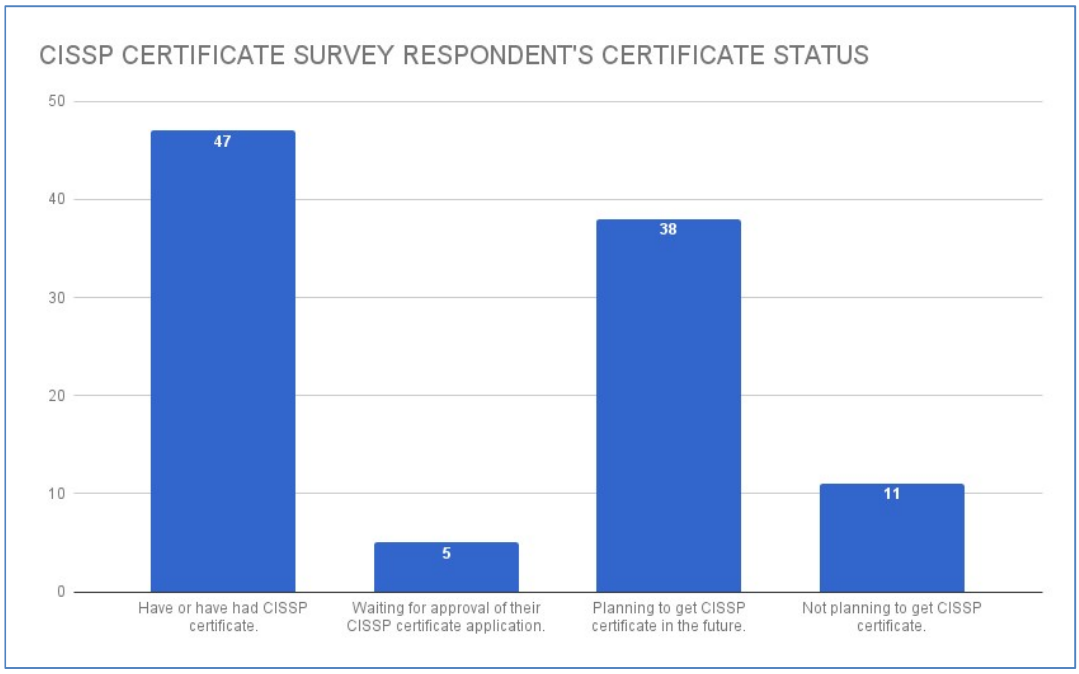

Figure 9: CISSP certificate survey respondent's current certificate status Figure.

The primary focus of this thesis is to research the value of CISSP certificate for the individual certificate holder and those who recruit IT professionals. According to the survey, as shown in *Figure 10*, 77 out of 96 responders agree or somewhat agree that their salary would increase when a CISSP certificate achieved.

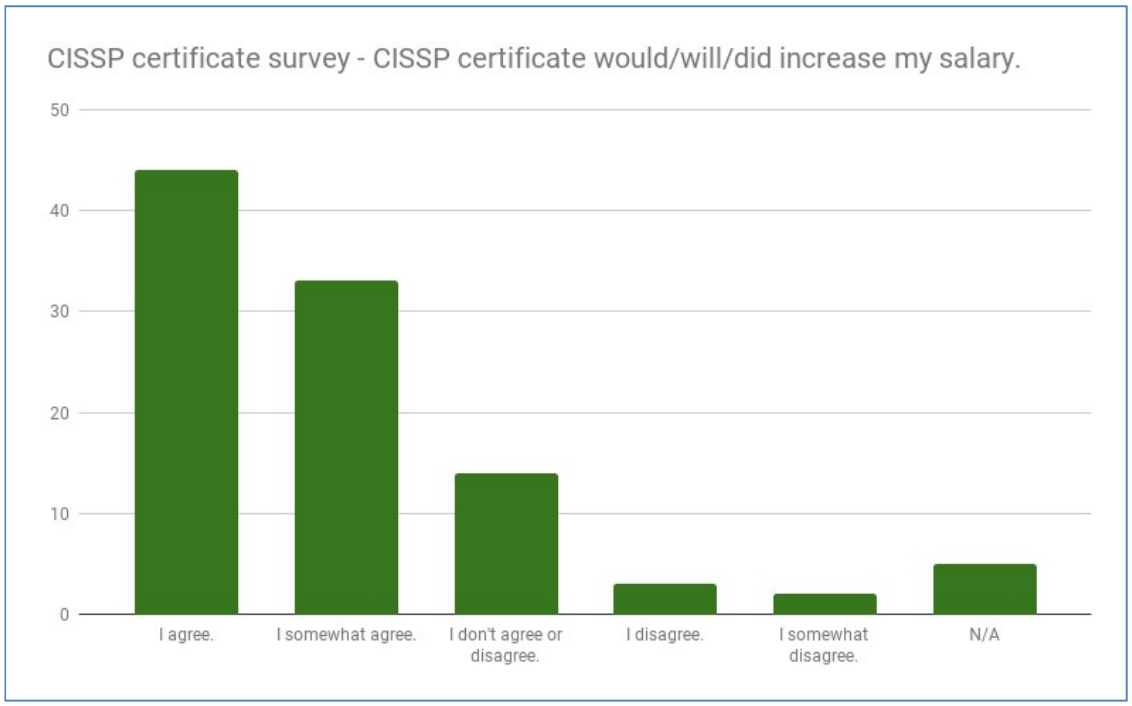

Figure 10: CISSP certificate survey, acquired CISSP certificate increase salary Figure.

In next survey question, about CISSP providing new job opportunities; 95 out 100 responders, as displayed in *Figure 11,* agree or somewhat agree that getting CISSP certificate would open new job opportunities for them. The majority results show the CISSP certificates clearly feel the certificates positive has affected not only salary but also providing new job positions.

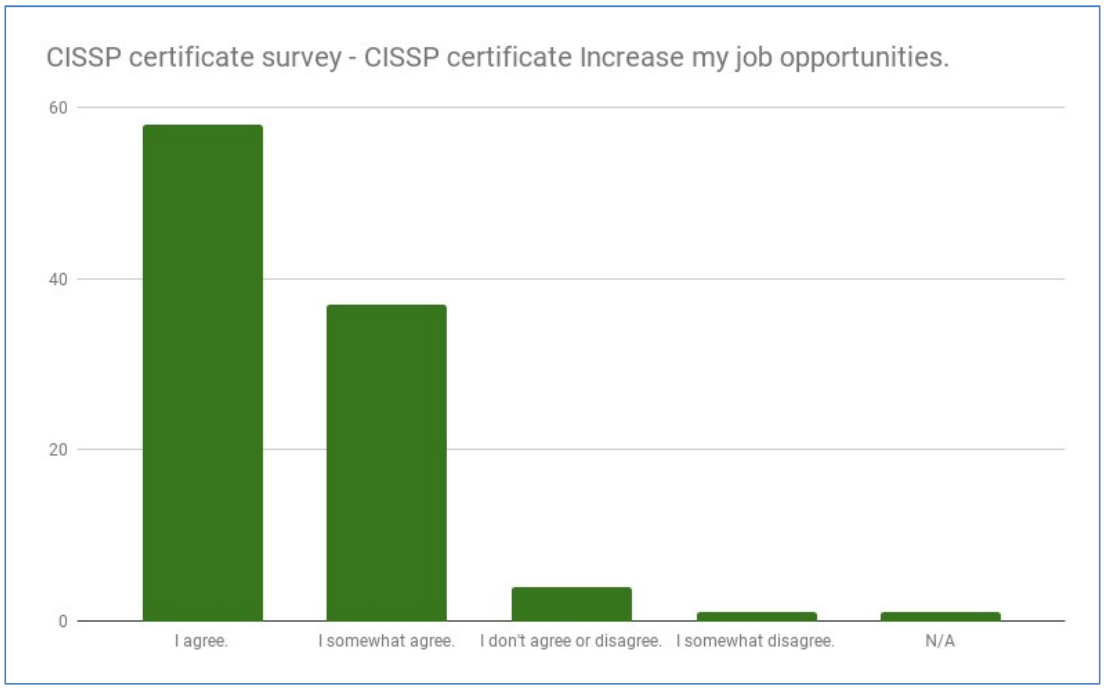

Figure 11: CISSP certificate survey, acquired CISSP certificate increase job opportunities Figure.

The survey results show that while the CISSP certificate is considered suitable for both IT security manager and non-managers; it is among the survey responders more seen as a managerial certificate than a technical one (Figure 12).

Figure 12: CISSP certificate survey, CISSP designed for security managers vs non-managers Figures.

The CISSP certificate exam and upkeep have upfront costs, the certification exam and yearly fees, but it also requires studies to pass the exam and yearly efforts to keep certificate active by collecting CPEs (CISSP *CPEs are described in thesis chapter 3.2.3 Keeping certificate active*). The majority of the responders of the survey considered that the cost and effort required getting and maintaining CISSP certificate was worth it as displayed in Figure 13.

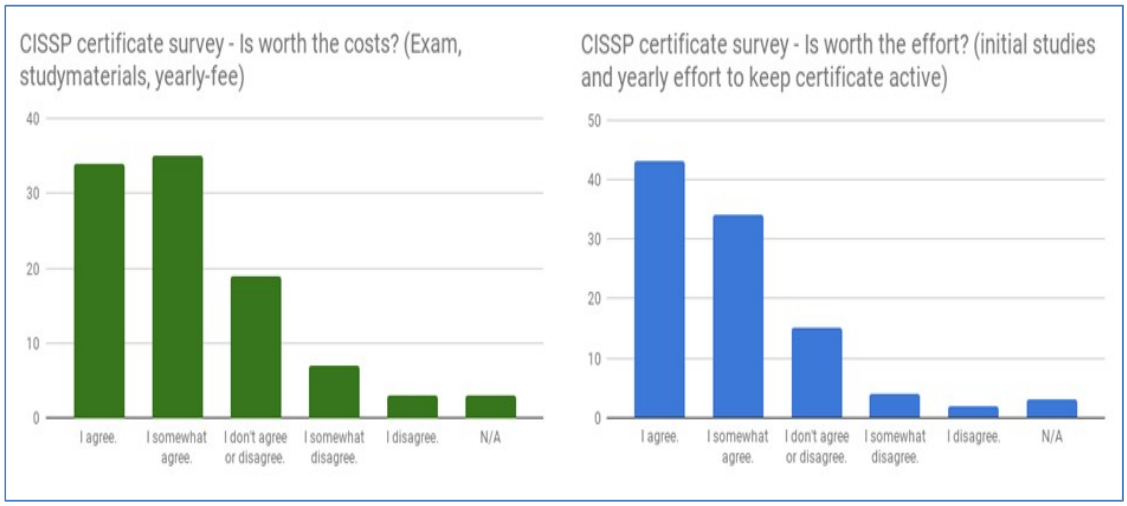

Figure 13: CISSP certificate survey is CISSP certificate worth the cost and effort.

A majority of respondents felt that their employers recognized and valued the CISSP certificate at their workplace (Figure 14).

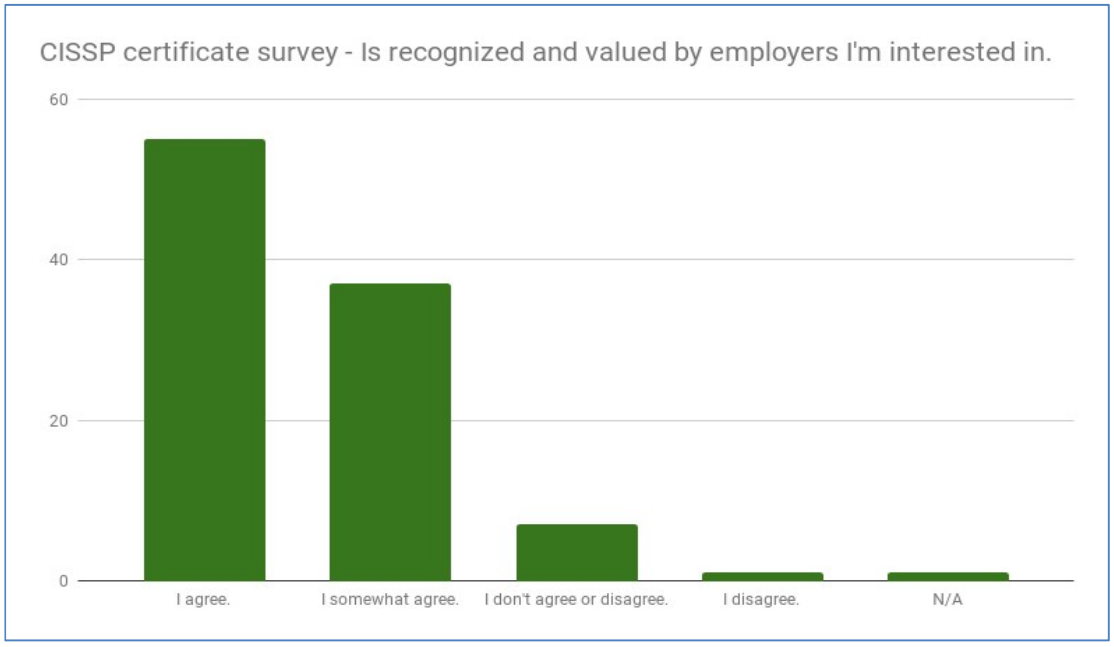

Figure 14: CISSP certificate survey, employers that recognize and value CISSP certificate.

The final, open question, where the responders could freely comment about CISSP certificate and their value to them it became apparent that in the United States of America CISSP certificate was sometimes required when working for US Department of Defense (DOD); that made the CISSP certificate especially valuable to some. Others felt it gave them confidence when working in IT security field, while some individuals didn't think it had much impact on one's abilities working in the IT security field.

This survey with over 100 responders provided valuable data for this thesis. Among the CISSP holders and IT security professionals, the data shows that CISSP certificate is well known and valued highly, having a direct impact on job opportunities and responders salary.

4.3.2 Survey two: Recruiter's certificate value survey

The recruiter's certificate value survey was distributed online using Google forms online service. The survey questions can be read in *Appendix 2* of this thesis. The survey was distributed among recruitment professionals the popular social media site called Facebook (facebook.com) in recruitment specific interest groups and through the popular reddit.com forum site.

The recruitment professional's survey was answered by more than 20 respondents and the survey was complemented by more in-depth interviews of three recruitment professionals with a long experience in recruiting IT professionals. Respondents had recruitment positions such as *Recruiter account manager, Controller, Tech recruiter, Director, Talent Agent, Recruiter, Top talent recruiter, Corporate Recruiting Manager, HR, CEO, Head of HR,* to name some of them.

More than half of the survey respondents were working in a recruitment position in Finland, but there were also answers from the United States of America and Canada as seen in *Figure 15*. Almost 75 percent of the respondents were involved in the recruitment of IT personnel and more than half of the respondents had acquired some kind of career-related certificate themselves.

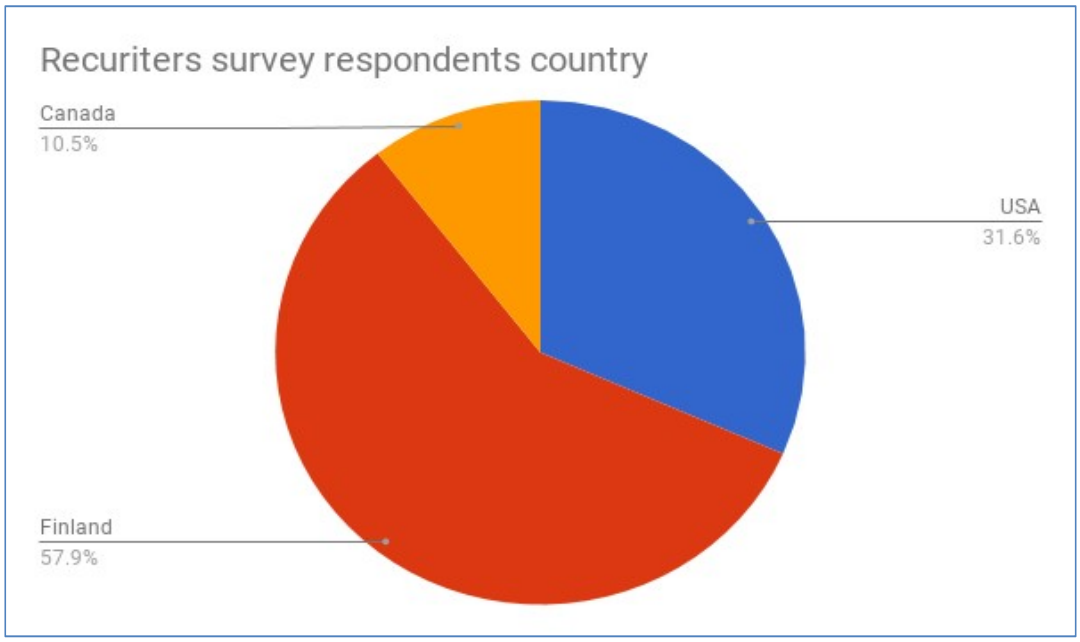

Figure 15: Recruiters survey, respondent's country of residence.

Analysing certifications impact on the recruitment situation, the survey reveals that most recruiters consider certifications only a small part of a potential recruit's qualification for a position, as shown in Figure 16. Additionally, only 25% of the responding recruiter considers that at certain job positions expect that applications to have a certification within their field.

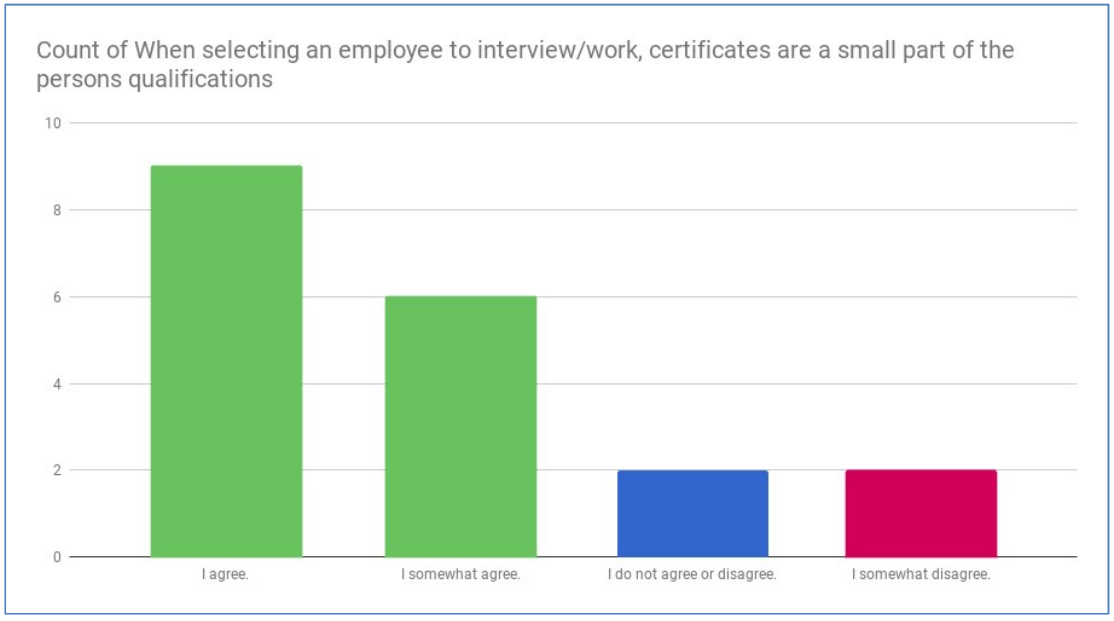

Figure 16: Recruiters survey, most respondents consider certificates only a small part of a person's qualifications.

Certifications are not required for potential recruits according to the survey, however, the survey respondents acknowledge that at certain job positions or levels employees are expected to have certifications displayed in figure 17.

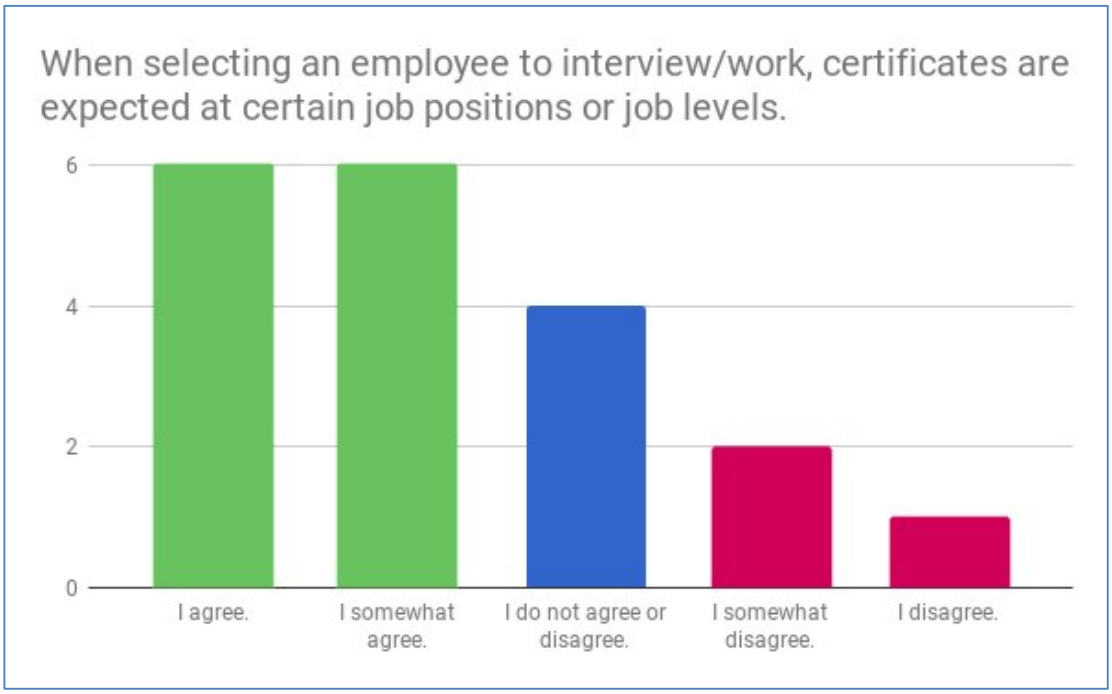

Figure 17: Recruiter's survey, more than half of the respondents consider certificates to be expected at certain job positions or job levels.

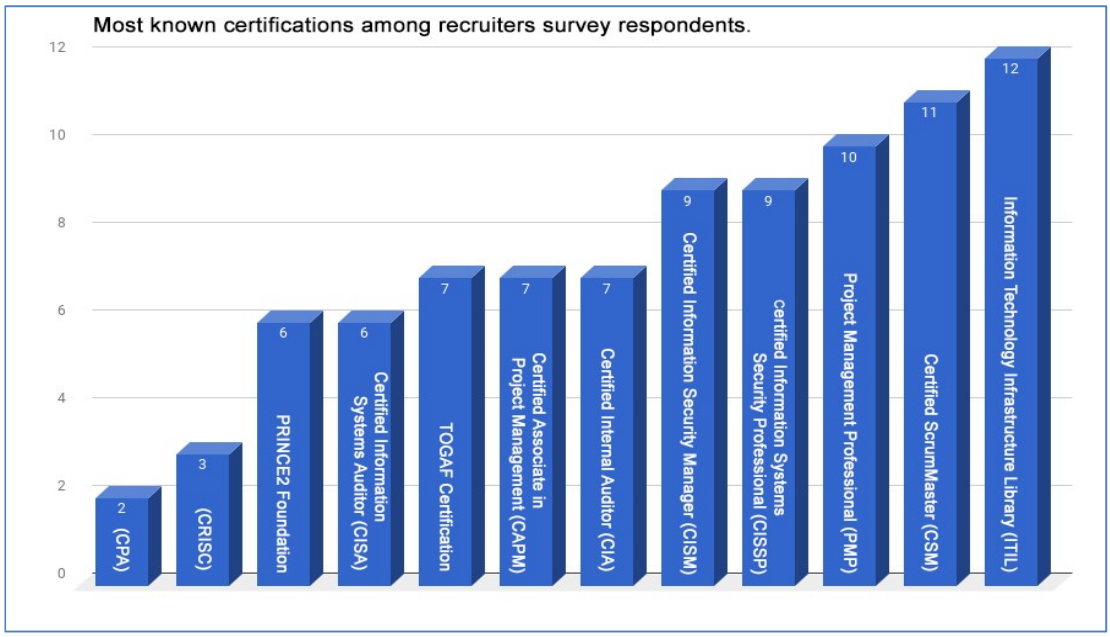

Figure 18: Recruiters survey, most well-known certifications among respondents.

As shown in Figure 18, the most well-known certificates among the respondents are (*in order from most-known to least-known*):

- *Information Technology Infrastructure Library (ITIL),*
- *Certified ScrumMaster (CSM),*
- *Project Management Professional (PMP),*
- *Certified Information Systems Security Professional (CISSP),*
- *Certified Information Security Manager (CISM),*
- *Certified Internal Auditor (CIA),*
- *Certified Associate in Project Management (CAPM),*
- *TOGAF Certification, Certified Information Systems Auditor (CISA),*
- *PRINCE2 Foundation,*
- *Certified in Risk and Information Systems Control (CRISC),*
- *Certified Public Accountant (CPA).*

ITIL certification was the most well-known certification. CSM, PMP and CISSP certificate following closely. Additionally to the certificates listed above, some respondents knew company specific certificates by enterprise IT companies such as *Microsoft* and *Cisco Systems*.

The survey question that divides recruiter most was the question *that certificates are an important part of a person's CV (curriculum vitae)*. While the answers' amount is (Figure 19) slightly on the agreeing side, many respondents did disagree with the statement and many chose to stay neutral to the question.

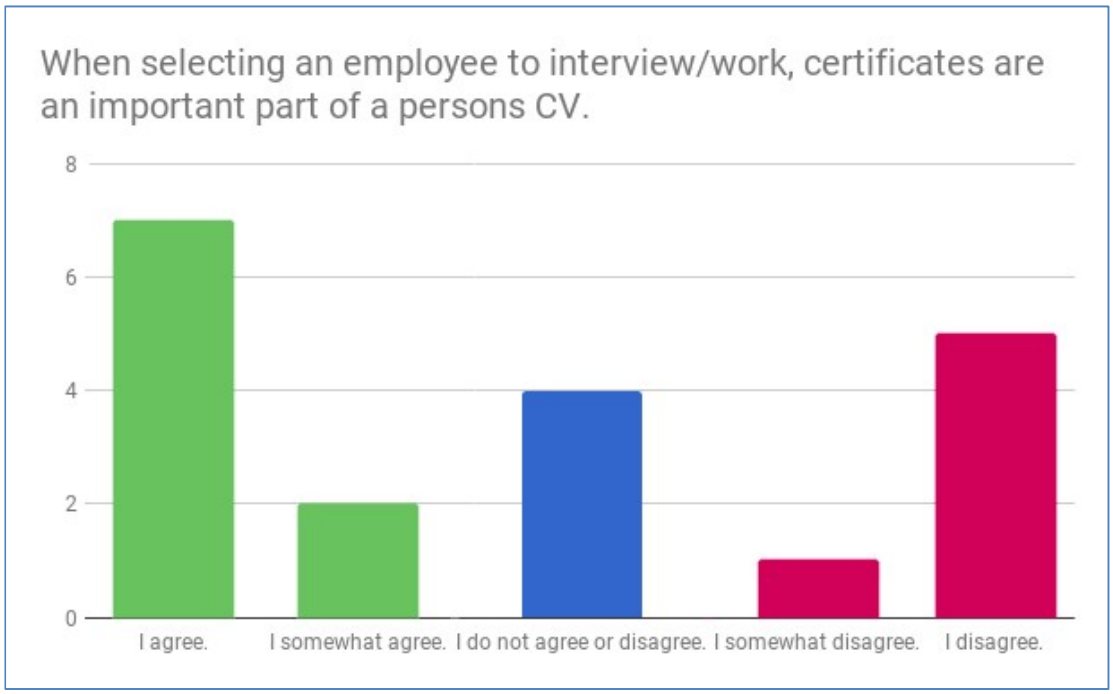

Figure 19: Recruiters survey, certificate status on job position candidates CV (curriculum vitae).

The survey answered by recruiters gave valuable insights into how the people in positions hiring people to various organisations, see and value certifications in a recruitment situation. There are many certificates on the market and the survey shows the most known ones.

The graphs show quite clearly, that according to professionals, recruiters' certificates are only a part of a person's qualification in a job position. However, having or not having a certificate might be decisive when a recruiter is deciding between candidates for a position. Another observation from the survey is that certain certificates are more well-known than

others, ITIL certificate being the most known certificate and CISSP being fourth on the list.

The recruitment survey gave insight on how recruitment professionals' value certificates, however, for now, they are not an integral part of the potential candidate's qualifications, and even they might give an edge over candidates who do not have certificates. A candidate with the work experience, cultural fit and needed skills-set validated with certifications in his/her field would be an ideal candidate for almost any specialist position. According to the interviewees, the most important assets of a potential recruit are work practice and personality features such as cultural fit and potential for growth.

4.3.3 Interviews: Recruiting professionals

This chapter analyses the results of three recruitment professionals' interviews. Interviews are done to complement the 'recruiter's certificate value survey', for more insights into the results. The interview official transcripts can be found at end of this thesis in Appendix 3, 4 and 5. However, more verbal communication outside of the official interview transcripts' was discussed in the interview sessions.

The interviews were conducted to give insight and help to support or refute any of my conclusions drawn from the recruiter's survey. The interview questions were set up as a general interview about recruiting professional and certificates; not trying to lead into specific certificates such as CISSP.

The interviews were short with mostly close-ended questions and some open-ended questions, each interview session taking about 30 minutes. The questions were partly based on the (then in-progress) results gathered from the recruiter survey. The interviews were conducted to provide my research with some additional confirmation to the recruiter's survey results and provide me with a broader viewpoint of the recruitment process and potential recruits characteristics on a general level.

All three interviewees wanted to stay anonymous; together they have over 25 years of work experience in recruiting and have Finnish cultural background or nationality. The three interviewee's job titles are *Recruitment manager*, *Recruitment consultant* and *Talent*

Acquisition Professional. They all have a long experience in recruiting both non-IT and IT professionals for various companies and organisations.

According to the interviewees, the most important assets of a potential recruit are work practice and personality features such as cultural fit and potential for growth. (personal communication with talent acquisition professional 17.10.2017). The interviews reaffirmed some of the questions' result in the recruiter's survey. The notions, among recruiters in Finland, is that certificates are not an essential part of an applicant's CV, and lack of certificates are usually not a "deal-breaker" for someone losing a job, however, it might give a boost among otherwise equally skilled candidates. (personal communication with recruitment consultant 18.1.2018)

One viewpoint, provided by one of the interviewees, is that some industries, such as IT security, have more demand for certifications than other industries, sometimes even required by contractual agreements (personal communication with recruitment manager 18.1.2018). This was also supported by the CISSP recognition survey, especially among the US residents, where CISSP might even be a requirement to work with US Department of Defense in IT security as stated in chapter *4.3.1. CISSP certificate value survey*.

All interviewees considered themselves lacking enough up to date information about certificates in general. This, however, is usually not a problem as according to them, as the certificates are one more validation about a candidate's skill, not a definitive factor in selecting a recruit. A candidate with the work experience, cultural fit and needed skills-set validated with certifications in his/her field would be an ideal candidate for almost any specialist position.

5 CONCLUSION

Companies and other organisations have a hard time to fill their vacant IT security positions. The technology company *Cisco Systems* estimates that there are 1 million IT security positions unfulfilled worldwide and demand for competent IT security personnel is growing (IEEE Cyber Security, 2017). At the same time, IT security threats are getting more sophisticated every year, as more services are digitized and automated at an increasing pace.

According to Jonathan Katz, director of Maryland Cybersecurity Centre in the United States of America: *"The increased demand for cybersecurity professionals is relatively new, and universities are still unable to respond to this demand by incorporating it in their curricula,"* (IEEE Cyber Security, 2017).

IT security-focused educational programs are still a new phenomenon, so there is an increasing demand for ways to prove IT security skills among IT security professionals that do not have school credentials to prove their skills. The constant demand for IT security professionals and increased requirements for said professionals raises the demand for know-how among professional recruiters. These recruiters must find ways to identify and verify as IT security recruits skillset during the recruitment process. This is when security certificates such as CISSP become increasingly important to differentiate candidates from each other.

The thesis sets out to investigate if there is value or benefits in acquiring a CISSP certificate from two perspectives, the certificate holder's perspective and the recruiter's perspective. In the introduction there were two research questions defined as following:

- Do IT security professionals and CISSP certificate holders feel the certificate provides better job opportunities and salary?

- Do recruiters believe that CISSP certificates and/or IT certificates, in general, make potential recruitment candidates more attractive on the job market?

The short answers to the above two research questions would be *yes,* with some remarks described in the chapters below.

The thesis used multiple different research methods to answer the questions and to figure out if CISSP accreditation adds value to IT security employees and recruiters. The research included surveys and interviews with recruitment professionals and IT security professionals. Additionally, during the writing of this thesis, I myself studied for the CISSP certificate and became a *Certified Information Systems Security Professional certificate* holder. The CISSP survey answered by almost 50 CISSP certificate holders and approximately another 50 IT security professionals were planning to get the CISSP certificate in the future.

Referring to my research and surveys in the *research results* chapter in this thesis, a vast majority of CISSP holders or persons on track to become a CISSP felt that the certificate

would open new opportunities and increase their salary once they have acquired the *Certified Information Systems Security Professional* status. The survey also covered a variety of other opinions and insights of the effort on getting and holding an active CISSP certificate.

The recruitment professional's survey was answered by more than 20 respondents and the survey was complemented by more in-depth interviews of three recruitment professionals with a long experience in recruiting IT professionals. The answers they provided gave not only answers to the research questions but also insights into other important factors in a candidate recruitment process.

The answer to the question: *Do recruiters believe that CISSP certificates and/or IT certificates, in general, make potential recruitment candidates more attractive on the job market?* I stated a above that the short answer was yes. The recruitment survey and interviews agree that CISSP and other certificates make candidates more attractive to the job market; however, it is not necessarily the deciding factor for a recruiter when recruiting a new employee. Other factors such as work experience, cultural fit to the organisation and candidate potential to grow in the positions are in general more important than acquired certifications.

Based on the data gathered from my research I dare to state that IT certifications in general and the Certified Information Systems Security Professional certificate (CISSP) provide value to not only the certificates holders but also helps the organisations in the recruitment process. As previously stated in the thesis, some organisations might even require the consultants have a security certificate acquired to be able to work for them. This opens opportunities for both certificate holders and companies that hire consultants to these organisations with high-security standards.

In lack of formal IT security training and courses on University curriculums, older IT professionals must find other ways to validate their IT security skills. Work experience is still the most important qualification a recruiter looks for but especially in IT security, certificates seems to become a way to validate your skills.

Certificates such as CISSP provide a third party validated level of certainty, for both the certificate holder and the recruiter that the candidate is suitable for the position. This is the desired situation for both the recruiter and the potential candidate to be able to give additional verification that they are qualified for the position. I conclude that, like many

other certifications, CISSP certification provides value both the certificate holders and the recruiting organisations.

5.1 Final thoughts

Few things are “black and white” in the real world; however, research easily makes things appear so. I truly feel I learned a lot about the subjects I was researching and about research methods. Surely, my methods are not without flaws and gathering enough data was the hardest part of the thesis. I feel I had large enough samples to get a real indicator of how the certificates are precept inside the target groups.

The thesis is set out with an ambitious goal, which was refined and tuned until the very end of my research; however, the core of the thesis stayed the same. The answers to the research questions seem to fall in line with my own experience as a CISSP certificate holder and an experienced IT professional.

It has been a learning experience in research and a valuable insight into CISSP certificate and recruitment process of IT personnel. It has shown me that people are passionate about their certifications and proud to belong to a group with the same interests. As an employee of a cybersecurity company, I have had due to this thesis, many informal non-recorded discussions about the subject of my thesis with IT security professionals and recruiters alike. I value all learning experience this thesis has provided me with, and like to thank everyone who has supported me on the way.

REFERENCE LIST

Akamai, 2017. *Q4 2017 State of the Internet / Security Report,* [online] https://www.akamai.com/us/en/multimedia/documents/state-of-the-internet/q4-2017-state-of-the-internet-security-executive-summary.pdf (Retrieved 21.04.2018).

Boussalis, C. 2012. *Basic Survey Theory and Design,* [online] http://hnmcp.law.harvard.edu/wp-content/uploads/2012/02/Constantine-Boussalis-Training-on-Basic-Survey-Theory-and-Design.pdf (Retrieved 12.10.2017).

Curedale, R. 2013. *Service Design 250 essential methods.* Los Angeles: Design Community College Inc.

CSO online. 2017. *2018 prediction: securing IoT-connected devices will be a major cybersecurity challenge,* [online] https://www.csoonline.com/article/3244467/internet-of-things/2018-prediction-securing-iot-connected-devices-will-be-a-major-cybersecurity-challenge.html (Retrieved 21.04.2018).

CSO online. 2018. *The global cyber war is heating up: Why businesses should be worried,* [online] https://www.csoonline.com/article/3257404/cyber-attacks-espionage/the-global-cyber-war-is-heating-up-why-businesses-should-be-worried.html (Retrieved 21.04.2018).

Doom, C. 2010. *Introduction to Business Information Management*. Brussels: Vubpress.

EITCA. 2017. *EITCA/IS Information security academy,* [online] https://eitca.org/eitca-is-information-security-academy/ (Retrieved 13.10.2017).

GIAC. 2017. *GIAC Certifications: Categories,* [online] https://www.giac.org/certifications/categories (Retrieved 13.10. 2017).

Gordon, A. 2015. *Official ISC^2 Guide to the CISSP CBK, Fourth Edition*. Electronic book.

Harris, S. 2016. *CISSP Exam Guide, Seventh Edition.* New York: McGraw-Hill Education.

Hohwü, L et al. 2013. *Web-Based Versus Traditional Paper Questionnaires: A Mixed-Mode Survey With a Nordic Perspective,* [online] https://www.ncbi.nlm.nih.gov/pmc/articles/PMC3757995/ (Retrieved 12.10.2017).

IEEE Cyber Security. 2017. *The Institute: The Cybersecurity Talent Shortage Is Here, and It's a Big Threat to Companies,* [online] https://cybersecurity.ieee.org/blog/2017/04/13/the-institute-the-cybersecurity-talent-shortage-is-here-and-its-a-big-threat-to-companies/ (Retrieved 15.04.2018).

Infosec institute. 2017. *CISSP Drag & Drop and Hotspot Questions: 5 Example,* [online] http://resources.infosecinstitute.com/cissp-test-1-2-new/ (Retrieved 28.10.2017).

ISC². 2015. *CISSP (ISC)² Certified Information Systems Security Professional Official Study Guide, Seventh Edition*. Indianapolis: John Wiley & Sons, Inc.

ISC². 2016. *CAP - Why Certify*, [online] https://www.isc2.org/cap-why-certify.aspx (Retrieved 25.12.2016).

ISC², 2017. *ISC² Overview,* [online] https://www.isc2.org/About (Retrieved 13.10.2017).

ISC² II. 2017. *Cybersecurity Certification,* [online] https://www.isc2.org/Certifications/CISSP (Retrieved 25.10.2017).

ISC² III. 2017. *Continuing professional education (CPE) policies and guideline 2015,* [online] https://downloads.isc2.org/certifications/cpe-guidelines.pdf (Retrieved 25.10.2017).

ISC² IV. 2017. *2017 CISSP Detailed Content Outline (DCO) with Weights Final,* [online] https://downloads.isc2.org/credentials/cissp/CISSP-Detailed-Content-Outline.pdf (Retrieved 29.10.2017]

ISACA. 2017. *About ISACA*, [online] http://www.isaca.org/about-isaca/Pages/default.aspx (Retrieved 13.10.2017).

IT Governance Ltd. 2016. *What is CISSP?*, [online] http://www.itgovernance.co.uk/cissp.aspx (Retrieved 27.12.2016).

Pilon, A. 2017. *Self-Service Kiosks Survey: Consumers Appreciate Multiple Options,* [online] https://aytm.com/blogmarket-pulse-research/self-service-kiosks-survey/ (Retrieved 12.10.2017).

Porup, J.M. 2016. *CISSP certification: Are multiple choice tests the best way to hire infosec pros?*, [online] http://arstechnica.com/security/2016/07/cissp-certification-how-to-hire-infosec-pros/ (Retrieved 27.12.2016).

PricewaterhouseCoopers. 2015. *Turnaround and transformation in cybersecurity: Key findings from The Global State of Information Security Survey 2016,* [online] http://www.pwc.com/sg/en/publications/assets/pwc-global-state-of-information-security-survey-2016.pdf (Retrieved 28.12.2016).

SC Media. 2009. *A brief history of internet security,* [online] https://www.scmagazine.com/a-brief-history-of-internet-security/article/556389/ (Retrieved 12.03.2018).

Stickdorn M. & Schneider J. 2011. *This is service design thinking.* New Jersey: John Wiley & Sons Inc.

Tittel, E. 2016. *How To Become a Certified Information Systems Security Professional (CISSP)*, [online] http://www.tomsitpro.com/articles/how-to-become-cissp,1-615.html (Retrieved 29.10.2017).

Vijayan, J. 2018. *What is a security operations centre (SOC)?*, [online] https://learn.techbeacon.com/units/what-security-operations-center-soc (Retrieved 22.04.2018).

Warner, T. 2010. *Just the Facts: How to Become a CISSP,* [online] http://www.pearsonitcertification.com/blogs/blog.aspx?uk=Just-the-Facts-How-to-Become-a-CISSP (Retrieved 25.10.2017).

LIST OF FIGURES

Page Element

ABBREVIATIONS

AIC or CIA	Availability, Integrity, Confidentiality *(so-called security triad principle)*
BC	Business Continuity
CBK	Common Body of Knowledge *(CISSP domain)*
CCNA	Cisco Certified Network Associate
CCTV	Closed-circuit television *(video surveillance system)*
CEO	Chief Executive Officer
CISO	Chief Information Security officer
CISSP	Certified Information Systems Security Professional
COO	Chief Operating Officer
CPE	Continuing Professional Education *(credits for maintaining CISSP certificate)*
CSO	Chief Security Officer
CTO	Chief Technology Officer
CV	Curriculum vitae *(overview of a person's qualifications)*
EITCI	European Information Technologies Certification Institute
ESA	Enterprise Security Architecture
GDPR	General Data Protection Directive *(European Union)*
IAAA or AAA	Identification, Authentication, Authorization, Auditing and Accounting *(a security principle)*
ISACA	Information Systems Audit and Control Association
IT	Information technology
IoT	Internet of Things (Internet connected devices controlling various functions such as thermostats in homes or organisations)
ISC^2 or $(ISC)^2$	International Information Systems Security Certification Consortium
KPI	Key Performance Indicator
OSI	Open System Interconnect (*network model)*
PwC	PricewaterhouseCoopers *(a consulting professional services firm)*
SANS	Escal Institute of Advanced Technologies
SOC	Security Operations Centre
TCP/IP	Transmission Control Protocol/Internet Protocol *(a commonly used network protocol)*

Appendices

Appendix 1: CISSP certificate perception survey

CISSP recognition survey

This is survey is part of my masters thesis where I research Certified Information Systems Security Professional (CISSP) certificate recognition, perception and value to the individual certificate holder. If you have any questions about my thesis you can contact me by e-mail: cisspsurvey[at]aaneton.net

This survey is only 10 questions , data is used for research purposes only.

Country *

Where do you live.

Short answer text

Age *

- Younger than 18.
- 18-28.
- 29-39.
- 40-49.
- 50 or older.
- Prefer not to say.

Occupation (not required)

Job or profession.

Short answer text

1) CISSP certificate status (select all that apply) *

- I have active CISSP certificate.
- I have achieved CISSP certificate before but it has expired.
- I do not have and never had active CISSP certificate.

- [ ] I have tried to get CISSP certified but failed the exam (and still do not have it).
- [ ] I did not pass the CISSP certificate exam on first try.
- [ ] I'm planning to get CISSP certified (active) in the near future.
- [ ] I do not have, nor do I plan to get CISSP certified.
- [ ] I have other certificates by International Information System Security Certification Consortium (ISC2).
- [ ] I have information security certificates by other organisations than ISC2.
- [ ] I have passed my CISSP and submitted my endorsement documents (I'm still waiting for approval).
- [ ] I have passed my CISSP but have not yet submitted my endorsement documents.

CISSP certificate *

	I agree.	I somewhat agree.	I don't agree or disagree.	I somewhat disagree.	I disagree.	N/A
2) Would/will/did increase my salary.	○	○	○	○	○	○
3) Increase my job opportunities.	○	○	○	○	○	○
4) Is a more valuable addition on my CV compared to other certificates.	○	○	○	○	○	○
5) Tells me something about a certified persons information security knowledge/abilities.	○	○	○	○	○	○
6) Is designed for information security managers.	○	○	○	○	○	○
7) Is designed for information security professionals (non-managers).	○	○	○	○	○	○
8) Is worth the costs? (Exam, studymaterials, yearly-fee).	○	○	○	○	○	○
9) Is worth the effort? (initial studies and yearly effort to keep certificate active by gathering points).	○	○	○	○	○	○
10) Is recognized and valued by employers I'm interested in.	○	○	○	○	○	○

Free comment about CISSP certificate and it's value/reputation to you

Long answer text

Appendix 2: Recruiters certificate value survey

Recruiters certificate significance survey

This is survey is part of my masters thesis where I research (IT focused) certificate recognition, perception and value to the individual certificate holder. The questions in this survey are mostly about perception of certificates in general.

This survey is primarly meant for people somehow involved in the recruitment process of employees such as HR, recruiters, managers, leadership, team leaders, senior staff. However anyone is allowed to participate; also you don't need to recognize any specific certificates to participate.

The survey will only take a few minutes to fill in.
All data is used for research purposes only and no personal details are stored in the form.
If you have any questions about my thesis you can contact me by e-mail: mastersurvey[at]aaneton.net

Country *

Where do you currently live?

Short answer text

Occupation

Job or profession.

Short answer text

I am / have been involved recruiting employees to an organisation/company. *

- ◯ Yes
- ◯ No

I am part of IT staff recruitment process in my organisation/company. *

- ◯ Yes
- ◯ No

Do you have any career related certifications yourself? *

- ◯ Yes
- ◯ No

When selecting an employee to interview/work, certificates *

	I agree.	I somewhat agree.	I do not agree or disagree.	I somewhat disagree.	I disagree.	N/A
give an edge to a person is certified, compared to person that do not have one.	○	○	○	○	○	○
tell me something about a persons career.	○	○	○	○	○	○
are in general a representation of a persons skills.	○	○	○	○	○	○
are a small part of the persons qualifications.	○	○	○	○	○	○
are expected at certain job positions or job levels.	○	○	○	○	○	○
are an important part of a persons CV.	○	○	○	○	○	○

What certificates do you know/have you heard of? (select all that apply)

- ☐ Certified Associate in Project Management (CAPM)
- ☐ Certified Information Security Manager (CISM)
- ☐ Certified Information Systems Security Professional (CISSP)
- ☐ Certified Information Systems Auditor (CISA)
- ☐ Certified in Risk and Information Systems Control (CRISC)
- ☐ Certified Internal Auditor (CIA)
- ☐ Certified ScrumMaster (CSM)
- ☐ Information Technology Infrastructure Library (ITIL)
- ☐ PRINCE2 Foundation
- ☐ Project Management Professional (PMP)
- ☐ TOGAF Certification
- ☐ Other...

Free comment about certificates in recruitment.

Long answer text

Appendix 3: Recruiting professional interview 1/3

Interview transcript with N.N on 17.10.2017

Country of residence: Finland

Profession: Talent Acquisition Manager

I am/have been involved recruiting employees to an organization/company.
Yes

I am part of IT staff recruitment process in my organization/company.
Yes

Do you have any career related certifications yourself?

No.

What is the most important asset in a potential recruit?
Demonstrated skill, future potential and cultural fit.

Please set in order of importance:
Matching posted qualifications for the job: 4
Skills: 4
Potential, 5
Education, 3
Work experience, 5
Courses: 2
Referrals: 3
Certificates: 5
Comment: An indicator that you can do what you say.
Personality: 3
Cultural fit: 5

Most important: work experience

Is there any IT certificate you would recommend?
CISSP

Do you feel that there is knowledge about certificates among recruiters?
No sufficiently,

Can certificates compensate other lacking qualifications such as education or work experience? Yes

Are certificates expected at a certain level of expertise?
No.

Free comment:

Appendix 4: Recruiting professional interview 2/3

Interview transcript with N.N on 18.01.2018

Country of residence: Finland

Profession: Recruitment consultant

I am/have been involved recruiting employees to an organization/company.
Yes

I am part of IT staff recruitment process in my organization/company.
Yes

Do you have any career related certifications yourself?
No.

What is the most important asset in a potential recruit?
Readiness or potential for the position.

Please set in order of importance:
Matching posted qualifications for the job: 3
Skills: 4
Potential, 3
Education, 4
Work experience, 4
Courses: 3
Referrals: 3
Certificates: 3
Personality: 4
Cultural fit: 4

Most important: The whole package.

Is there any IT certificate you would recommend?
-

Do you feel that there is knowledge about certificates among recruiters?
No.

Can certificates compensate other lacking qualifications such as education or work experience? Yes.

Are certificates expected at a certain level of expertise?
No.

Free comment:

"Because certificates are not that sought after in Finnish IT industry, have some might give an edge when applying for a job."

Appendix 5: Recruiting professional interview 3/3

Interview transcript with N.N on 18.01.2018

Country of residence: Finland

Profession: Recruitment manager

I am/have been involved recruiting employees to an organization/company.
Yes

I am part of IT staff recruitment process in my organization/company.
Yes

Do you have any career related certifications yourself?
Yes. MPA and ACE.

What is the most important asset in a potential recruit?
Personality, skillset and work experience.

Please set in order of importance:
Matching posted qualifications for the job: 4
Skills: 4
Potential, 5
Education, 3
Work experience, 5
Courses: 4
Referrals: 3
Certificates: 4
Personality: 4
Cultural fit: 4

Most important: work experience

Is there any IT certificate you would recommend?
ITIL, PMP,

Do you feel that there is knowledge about certificates among recruiters?
Yes, getting better.

Can certificates compensate other lacking qualifications such as education or work experience? Yes.

Are certificates expected at a certain level of expertise?
Definitely helps.

Free comment: "*Certifications are not that know in Finland, except in certain areas such as IT security were there could be demands for certified persons by contract."*

Appendix 6: CISSP detailed content outline with weights (2017)

2017 CISSP Detailed Content Outline (DCO) with Weights Final
Effective Date: April 2018

2017 CISSP Detailed Content Outline With Weights Final (Public Version)		
Classification	Domain/Task/Subtask	Weight
Domain 1	Security and Risk Management	15%
1.1	Understand and apply concepts of confidentiality, integrity, and availability	
1.2	Evaluate and apply security governance principles	
1.2.1	Alignment of security function to business strategy, goals, mission, and objectives	
1.2.2	Organizational processes (e.g., acquisitions, divestitures, governance committees)	
1.2.3	Organizational roles and responsibilities	
1.2.4	Security control frameworks	
1.2.5	Due care/due diligence	
1.3	Determine compliance requirements	
1.3.1	Contractual, legal, industry standards, and regulatory requirements	
1.3.2	Privacy requirements	
1.4	Understand legal and regulatory issues that pertain to information security in a global context	
1.4.1	Cyber crimes and data breaches	
1.4.2	Licensing and intellectual property requirements	
1.4.3	Import/export controls	
1.4.4	Trans-border data flow	
1.4.5	Privacy	
1.5	Understand, adhere to, and promote professional ethics	
1.5.1	(ISC)² Code of Professional Ethics	
1.5.2	Organizational code of ethics	
1.6	Develop, document, and implement security policy, standards, procedures, and guidelines	
1.7	Identify, analyze, and prioritize Business Continuity (BC) requirements	
1.7.1	Develop and document scope and plan	
1.7.2	Business Impact Analysis (BIA)	
1.8	Contribute to and enforce personnel security policies and procedures	
1.8.1	Candidate screening and hiring	
1.8.2	Employment agreements and policies	
1.8.3	Onboarding and termination processes	
1.8.4	Vendor, consultant, and contractor agreements and controls	
1.8.5	Compliance policy requirements	
1.8.6	Privacy policy requirements	
1.9	Understand and apply risk management concepts	
1.9.1	Identify threats and vulnerabilities	
1.9.2	Risk assessment/analysis	
1.9.3	Risk response	
1.9.4	Countermeasure selection and implementation	
1.9.5	Applicable types of controls (e.g., preventive, detective, corrective)	
1.9.6	Security Control Assessment (SCA)	
1.9.7	Monitoring and measurement	
1.9.8	Asset valuation	
1.9.9	Reporting	
1.9.10	Continuous improvement	
1.9.11	Risk frameworks	
1.10	Understand and apply threat modeling concepts and methodologies	
1.10.1	Threat modeling methodologies	
1.10.2	Threat modeling concepts	
1.11	Apply risk-based management concepts to the supply chain	
1.11.1	Risks associated with hardware, software, and services	
1.11.2	Third-party assessment and monitoring	
1.11.3	Minimum security requirements	
1.11.4	Service-level requirements	
1.12	Establish and maintain a security awareness, education, and training program	
1.12.1	Methods and techniques to present awareness and training	
1.12.2	Periodic content reviews	
1.12.3	Program effectiveness evaluation	
Domain 2	Asset Security	10%
2.1	Identify and classify information and assets	
2.1.1	Data classification	
2.1.2	Asset Classification	
2.2	Determine and maintain information and asset ownership	
2.3	Protect privacy	
2.3.1	Data owners	
2.3.2	Data processors	
2.3.3	Data remanence	
2.3.4	Collection limitation	
2.4	Ensure appropriate asset retention	
2.5	Determine data security controls	
2.5.1	Understand data states	
2.5.2	Scoping and tailoring	
2.5.3	Standards selection	
2.5.4	Data protection methods	
2.6	Establish information and asset handling requirements	
Domain 3	Security Architecture and Engineering	13%

2017 CISSP Detailed Content Outline (DCO) with Weights Final
Effective Date: April 2018

2017 CISSP Detailed Content Outline With Weights Final (Public Version)		
Classification	Domain/Task/Subtask	Weight
3.1	Implement and manage engineering processes using secure design principles	
3.2	Understand the fundamental concepts of security models	
3.3	Select controls based upon systems security requirements	
3.4	Understand security capabilities of information systems (e.g., memory protection, Trusted Platform Module (TPM), encryption/decryption)	
3.5	Assess and mitigate the vulnerabilities of security architectures, designs, and solution elements	
3.5.1	Client-based systems	
3.5.2	Server-based systems	
3.5.3	Database systems	
3.5.4	Cryptographic systems	
3.5.5	Industrial Control Systems (ICS)	
3.5.6	Cloud-based systems	
3.5.7	Distributed systems	
3.5.8	Internet of Things (IoT)	
3.6	Assess and mitigate vulnerabilities in web-based systems	
3.7	Assess and mitigate vulnerabilities in mobile systems	
3.8	Assess and mitigate vulnerabilities in embedded devices	
3.9	Apply cryptography	
3.9.1	Cryptographic life cycle (e.g., key management, algorithm selection)	
3.9.2	Cryptographic methods (e.g., symmetric, asymmetric, elliptic curves)	
3.9.3	Public Key Infrastructure (PKI)	
3.9.4	Key management practices	
3.9.5	Digital signatures	
3.9.6	Non-repudiation	
3.9.7	Integrity (e.g., hashing)	
3.9.8	Understand methods of cryptanalytic attacks	
3.9.9	Digital Rights Management (DRM)	
3.10	Apply security principles to site and facility design	
3.11	Implement site and facility security controls	
3.11.1	Wiring closets/intermediate distribution facilities	
3.11.2	Server rooms/data centers	
3.11.3	Media storage facilities	
3.11.4	Evidence storage	
3.11.5	Restricted and work area security	
3.11.6	Utilities and Heating, Ventilation, and Air Conditioning (HVAC)	
3.11.7	Environmental issues	
3.11.8	Fire prevention, detection, and suppression	
Domain 4	Communication and Network Security	14%
4.1	Implement secure design principles in network architectures	
4.1.1	Open System Interconnection (OSI) and Transmission Control Protocol/Internet Protocol (TCP/IP) models	
4.1.2	Internet Protocol (IP) networking	
4.1.3	Implications of multilayer protocols	
4.1.4	Converged protocols	
4.1.5	Software-defined networks	
4.1.6	Wireless networks	
4.2	Secure network components	
4.2.1	Operation of hardware	
4.2.2	Transmission media	
4.2.3	Network Access Control (NAC) devices	
4.2.4	Endpoint security	
4.2.5	Content-distribution networks	
4.3	Implement secure communication channels according to design	
4.3.1	Voice	
4.3.2	Multimedia collaboration	
4.3.3	Remote access	
4.3.4	Data communications	
4.3.5	Virtualized networks	
Domain 5	Identity and Access Management (IAM)	13%
5.1	Control physical and logical access to assets	
5.1.1	Information	
5.1.2	Systems	
5.1.3	Devices	
5.1.4	Facilities	
5.2	Manage identification and authentication of people, devices, and services	
5.2.1	Identity management implementation	
5.2.2	Single/multi-factor authentication	
5.2.3	Accountability	
5.2.4	Session management	
5.2.5	Registration and proofing of identity	
5.2.6	Federated Identity Management (FIM)	
5.2.7	Credential management systems	
5.3	Integrate identity as a third-party service	
5.3.1	On-premise	
5.3.2	Cloud	

2017 CISSP Detailed Content Outline (DCO) with Weights Final
Effective Date: April 2018

2017 CISSP Detailed Content Outline With Weights Final (Public Version)		
Classification	Domain/Task/Subtask	Weight
5.3.3	Federated	
5.4	Implement and manage authorization mechanisms	
5.4.1	Role Based Access Control (RBAC)	
5.4.2	Rule-based access control	
5.4.3	Mandatory Access Control (MAC)	
5.4.4	Discretionary Access Control (DAC)	
5.4.5	Attribute Based Access Control (ABAC)	
5.5	Manage the identity and access provisioning lifecycle	
5.5.1	User access review	
5.5.2	System account access review	
5.5.3	Provisioning and deprovisioning	
Domain 6	Security Assessment and Testing	12%
6.1	Design and validate assessment, test, and audit strategies	
6.1.1	Internal	
6.1.2	External	
6.1.3	Third-party	
6.2	Conduct security control testing	
6.2.1	Vulnerability assessment	
6.2.2	Penetration testing	
6.2.3	Log reviews	
6.2.4	Synthetic transactions	
6.2.5	Code review and testing	
6.2.6	Misuse case testing	
6.2.7	Test coverage analysis	
6.2.8	Interface testing	
6.3	Collect security process data (e.g., technical and administrative)	
6.3.1	Account management	
6.3.2	Management review and approval	
6.3.3	Key performance and risk indicators	
6.3.4	Backup verification data	
6.3.5	Training and awareness	
6.3.6	Disaster Recovery (DR) and Business Continuity (BC)	
6.4	Analyze test output and generate report	
6.5	Conduct or facilitate security audits	
6.5.1	Internal	
6.5.2	External	
6.5.3	Third-party	
Domain 7	Security Operations	13%
7.1	Understand and support investigations	
7.1.1	Evidence collection and handling	
7.1.2	Reporting and documentation	
7.1.3	Investigative techniques	
7.1.4	Digital forensics tools, tactics, and procedures	
7.2	Understand requirements for investigation types	
7.2.1	Administrative	
7.2.2	Criminal	
7.2.3	Civil	
7.2.4	Regulatory	
7.2.5	Industry standards	
7.3	Conduct logging and monitoring activities	
7.3.1	Intrusion detection and prevention	
7.3.2	Security Information and Event Management (SIEM)	
7.3.3	Continuous monitoring	
7.3.4	Egress monitoring	
7.4	Securely provisioning resources	
7.4.1	Asset inventory	
7.4.2	Asset management	
7.4.3	Configuration management	
7.5	Understand and apply foundational security operations concepts	
7.5.1	Need-to-know/least privileges	
7.5.2	Separation of duties and responsibilities	
7.5.3	Privileged account management	
7.5.4	Job rotation	
7.5.5	Information lifecycle	
7.5.6	Service Level Agreements (SLA)	
7.6	Apply resource protection techniques	
7.6.1	Media management	
7.6.2	Hardware and software asset management	
7.7	Conduct incident management	
7.7.1	Detection	
7.7.2	Response	
7.7.3	Mitigation	
7.7.4	Reporting	

2017 CISSP Detailed Content Outline (DCO) with Weights Final
Effective Date: April 2018

2017 CISSP Detailed Content Outline With Weights Final (Public Version)		
Classification	Domain/Task/Subtask	Weight
7.7.5	Recovery	
7.7.6	Remediation	
7.7.7	Lessons learned	
7.8	Operate and maintain detective and preventative measures	
7.8.1	Firewalls	
7.8.2	Intrusion detection and prevention systems	
7.8.3	Whitelisting/blacklisting	
7.8.4	Third-party provided security services	
7.8.5	Sandboxing	
7.8.6	Honeypots/honeynets	
7.8.7	Anti-malware	
7.9	Implement and support patch and vulnerability management	
7.10	Understand and participate in change management processes	
7.11	Implement recovery strategies	
7.11.1	Backup storage strategies	
7.11.2	Recovery site strategies	
7.11.3	Multiple processing sites	
7.11.4	System resilience, high availability, Quality of Service (QoS), and fault tolerance	
7.12	Implement Disaster Recovery (DR) processes	
7.12.1	Response	
7.12.2	Personnel	
7.12.3	Communications	
7.12.4	Assessment	
7.12.5	Restoration	
7.12.6	Training and awareness	
7.13	Test Disaster Recovery Plans (DRP)	
7.13.1	Read-through/tabletop	
7.13.2	Walkthrough	
7.13.3	Simulation	
7.13.4	Parallel	
7.13.5	Full interruption	
7.14	Participate in Business Continuity (BC) planning and exercises	
7.15	Implement and manage physical security	
7.15.1	Perimeter security controls	
7.15.2	Internal security controls	
7.16	Address personnel safety and security concerns	
7.16.1	Travel	
7.16.2	Security training and awareness	
7.16.3	Emergency management	
7.16.4	Duress	
Domain 8	Software Development Security	10%
8.1	Understand and integrate security in the Software Development Life Cycle (SDLC)	
8.1.1	Development methodologies	
8.1.2	Maturity models	
8.1.3	Operation and maintenance	
8.1.4	Change management	
8.1.5	Integrated product team	
8.2	Identify and apply security controls in development environments	
8.2.1	Security of the software environments	
8.2.2	Configuration management as an aspect of secure coding	
8.2.3	Security of code repositories	
8.3	Assess the effectiveness of software security	
8.3.1	Auditing and logging of changes	
8.3.2	Risk analysis and mitigation	
8.4	Assess security impact of acquired software	
8.5	Define and apply secure coding guidelines and standards	
8.5.1	Security weaknesses and vulnerabilities at the source-code level	
8.5.2	Security of application programming interfaces	
8.5.3	Secure coding practices	

Source: ISC² IV, 2017