TALLINN UNIVERSITY OF TECHNOLOGY
School of Information Technologies

Elina Kurr 201720IVSB

# Application of HFACS Model for Minimizing Human Error in Cyber Security

Bachelor's thesis

Supervisor: Kaido Kikkas

Doctor of Philosophy
in Engineering (PhD)

Tallinn 2023

TALLINNA TEHNIKAÜLIKOOL
Infotehnoloogia teaduskond

Elina Kurr 201720IVSB

# HFACS-mudeli rakendamine inimvigade minimeerimiseks küberturvalisuses

Bakalaureusetöö

Juhendaja: Kaido Kikkas
Tehnikateaduste doktor

Tallinn 2023

# Author’s declaration of originality

I hereby certify that I am the sole author of this thesis. All the used materials, references to the literature and the work of others have been referred to. This thesis has not been presented for examination anywhere else.

Author: Elina Kurr

22.04.2023

# Abstract

Human error remains one of the main cyber security threats nowadays. Understanding the causes of human failure is often undervalued and the focus in information security remains on technological solutions. Risky behaviours and errors among employees can lead to cyber security breaches and result in revenue loss and reputational damage to a company. Therefore, it is important to understand causative factors of the errors and recognise possible areas of improvement in an organization.

The Human Factors Analysis and Classification System (HFACS) is a structured human error analysis framework that was initially developed for investigation of aviation accidents and is used to identify areas that are required to be addressed by an organization to minimize future occurrences of human errors. It offers a detailed and structured analysis approach that allows to determine root causes more accurately.

The theoretical part of the thesis includes an overview of the model and a review of literature on its application in a variety of industries. The conducted review indicates the advantages of HFACS implementation and shows that the model can be widely used in various fields.

The practical part of the work in Chapter 5 covers adaptation of the HFACS model and its implementation for analysis of actual risky cyber security behaviours in a focus group of 10 employees in an organization (which for the scope of this paper will be named Company X). The data collection method for the research is qualitative and includes interviews with employees who failed to demonstrate expected behaviour in password security, phishing identification, and physical security.

As a result, this thesis includes a set of reasoned recommendations for practical implementation offered to the Company X for minimizing human error based on the performed analysis.

This thesis is written in English and is 30 pages long, including 6 chapters and 10 figures.

# Annotatsioon

# HFACS-mudeli rakendamine inimvigade minimeerimiseks küberturvalisuses

Inimlikud vead on tänapäeval endiselt üks peamisi ohte küberturvalisuses. Inimvigade põhjuste mõistmist sageli alahinnatakse ja infoturbe fookus jääb tehnoloogilistele lahendustele. Töötajate riskantne käitumine ja vead võivad põhjustada küberturvalisuse rikkumist ning viia tulude kaotusele ja ettevõtte maine kahjustamisele. Seetõttu on oluline mõista vigade põhjuslikke tegureid ja ära tunda võimalikud parendusvaldkonnad organisatsioonis.

Human Factors Analysis and Classification System (HFACS) on struktureeritud inimvigade analüüsi raamistik, mis töötati algselt välja lennuõnnetuste uurimiseks ja mida kasutatakse parandamist vajavate valdkondade tuvastamiseks, millega organisatsioon peab tegelema, et minimeerida tulevaste inimlike vigade esinemist. See pakub üksikasjalikku ja struktureeritud analüüsimeetodit, mis võimaldab täpsemalt määrata algpõhjuseid.

Töö teoreetiline osa sisaldab mudeli ülevaadet ja kirjanduse ülevaadet selle rakendamise kohta erinevates tööstusharudes. Läbiviidud ülevaade näitab HFACS-i rakendamise eeliseid ja näitab, et mudelit saab laialt kasutada erinevates valdkondades.

Töö praktiline osa 5. peatükis hõlmab HFACS mudeli kohandamist ja selle rakendamist tegelike riskantsete küberturbekäitumiste analüüsimiseks 10 töötaja fookusgrupis organisatsioonis (mis käesoleva töö raames saab nimeks Company X). Uuringu andmete kogumise meetod on kvalitatiivne ja hõlmab intervjuusid töötajatega, kes ei suutnud näidata õiget käitumist parooliturbes, andmepüügi tuvastamises ja füüsilise turvalisuses.

Sellest tulenevalt sisaldab käesolev lõputöö läbiviidud analüüsi põhjal ettevõttele pakutud argumenteeritud ettepanekuid praktiliseks rakendamiseks inimlike vigade minimeerimiseks.

Lõputöö on kirjutatud inglise keeles ning sisaldab teksti 30 leheküljel, 6 peatükki ja 10 joonist.

# List of abbreviations and terms

| | |
|---|---|
| ACCIMAP | Accident Mapping |
| Company X | Alias for the IT company where the research for this thesis was conducted. The alias was used for anonymity purposes. |
| DoD | Department of Defense |
| ECF | Events and Causal Factors |
| HFACS | Human Factors Analysis and Classification System |
| HSE | Health and Safety Executive |
| IBM | International Business Machines Corporation |
| KSU | Kennesaw State University |
| RCA | Root Cause Analysis |
| STAMP | Systems Theoretic Accident Model and Process |
| URL | Uniform Resource Locator |

# Table of contents

# List of figures

# 1 Introduction

Human error is one of the biggest threats to cyber security in this day and age. According to Nobles [1], despite the tendency for security investments to increase over the years, companies and organizations are still affected by cyber breaches. The most successful cyber security breaches share human error as a common factor. Businesses are adjusting to constantly evolving information security threats mainly by applying various technological solutions. Even with the implementation of the newest technological means, cyber criminals continue to take advantage of human failure with the use of malware and phishing to get hold of critical data.

Organizations and companies have not yet managed to succeed in introducing effective solutions that would help to address human factors in information security. Understanding the way employees interact with information systems and behave in critical situations is very often undervalued [1].

Recent IBM studies [2] show that information security breaches result in significant revenue losses with an average of USD 4.35 million per breach in the year 2022, while phishing and compromised emails reached the highest average among initial attack vectors. It is worth mentioning that compared to the year 2020, the average cost of a data beach rose by 12.7% [2].

According to the Verizon 2022 Data Breach Investigations Report [3], human failure remains one of the main driving elements of successful cyber security breaches and statistics show that 82% of cases include it as a causative factor. This percentage emphasizes that human behaviour holds a central position in information security [3].

It is important to acknowledge that managing human error in an effective way is the key to achieving cyber security today and in the future. Overall, human factors as a cause result in major consequences in a variety of industries, including aviation, medicine, industrial etc., and there can be different approaches and perspectives on its management.

Introducing effective approaches from other fields can be beneficial for tackling human failure in cyber security.

Information security professionals should have a deeper understanding of human factors to mitigate the role of this aspect in information security. Introducing more strategies to explore behaviour-based risks together with comprehensive assessments could help collect data to identify the causative trends that lead to human error [1].

## 1.1 Problem Statement and Research Questions

As previously mentioned, human error plays a significant role in information security. There are several different risky security behavioural tendencies and repeated errors noticed in a team of employees in an IT company (which for the scope of this paper will be named Company X). Observed behaviours of employees in an examined focus group do not meet expectations in password security, phishing identification, and physical security. Spotted risky behaviours can result in actual cyber security breaches and cost the Company X its reputation and lead to financial losses.

The analysed behaviours include:

- Unsafe practices in generating credentials/passwords in user access management
- Occasional failure to identify simulated phishing emails
- Occasional tailgating

This thesis is aimed at finding answers to the following questions:

- What are the actual factors that either cause or contribute to risky behaviours?
- What are the areas of improvement in the Company X that correlate to the factors?
- What can be done in the Company X to manage and minimize human error?

The goal of this thesis is to understand what can be done to improve the behaviours and minimize human error in the team. To achieve this objective, known investigation and root cause analysis techniques had to be implemented to determine causative factors of examined errors and identify areas of improvement in the Company X.

The Human Factors Analysis and Classification System (HFACS) is widely and successfully used in various industries where human error is critical and can lead to significant consequences [4]. It is applied for investigation and error analysis to diagnose causal individual and organizational factors that lead to an incident or an accident [5]. The purpose of this research is to adapt the HFACS model to actual risky cyber security scenarios and implement it for RCA in a focus group of 10 employees working in one team in the Company X.

The final goal is to offer a set of realistic suggestions to the Company X that can be applied to address the sectors of necessary advancement for minimizing human failure based on the investigation and the final evaluation outcome. It is worth pointing out that identified areas of development include both team-specific adjustments implemented inside the local unit and enhancements to be considered and introduced at a higher organizational level.

## 1.2 Scope and Limitations

Theoretical scope of this thesis includes the role of human error in cyber security, a brief overview of various approaches to human factor management and application of the Human Factors Analysis Classification System for effective handling and control of human failure.

The thesis covers the HFACS model adaptation in accordance with actual undesired cyber security behaviours in the team of 10 employees, qualitative research process conducted in the focus group in the form of individual interviews and consequent evaluation of the collected data. The structure of performed interviews is based on the adaptation of HFACS model Version 7.0.

The final part of the practical contribution is represented by a reasoned action plan with a set of suggestions either practically introduced or considered to be implemented in the future. In addition, a possibility of the HFACS model implementation in risk management in the future is also mentioned. Complete implementation of suggested solutions is out of scope of this thesis.

# 2 Background Information

As recent IBM studies [2] show, companies are facing more security breaches over the years and there is a constant rise in costs consequently. In 60% of cases, organizations had to overlook prices on services or products after revenue loss caused by breaches which had an impact on their customer base. Moreover, 83% of organizations experienced more than one security breach in the year 2022, meaning the issue was repeated.

The leading industries affected by cyber threat actors are healthcare, the financial services sector, the pharmaceuticals, technology, and the energy industries. Among the mentioned industries, healthcare and the financial sector are the primary targets for breaches of sensitive information. Healthcare has remained the costliest in terms of financial loss caused by data breaches for 12 years and compared to 2020 there was an increase in expenses by 41.6% [2].

The latest 2022 Data Breach Investigations Report by Verizon [3] indicates that no organization can be safe without having a good strategy to manage the most prevalent cyber-attack paths, which are compromised credentials, phishing, exploiting existing vulnerabilities and using botnets [3].

According to the 2021 Unisys Security Index [6] conducted in 11 countries in North and Latin America, Asia Pacific, and Europe, nearly 38% of employees do not consider themselves to be responsible for data security while working remotely and 45% of questionees confirmed downloading unauthorized software or applications for the purpose of work [6]. The statistics emphasize a lack of substantial security awareness and understanding of responsibility.

## 2.1 The Role of Human Error in Cyber Security

For many years, human failure has persistently been identified as a major causative factor for cyber security incidents, and examples of serious data breaches triggered by human error are countless till this day. According to Nobles [1], social engineering attacks, information breaches and ransom attacks continue to occur nowadays at levels that are higher than ever before.

Cyber security professionals keep their focus on integrating emerging technologies to defend against persistently evolving security threats. It is common for organizations to make significant investments in advanced technological solutions and shift defence aspects to technology. Human errors in information security do not show a tendency to reduce with the use of new technological means [1].

According to the latest IBM Report [2], stolen credentials and phishing appeared to be the most recurrent initial attack vectors in the year 2022 at 19% and 16% of breaches respectively. As for revenue loss, phishing and compromised emails had the highest average cost by the initial attack vector in the same year and reached correspondingly USD 4.91 million and USD 4.89 million. Furthermore, identifying the breaches caused by stolen credentials and compromised emails took the longest mean time to recognize, with an average of over 300 days each [2].

The Verizon 2022 Data Breach Investigations Report [3] shows that human failure as a contributory factor is driving most cyber security breaches. Looking at the Social Engineering patterns, there is notable domination of phishing in the graphs. Even though the percentage of personnel capable of falling victims to email phishing seems low and remains approximately 2.9% over the years, it indicates persistent vulnerability resulting in actual costly breaches [3].

The way a user responds to security significant events is a critical aspect to be considered for the security of an organization. Human factors objectives could be introduced to cyber security management approaches and the risk assessment process, and the expertise of behavioural specialists involved. These strategies could overall contribute to the development of a stronger organizational culture and improve understanding of human decision-making and its effect on staff performance [1].

## 2.2 Approaches to Human Factor Management

There is a variety of human performance models that can be used for error classification and analysis. According to Karanikas, Chionis & Plioutsias [7], the key principles of contemporary human error analysis approaches imply that human failure is only a symptom of deeper issues within a system. Eventually, all organisational aspects should be explored proportionally during the investigation instead of putting the blame on a

single individual involved in the events. Modern practices support sharing of responsibility and a non-judgmental outlook.

As an example, the Swiss-cheese type of model includes both active errors together with existing hidden problems and their cause-effect interdependencies. The Human Factors Analysis and Classification System (HFACS) is based on principles of the Swiss-cheese model. The Systems Theoretic Accident Model and Process (STAMP) and the ACCIMAP model similarly take an entire organisation with internal cause-effect relationships and connections as a basis for the analysis [7]. According to Igene & Johnson [8], the STAMP model is based on a control structure with emphasis on safety constraints between various components of the system. As for the ACCIMAP model, it includes initiating events that occur, and decisions made in its diagram as factors, together with interconnections between different layers of the system. Another example is the Events and Causal Factors (ECF) approach, which implements a linear model and takes in contributory events in a form of chronological sequence in its chart.

Comparing the above-mentioned models and the potential level of complexity for practical implementation, the ECF and the HFACS models are relatively easy to understand and do not necessarily require previous experience and additional knowledge for conducting the analysis. Regarding the STAMP and the ACCIMAP models, applying these would be more challenging as there is a lack of a clear structured guide for the ACCIMAP and, as for the STAMP model, familiarity with the concept of control theory and prior experience would be highly recommended [8].

The ECF model is quite simple, while it implies that the emphasis during the investigation is made on the chronological sequence of events. The main concept will not necessarily bring a relevant contribution to the research and the analysis process and might not show the broad picture.

The advantage of the HFACS model is that it has a good structure for the analysis, provides a fuller perspective rather than a narrow view on the investigated situation, is proven to be quite flexible for implementation in various industries and it has an accessible and easy to understand guide available.

According to the HSE (The Health and Safety Executive) [9], human factors include three major aspects that can have an impact on behaviour in the work environment – individual,

organisational and job factors. Individual factors can be either unlikely to change, such as personality traits, or changeable characteristics, including skill level, work habits and personal attitude. As for job factors, it is implied that the type of job tasks, workload and working conditions should meet the mental and physical abilities of employees. Regarding organisational factors, they are represented by corporate culture within the company, training programmes, management, and communication. Organisational factors are highly influential on behaviours of employees [9].

It is crucial to understand and acknowledge that human failure should be managed and causal factors that contribute to its occurrence can be controlled. There are two different types of human failure: unintended actions or errors, and violations or intentional misconduct. It is worth mentioning that breaking the rules deliberately is often provoked by an intention to fulfil work tasks rather than being mischievous wrongdoing [10].

Recognizing the difference between various types and understanding the nature of human failure are the keys to its identification and effective management. A structured analysis approach in risk assessment is essential for a successful evaluation and having a broader perspective during the root cause analysis process, rather than narrowing down causative factors to individual accountability of an employee, is important.

# 3 Literature Review

This chapter gives an overview of the HFACS model that was chosen for the analysis and identifying factors leading to risky behaviours in the focus group. Cases of successful implementation of the model in various fields are also included in the chapter.

## 3.1 Overview of Human Factors Analysis Classification System

The Human Factor Analysis and Classification System was originally developed back in 1997 as a framework for evaluating occurring aviation accidents [11]. It is a well-structured and organized model that systematically covers all behavioural aspects potentially leading to an incident and is used as a tool for mishap investigation and prevention [5]. The HFACS model is currently applied to understand the role of human factors in incidents and determine existing causative factors within an organization. Today, it is widely implemented in aviation for tracking human error in plane crashes. Development of HFACS introduced a structured classification scheme for human error and contributed to defining it in a more comprehensible way [11].

According to the DoD HFACS guide [5], incidents are caused by individual and organizational factors which can also be referred to as causal and contributory. Causal factors imply a direct cause-effect relationship in regard to the events and contributory factors are conditions within the system that impact the situation and form a progressive sequence leading to the events [5]. This outlook allows to better understand the nature of occurring failure and internal dependencies of various factors in a multi-level scheme.

The Swiss-cheese model can be viewed as a sequence of preventive barriers that are supposed to mitigate or stop incidents from happening. Most organizations mostly have four levels of barriers in place all together. The barriers are interconnected and the ones at the top of the scheme, such as organizational influences and unsafe supervision, appear to be the most influential and have an impact on the levels placed lower in the system. Eventually, holes in the barriers represent gaps, problems, and misses, both individual and organizational, that, forming a combination, lead to adverse events [4].

The Human Factor Analysis and Classification System is based on the model of latent and active failures, dividing human error into four levels. These are unsafe acts of

operators, preconditions for unsafe acts, unsafe supervision, and organizational influences. The unsafe acts level can be broken down into two categories - errors and violations. Errors are unintended actions in comparison with violations that imply a conscious deviation from the existing procedures [12]. The scheme of the HFACS framework can be found in Appendix 2.

Errors are divided into three subcategories as follows:

- Skill-Based Errors: Errors which take place during performance of a highly practiced routine and occur unconsciously either by failing to pay attention or falling into a bad habit.

- Decision Errors: Errors which take place when performed actions are intentional however the choice of an action plan appears not suitable for the situation and fails to achieve an expected result [12], they are driven either by inappropriate choices or misconception of information [4].

- Perceptual Errors: Errors which occur when initial information was inaccurate or invalid and consequent decisions made and incorrect actions followed as an outcome [12].

In information security, users tend to make incorrect decisions in critical situations mainly due to false assumptions made and the lack of training. There is a tendency for a lack of proper risk perception among system users that malicious actors often take advantage of to achieve security breaches. It is worth mentioning that both users and system administrators may fall victims to cyber-attacks [11]. The causative nature of the above-mentioned types of errors is different, so it requires addressing different areas within an organization for taking further corrective and preventive measures. Introducing basic principles of HFACS for analysing human errors in the cyber security incident management process would offer a new perspective on the matter for organizations to tackle most common trends and conduct deeper root cause analysis.

## 3.2 Application of HFACS in Various Industries

As has already been mentioned, the Human Factor Analysis and Classification System is widely implemented in aviation safety. Studies [13] prove that higher organizational

levels have a flow-on effect on the lower levels of organization and are inevitably influential in the occurrence of plane crashes. A detailed HFACS based analysis of the Asiana Airlines flight 214 accident in the year 2014 showed that the crash could have been averted and human lives saved. Due to its systematic and cautious approach, applying the HFACS model can prevent aviation accidents from happening and contribute to mitigating the major consequences [13].

In addition to that, the HFACS framework has proven to be effective in implementation in other sectors including the medical industry, mining, the construction sector, railway etc. Studies held in the pharmacy department of a public hospital in Bandung by the Bandung Institute of Technology [14] identified reasonable causal factors of medication error to be addressed, such as fatigue and information overload and helped the pharmacy department to indicate necessary improvements to be introduced [14].

Recent research in mining accidents in Iran [15] outlined the main factors, including inappropriate planned operation and environmental factors, as the most influential in the examined unsafe acts. The results of the study demonstrated the effectiveness of the HFACS framework and its contribution to the strategic development for further mitigation of errors that cause both fatal and disabling injuries [15].

Another study on the HFACS application in construction accidents in China in 2018 [16] showed how decisions made by management at a higher level can contribute to accidents and helped to evaluate the need for overlooking existing regulations and safety guidelines. The results of the research indicated meaningful improvement areas for construction safety [16].

In the year 2017, during the KSU (Kennesaw State University) Conference, it was suggested that it would be beneficial to introduce the Human Factor Analysis and Classification System to the information security incident analysis process to minimize the frequency of human errors [11]. Previous studies imply that the framework can be flexible for application in various sectors and appears to be an effective analysis tool. The DoD HFACS 7.0 Guide gives a comprehensive description and guidelines for the analysis and a detailed basis for interview questions [5].

# 4 Methodology

The chosen data collection method for the research is qualitative and includes interviews held in a focus group of 10 employees. Sampling is not random, and every participant of the observed focus group has encountered a risky cyber security situation failing to demonstrate expected behaviour in terms of information security. Every single employee in the examined team has committed at least one of the investigated security violations, and, therefore, can contribute to rich data collection for the research. Purposive sampling implies that selected participants can be a proper informational source for the analysed phenomenon [17] which, in this case, is actual human failure in information security. Analysed scenarios that were previously spotted and observed include incorrect behaviours in password security, phishing identification, and physical security, such as unsafe practices in generating credentials/passwords in user access management, occasional failure to identify simulated phishing emails, occasional tailgating, and are described in more detail in Chapter 5.1.

One of the goals of the conducted qualitative research is to achieve data saturation [17] and make sure that both causal and contributory factors are identified during the interviews and the results of the data collection include existing patterns and a sufficient variety of discovered factors. Both face-to-face in-depth interviews and additional focus group discussions have been held. Individual one-on-one meetings were initially included in the research plan while open brainstorm discussions appeared as a part of the emerging research process design.

The structure of the interviews is based on the DoD HFACS Guide [5] and five whys technique. The HFACS guide incorporates all factors potentially influential on human performance in an organised way and provides a structural basis for investigation and analysis. The suggested flow of closed questions starts with Acts or Active Failures, moving on to Preconditions or Latent Failures and ending up with Supervision and Organizational Influences [5]. Each relevant for checking factor was incorporated into the planned structure of interviews in the form of a closed Yes/No question.

Considering that not all the listed factors in the HFACS Guide are relevant to information security and particularly to the analysed scenarios, the initial HFACS model was adapted in accordance with the investigated situations for this research and irrelevant factors

excluded from the potential pool of interview questions. The adaptation process is covered in more detail in Chapter 5.2.

In addition to the HFACS based flow of questions, the series of conducted interviews started with a brief open conversation with the use of five whys technique [18]. The purpose of this kind of conversation starter was to encourage the participants to speak their minds more openly without pressure or a forced structure at first to get a broad look on the situation in general [17]. Five whys method is a well-known investigation technique applied for identifying cause-and-effect dependencies. This method implies answering successive open why questions in a row to reflect on the problem and understand systemic causes [18]. During this research, five whys technique was used mostly as a supporting activity and not as a primary investigation tool.

Throughout the interviews, the employees were encouraged to comment on their answers freely and give clarifications and reasoning for their choices. In case any special emphasis was made, or attention brought to a particular factor during the conversations, it was also documented. Similarly, open focus group discussions were held on phishing identification and physical security to stimulate sharing experiences in more depth and detail [17].

Additionally, covering some of the factors such as adequacy of organizational training and procedural guidance required additional research along with the held interviews for a fuller and more precise picture. The series of interviews were followed by the in-depth analysis of operational instructions and guidelines, onboarding process and daily procedures.

# 5 Solution Development

This chapter is dedicated to the practical contribution to the thesis and includes a description of the analysed behaviours in the focus group, adaptation of the Human Factors Analysis and Classification System, data collected during the interviews, identified factors, analysis of areas for potential improvement within the organization, the suggestions made to the Company X as a possible fix and the feedback received in the response.

## 5.1 Problem Description

As already mentioned, there are several behaviours that do not meet expectations in terms of information security in a team of employees chosen as a focus group for the qualitative research. The wrong cyber security behaviours occur in password security, phishing identification, and physical security on a regular basis and can pose an actual threat to the Company X.

The team of employees is responsible for user access management daily and most of the participants fail to comply with basic password security requirements while generating and providing credentials to the users. Temporary passwords are often copy-pasted for various accounts and lack the necessary complexity. Therefore, credentials for newly created accounts can be predictable. Weak and repeated passwords can potentially lead to account takeovers and data breaches. The described behavioural trend is consistent among employees and raises apparent security concerns.

The second risky cyber security behaviour that was noticed is occasional failure to identify simulated phishing emails received in the corporate mailbox. Some of the employees admitted to having clicked simulated malicious links or downloaded the attachments. Additionally, half of the team members were not familiar with the correct procedure for reporting phishing emails to the security team and, therefore, did not proceed with expected actions. Phishing is currently one of the biggest cybersecurity threats and, therefore, difficulties in its identification among employees can be considered an obvious vulnerability.

Lastly, looking into physical security, another spotted negative trend is tailgating, which is common in cases when a security badge is accidentally forgotten and left at home or lost. Employees without a badge tailgate rather than proceed with getting a temporary visitor badge as required. A casual attitude towards tailgating tends to form a negative organizational culture in terms of daily information security awareness and concern among the employees and consequently expose the organization to security threats.

## 5.2 Adaptation of the HFACS Model

As previously described, the HFACS model was initially developed for application in the aviation industry [11]. However, it has proven to be flexible and successfully used in a variety of sectors. Implementing the HFACS model in information security requires its adaptation. The process of adaptation implies going through the complete selection of factors in the initial model and eliminating the ones that are not relevant to cyber security situations. Moreover, during this research, three particular information security scenarios were analysed and, therefore, the list of interview questions was composed in accordance with the discussed situations. The complete list of questions after adaptation can be found in Appendix 3.

According to the DoD HFACS Guide [5], the main categories of factors are Acts, Preconditions, Supervision and Organizational Influences. Acts and Preconditions categories refer to the Person-Level Factors and the Mishap-Level Factors include Supervision and Organizational Influences. The layer of Preconditions is very broad and consists of Environment, Physical and Mental State and Teamwork. The Supervision category covers Supervisory Violations, Planned Inappropriate Operations, and Inadequate Supervision. The very upper level of Organizational Influences consists of Resource Problems, Personnel Selection & Staffing, Policy & Process Issues and Climate/Culture Influences. Each subcategory includes a list of multiple concrete factors to select from.

It is worth mentioning that it is crucial to move up above the lowest level of the scheme during the investigation as the layers placed above are the ones that can strategically be influenced in perspective. The level of Acts or Active Failures covers mistakes made by an individual that are not highly manageable from an organizational point of view. The factors included in this category were also incorporated into the interviews. However,

they are not a focal point of the research as the goal of the thesis is to determine practically implementable and potentially effective solutions for minimizing human failure in the Company X based on the conducted research. Therefore, during the conversations, the participants were mostly welcome to elaborate on the causal factors from the three upper layers of the model.

Looking into the Environment subcategory in the Preconditions layer, it is mostly specific to the transportation industry, and it can be divided into Physical and Technological Environment. Physical Environment mostly includes weather and climate conditions affecting performance, whereas Technological Environment refers to work equipment that can appear inadequate or problematic and influence the actions of an employee in a negative way. Both subcategories are irrelevant to the analysed cyber security scenarios and were excluded from the checklist of potential factors.

Another subcategory of the Preconditions is the Physical and Mental State. This subcategory consists of Physical Problems, State of Mind, Sensory Misperception and Mental Awareness. Physical Problems are physiological or medical states of employees that could contribute to an incident. The State of Mind mostly refers to personal characteristics of an individual that affect performance and Mental Awareness is mainly related to control of distractions and management of attention. The subcategory of Sensory Misperception does not appear to be very relevant to information security situations as it includes various types of distortions, illusions, and disorientations specific to motion in space and time. This subcategory of factors was also kept out of the research.

Supervision is the next layer of factors and is limited to the local unit in comparison with the Organizational Influences that imply an impact outside the local unit [5]. All the factors related to training programs and procedures in place on both levels were included for checking during the interviews as well as examined separately in detail after the conversations. The reason for additional inspection was to ensure accuracy of information in regard to training materials that could potentially be misjudged by the participants.

The same approach applied to guides and operational instructions that were analysed afterwards. Both actual consistency of needed materials and the ability of employees to retain knowledge were taken into consideration while analysing the related contributory factors.

## 5.3 Data Collection and Identification of Factors for the Analysis

During this research, three different risky cyber security behavioural tendencies within a team of employees were analysed. Data for the analysis was collected in the form of individual one-on-one interview sessions that were based on the adapted version of the DoD HFACS Guide [5].

In a focus group of 10 employees, every participant was involved in at least one critical situation. Among the investigated scenarios were consistent usage of insecure temporary passwords in the user access management process, occasional failure to correctly identify simulated phishing emails and tailgating in physical security. During the interviews, the participants were encouraged to comment and elaborate on their answers to understand the fuller picture.

The most frequently repeated violation among the employees was failure to comply with the password security requirements during creation of user credentials for various accesses. 9 out of 10 team members persistently used easily guessed temporary passwords on a regular basis.

Based on the collected information, the results of the conducted research indicated that there were several causal and contributory factors leading to the mentioned behavioural tendency among the participants.

Firstly, it was a Widespread/Routine Violation (AV002), meaning it was rather systematic within a local unit. It is most likely that the described behaviour initially occurred as an individual violation and then spread further as a negative example during the onboarding process and mentoring sessions for the newcomers. The violation was not timely disciplined and, therefore, turned into habitual behaviour within the team. Moving on to the Supervision layer, Failure to Enforce Existing Rules (SV001) as well as Allowing Unwritten Policies to Become Standard (SV002) can both be considered influential factors in the above scenario.

Continuing the investigation at the Supervision level within a local unit, there was clearly a Failure to Provide Proper Training (SI003) and Appropriate Policy/Guidance (SI004). Both factors are valid for the local unit only and not for the organizational level, as there are gaps identified in the local training and guidelines compared to the formal

organizational training that is complete and clear for understanding. The local introductory training in terms of the password security requirements in user management was misleading and taught by example, while correlating operational instructions in use had these requirements missing. In addition, one more supervisory factor was spotted as there was a Failure to Identify/Correct Risky or Unsafe Practices (SI007) that were spread among the employees during an extensive period of time.

Looking at the upper-level influences, one factor in this category can be considered valid and contributory as most of the team members referred to the high Pace of Ops-tempo/Workload (OP001). Using the same copy-pasted temporary passwords for multiple user accounts created at once instead of generating random passwords each time was less time-consuming and helped to keep up with the daily workload.

Overall, the above-mentioned factors are consistent for the participants and there is a clear causal pattern for the analysed behavioural trend. Faulty actions are systematic among the participants and are not accidental or occasional. The identified factors for risky behaviour in password security are represented in the Figures 1 and 2.

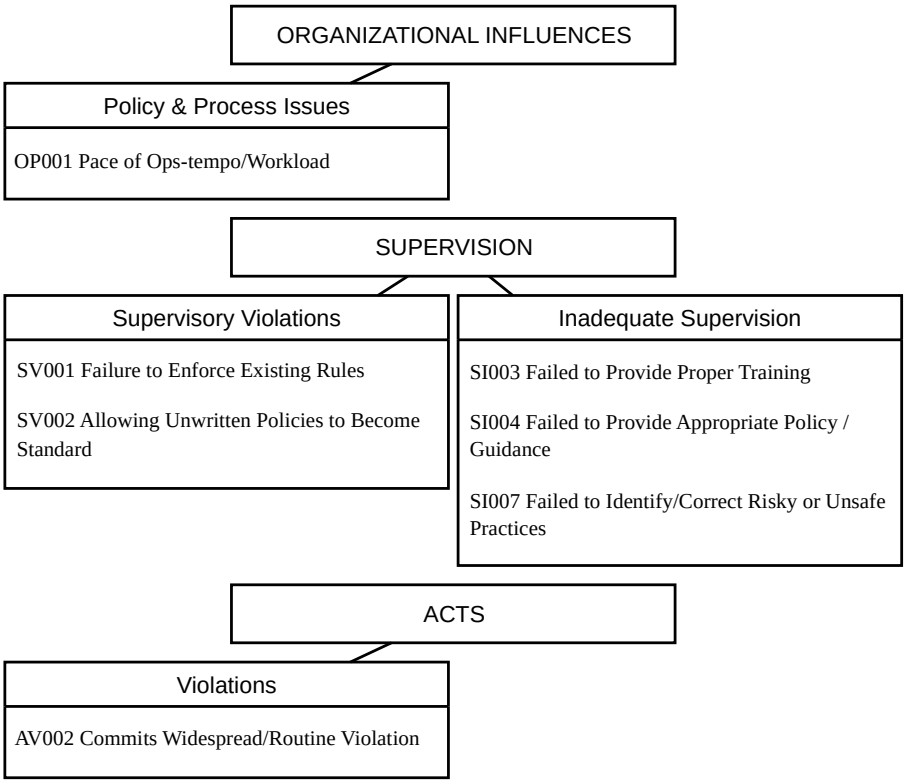


Figure 1. Identified factors in password security (generating credentials).

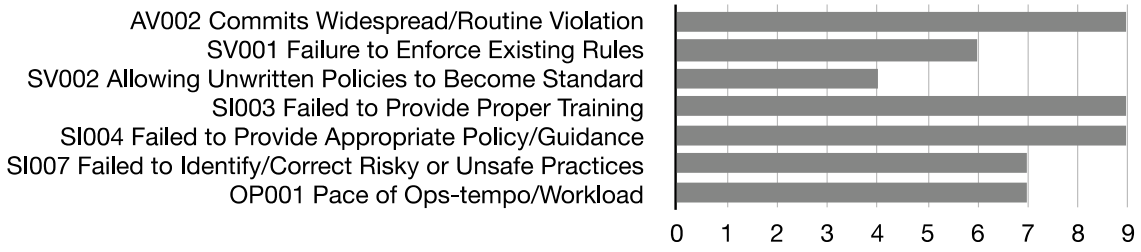


Figure 2. Frequency of factors in password security (generating credentials).

Another risky security behaviour that was analysed appeared in interaction with simulated phishing emails, resulting in difficulties identifying the threat for some of the employees and following incorrect actions including downloading the attachments, clicking the URLs and failure to report suspicious emails according to procedure. The identified factors for risky behaviour in phishing identification are represented in the Figures 3 and 4. Summing up the results of the interviews, repeated answers among the participants appeared for several factors including Pace of Ops-tempo/Workload (OP001), Not Paying Attention (PC101) and Emotional State (PC204).

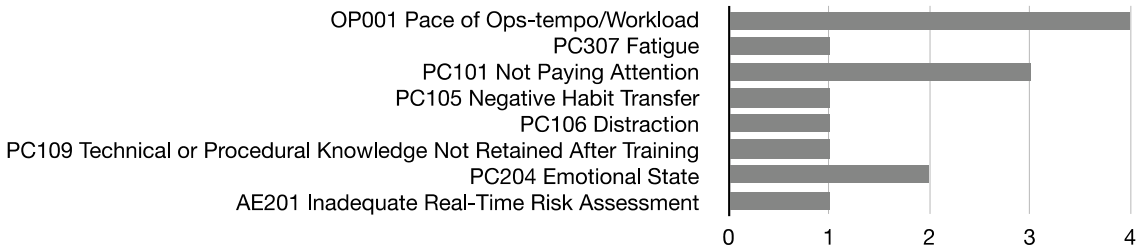


Figure 3. Frequency of factors in phishing identification (simulations).

The participants admitted not paying enough attention due to the volume of other tasks and high workload in general. Checking personal and shared mailboxes is considered a secondary task with lower significance compared to primary responsibilities. The amount of time that can be spent on thorough reading of emails is often limited because of daily prioritization of other tasks. Additionally, getting emotional about the email content and consequently being led by an emotional state was also common. The participants were influenced by emotions in cases when simulated phishing emails were related to payroll changes.

Among the other mentioned factors were Fatigue (PC307), Distraction (PC106), Inadequate Real-Time Risk Assessment (AE201), Negative Habit Transfer (PC105) and Technical or Procedural Knowledge Not Retained after Training (PC109).

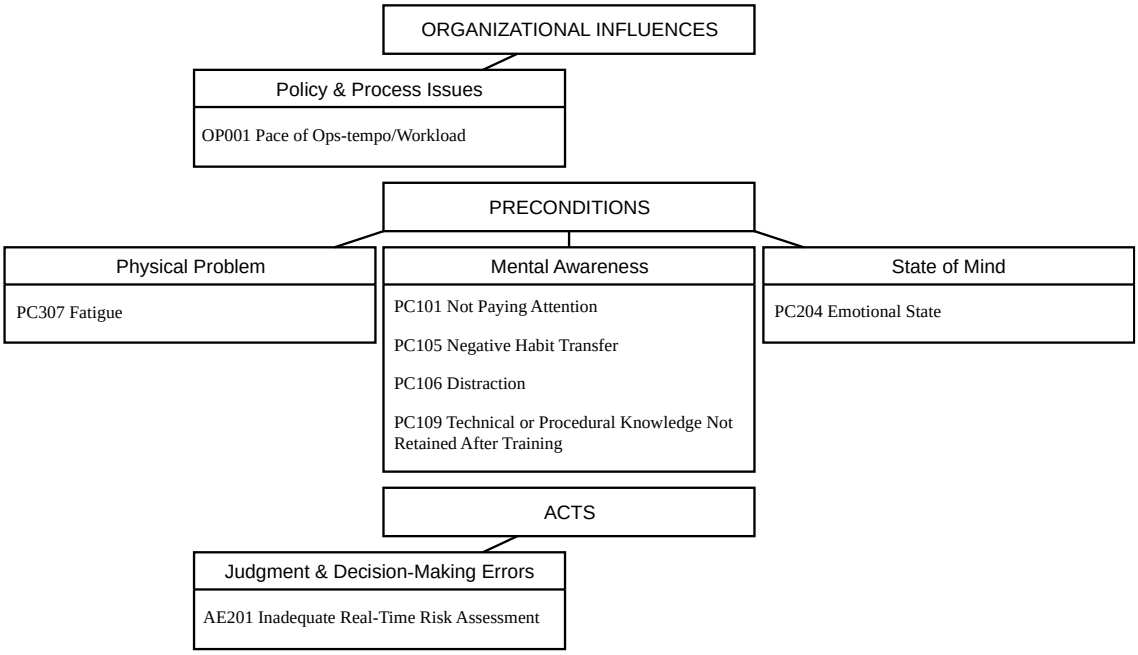


Figure 4. Identified factors in phishing identification (simulations).

Looking into details received from the comments, team members can experience fatigue at work due to lack of sleep and an overall poor sleep schedule. The combination of morning, day and night working shifts and constant working time rotation affect the quality of sleep among the team members. In addition to that, an insufficient number of employees on shift during the day leads to the necessity of multitasking and results in distraction and interruption of attention. There was also a possibility of a habitual daily action of downloading attachments in work emails mentioned, while it could also be considered a rushed action due to the work pace.

Regarding the organizational Information Security Awareness Training, it is assigned to the employees once a year regardless of onboarding time when an employee joins the company. It appears that in some cases, the participants either could not recall well the content of the training or had the training long after the first working day.

As for the expected behaviour while receiving a suspicious email, there is a procedure for reporting it to the security team. It appeared that half of the team members were not familiar with the possibility and necessity to report phishing timely.

Additionally, an open group discussion showed that there were doubts among the employees regarding the learning value of repeated simulated phishing emails as they

were overall quite similar. The team members admitted that they mostly learned to spot a simulated phishing email rather than an actual one.

Moving on to physical security, all employees are obligated to wear security badges and use them for entering the building. This information is present in the organizational Information Security Awareness Training, and it is well emphasized in the course that tailgating should be omitted. However, in cases when a security badge is forgotten, employees tailgate to enter the office which happens occasionally. The identified factors for risky behaviour in physical security are represented in the Figure 5 and Figure 6.

The interviewees expressed an overall relaxed attitude and no concern about this behaviour. Additionally, it appears that alternative options in such cases were not clear to the interviewees. In terms of factors, this kind of behaviour is a Work-Around Violation (AV001) as the requirements are known but violated with the intention of fulfilling work obligations and starting a work shift on time.

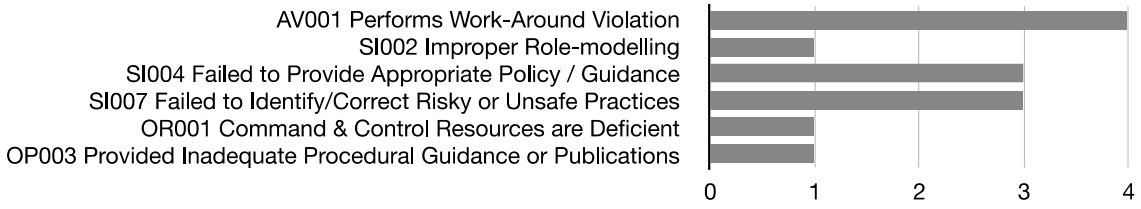


Figure 5. Frequency of factors in physical security (tailgating).

During the interviews it appeared that the participants were not aware of any other ways to act in the described scenario. Regarding available alternative courses of action, there is an opportunity to get a temporary visitor badge, if necessary, but the interviewees were not familiar with this option available.

As for the Supervision level, there was a Failure to Identify/Correct Risky or Unsafe Practices (SI007), Failure to Provide Appropriate Policy/Guidance (SI004) and Improper Role-Modelling (SI002) in the local unit. Tailgating was not commented on or discussed and there was a case of setting a negative example for a supervisee while being familiar with the correct alternative.

In addition to that, it is important to understand that the issue is not limited only to individual violations and supervision. Further investigation showed that there were existing gaps at the organizational level and that temporary visitor badges were not

tracked, were not timely deactivated and could remain in possession of an employee for an extensive amount of time. It also appeared that overall monitoring for violations at the organizational level was not sufficient. The described flawed situation and poor procedures refer to Policy & Process Issues among Organizational Influences, and the factors are Inadequate Procedural Guidance or Publications (OP003), and Command & Control Resources are Deficient (OR001) [5].

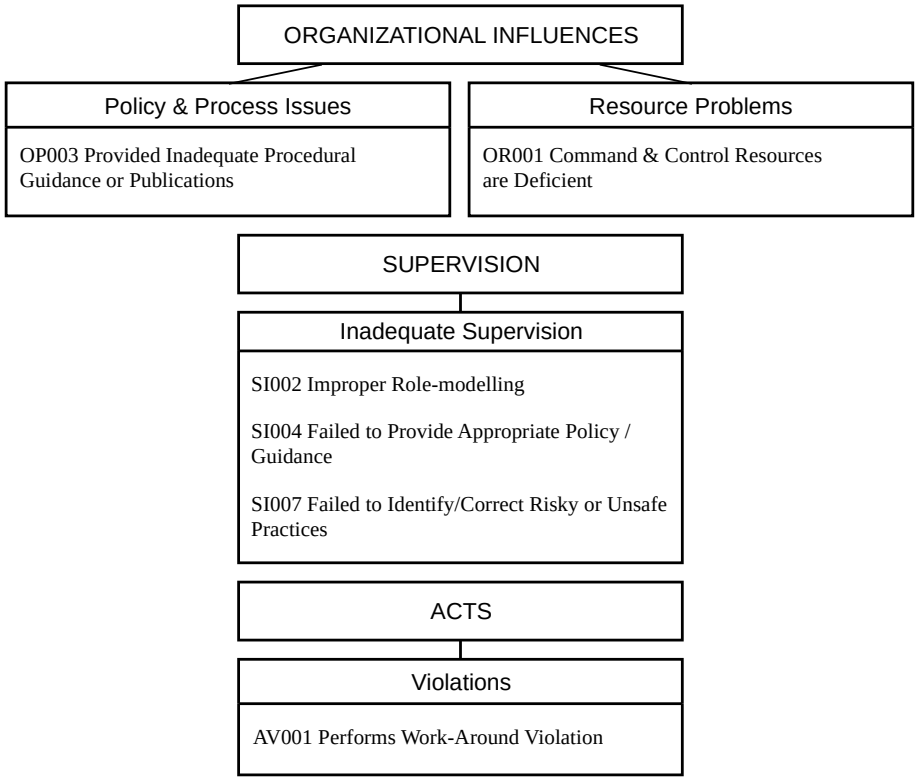


Figure 6. Identified factors in physical security (tailgating).

## 5.4 Identifying Areas of Improvement

To identify potential areas of further improvement, additional analysis of the training material and operational instructions was conducted. Both organizational and local training methods were examined, and existing guidelines followed by the team were inspected. Some of the aspects regarding the known processes in place were clarified with the management.

Analysing the organizational Information Security Awareness Training in detail, it appears to be clear and well informative. The training covers all the three aspects of information security investigated during this research. Overall, the training is

comprehensive and includes enough visual examples for better understanding. However, information on the procedure for reporting suspicious emails is very general. The exact steps are not obvious and require clarification for taking expected actions.

The Information Security Awareness Training is completed by employees once a year and does not depend on the hiring time. For this reason, an employee can end up completing the course sometime later after joining the company and be unaware of expectations and requirements in terms of information security before passing the training.

Looking into the onboarding training plan within a local unit, it does not contain Information Security Awareness Training or any other information on security requirements. Onboarding process includes going through operational instructions one by one with an assigned mentor.

There are several guidelines on user management for various accesses, while none of them has the basic password complexity requirements for the generated credentials mentioned. Most of the user access requests require manual creation. Among the listed necessary tools for work that are introduced to the newcomers, there are no recommendations or mentioning of password generator options.

Moving on to the daily workload within the team, it is reasonable to assume that the volume of tasks exceeds the human resources that are available. One of the reasons for daily under staffing is 24/5 coverage and an overall high employee turnover rate. A shortage of human resources in the local unit often results in a single team member out of the team completing all daily tasks at once and either multitasking or prioritizing more urgent responsibilities over the rest of the tasks left in a backlog. The outcome of the interviews clearly indicated that the level of workload had a significant influence on the behaviours and wrong choices made in phishing identification and unsafe practices in password security.

Among other identified contributory factors, fatigue of employees due to a lack of sleep was also mentioned. 24/5 coverage requires regular working time rotation between morning, day, and night shifts. Taking into consideration the above-mentioned issue with under staffing, it appears hardly possible to compose a well-balanced monthly schedule for the team members.

Individual schedules are often meant to fulfil the needs of the company rather than contribute to a healthy sleep schedule for employees. For one week, all types of shifts, including morning, day, and night-time, are often scheduled for a team member. There is no separation by weeks and no time for a gradual sleeping regime change. In addition, this aspect of work conditions consequently affects employee satisfaction and the turnover rate as a result.

Looking again at the Figures 1 and 6, it is visible how the factors at the supervisory level can be significantly influential on the behaviour of the employees. A leader is a role-model who sets an example to follow, has an opportunity to observe the behaviours of the supervisees daily and should correct unsafe practices once noticed.

It is also worth mentioning that the situation with password security related to daily responsibilities in user access management and the process of generating credentials is a team-specific trend within the local unit. As major causative factors appeared at this level, it would be optimal to address the issue from this perspective and understand that organizational measures at a higher level would be excessive and not suitable for the behavioural trend within the unit. Additionally, due to the number and variety of provided accesses and systems involved, a universal technical solution at the organizational level would not be feasible.

As for the current situation with security badges, similarly there was an obvious influence at the supervisory level. In addition to that, indirect organizational influences such as flaws in the procedure for issuing visitor badges related to tracking of the badges and possibly insufficient monitoring of violations such as tailgating, from the organizational point of view, should also be considered.

## 5.5 Suggestions for Further Improvement

Based on the conducted analysis of areas for further improvement in the organization, several reasoned suggestions for implementation were made to the Company X. These suggestions cover adjustments to the onboarding training plan for the newly hired employees, changes to operational instructions in place within the local unit, revision of related procedures, advised principles of monthly scheduling and overlooking the current hiring plan. Examples of suggestions can be found in the Figures 7, 8 and 9.

Starting with the onboarding process, it was offered to include the organizational Information Security Awareness Training in the training plan for the newcomers. It is important for the new employees joining the company to know and understand requirements and expectations in terms of information security from the start, to avoid confusion and possible risky cyber security behaviours. As the onboarding training is composed and courses for self-learning can be assigned by the supervisor, the timing of the mentioned training can be managed at the supervisory level.

The Information Security Awareness Training should be complete and possibly include currently missing information on phishing reporting procedures.

As it was mentioned during the interviews that procedural knowledge was not always retained after the training and was sometimes forgotten, increasing the frequency of the awareness training during the year could be considered. Assigning a dedicated time for its completion during the training plan instead of picking a random time during the shift among other work tasks would also be preferable. The outcome of the conversations showed that the interviewees were overloaded with daily work and, therefore, a dedicated time slot for learning would be beneficial for retaining the necessary knowledge.

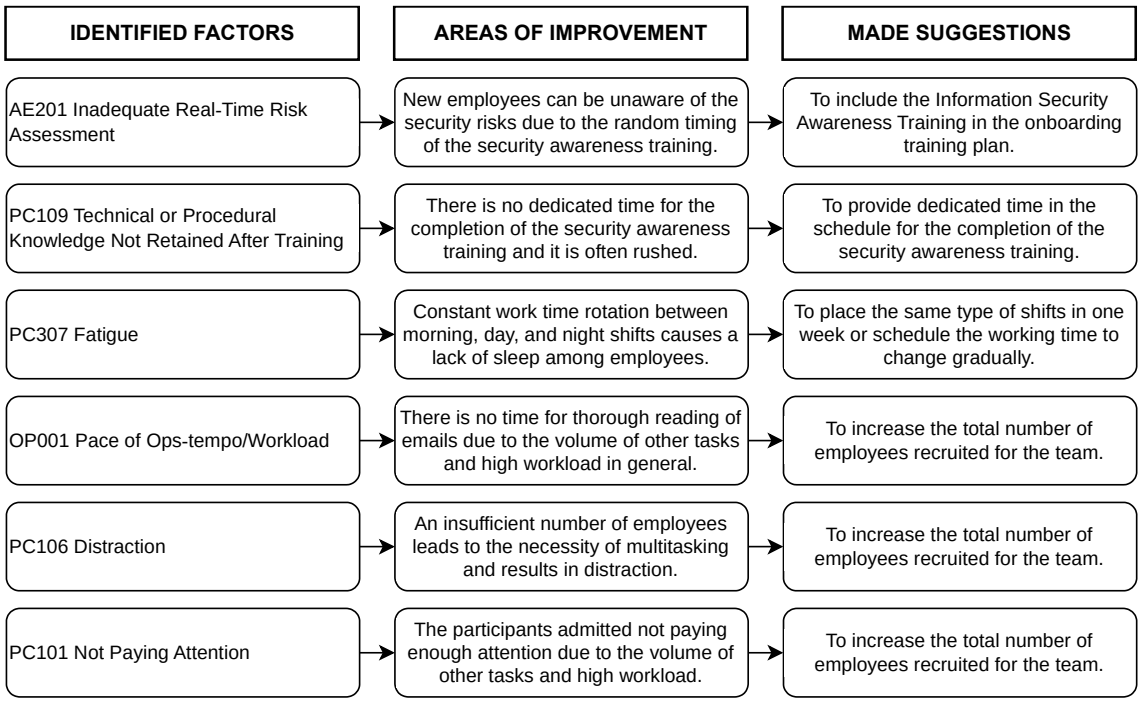


Figure 7. Factors affecting phishing identification and corresponding suggestions.

Considering simulated phishing emails to be a practical part of information security training and taking into consideration the open discussion with the team members on the topic, as similarity of repeated simulated phishing emails was mentioned, to achieve sufficient learning value, versatility of patterns and templates for creation of simulated emails would be beneficial.

The content of the organizational Information Security Awareness Training and following phishing simulation campaigns can only be adjusted at the organizational level.

As was previously mentioned, basic password security requirements for account creation were not present in the corresponding operational instructions on providing user access. Taking into account that the interviewed team members are responsible for granting several different types of accesses and permissions and there is a separate instruction or guideline for each type, it was suggested to either include a brief mentioning of requirements for password complexity in each user access management related instruction as a needed step or introduce a separate guideline on expected password generation process valid for all accesses and link the one to the existing instructions in place.

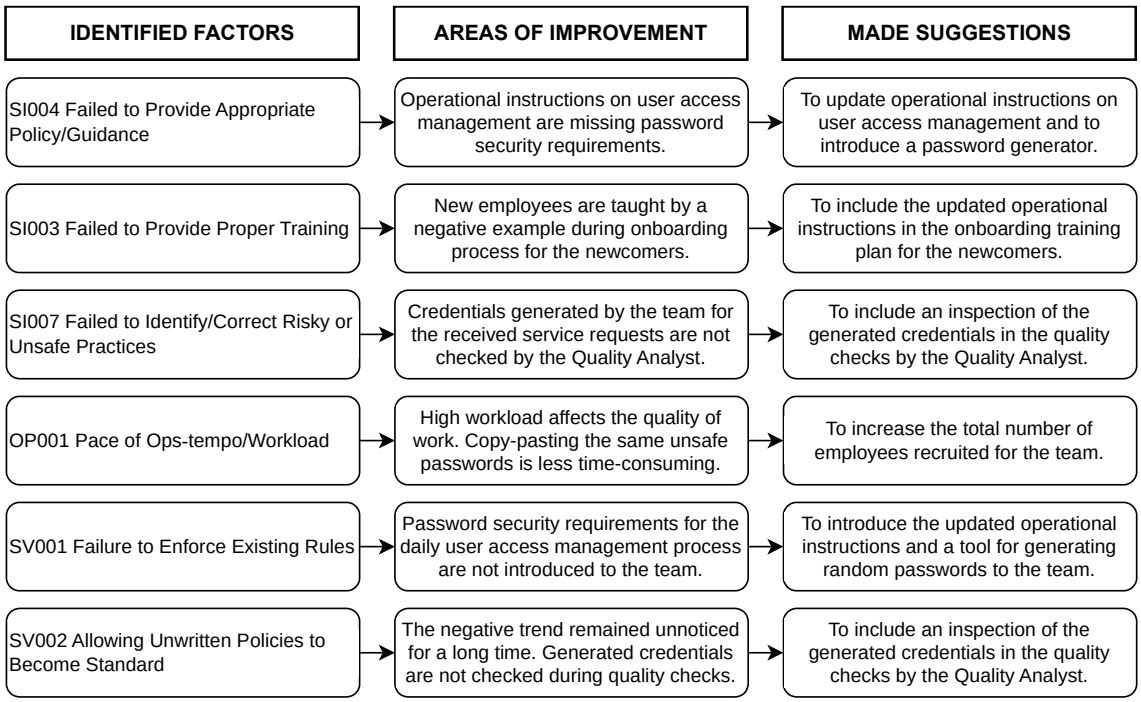


Figure 8. Identified factors in password security and corresponding suggestions.

As it was previously identified that the negative behavioural trend in password security remained unnoticed for an extensive period of time, it was advised to include the check for the generated credentials in the existing quality control procedure for user management, so that it would be monitored in the future.

In addition to that, it was advised to introduce a tool for generating random passwords that was necessary for completion of daily tasks related to user access management. The list of tools for work and guidelines for installation and registration if needed is provided to an employee during the onboarding process. There are several options for password generators available that allow to define a set of characters used for password creation in accordance with the security requirements. Adding a brief instruction on how to apply a tool was recommended.

Both adjustments, including the introduction of the password manager and the update of the operational instructions, can be done at the level of the local unit. There is no additional confirmation from the upper level required and the changes can be easily implemented and introduced to the team.

Taking into consideration that during the interviews such factors as a high workload, fatigue and distraction were mentioned and that the number of daily tasks per team member on shift can affect attention management and quality of work, adjusting the current recruitment plan for the team was suggested.

The decision to overlook hiring strategies for a local unit is made on the organizational level and must be approved by upper management. A noticeably high workload not only leads to a regular backlog of tasks but also contributes to the stress level and overall dissatisfaction with work among the team members and leads to higher attrition of employees.

Moving on to scheduling possibilities, achieving more flexibility in the placement of shifts would be possible if the human resources of the team were increased. The team members complained about the lack of sleep and chaotic work schedules affecting the quality of sleep. Even though the team operates 24/5 on a regular basis, it is still possible to achieve more balance in the work regime by either placing the same type of shifts in a week for an employee or scheduling the working time to change gradually. It was offered to avoid mixing early morning and night shifts in one week for a single team member and

to make sure that the switch of shifts goes from morning to evening and from evening to night or, if necessary, vice versa. However, keeping the same work schedule weekly and making the switch over the weekend is preferable.

Monthly schedules are composed by a local manager of the team and the change of the process does not require the involvement of the upper management. Therefore, the scheduling issue can be resolved at the supervision level. However, additional recruitment possibilities are approved at the organizational level.

Lastly, looking into occasional tailgating among the team members, there is room for improvement. To fix the existing behavioural trend, changes at the organizational and supervisory levels should be considered.

A clear and secure procedure for issuing temporary visitor badges is needed. Access should be temporary and the time of the active state of the badge issued must be clearly defined. It would be reasonable to have an expectation and agreement on when the visitor badge should be returned.

Additionally, it was advised to share existing information on the procedure for issuing visitor badges with the team at the supervisory level so that the employees would be familiar with it.

| IDENTIFIED FACTORS | AREAS OF IMPROVEMENT | MADE SUGGESTIONS |
|---|---|---|
| SI004 Failed to Provide Appropriate Policy/Guidance | Employees are not aware of the procedure for issuing temporary visitor badges if a badge is forgotten. | To share information on the existing procedure among team members at the supervisory level. |
| SI007 Failed to Identify/Correct Risky or Unsafe Practices | Tailgating remains unnoticed and is not commented. | To correct unsafe practices once noticed at the supervisory level and explain the procedure for issuing visitor badges. |
| OP003 Provided Inadequate Procedural Guidance or Publications | Gaps in the existing procedure. Issued badges are not tracked. | To perform regular audits of the issued visitor badges. |
| SI002 Improper Role-modelling | A single occasion of being a negative example. | To lead by example and adhere to existing procedures. |
| OR001 Command & Control Resources are Deficient | Tailgating not sufficiently monitored at the organisational level. | To monitor security cameras for violations on a regular basis. |

Figure 9. Identified factors in physical security and corresponding suggestions.

The current lack of requirements at the organizational level and communication at the supervisory level leads to a negative behavioural trend and a casual attitude towards tailgating in general, commonly used as a workaround for entering the office building. Considering possibilities for improvement at the organizational level, performing regular audits of the issued visitor badges and monitoring cameras for violations, including tailgating, on a regular basis would be beneficial.

## 5.6 Feedback and Future Work

The results of the analysis and a set of suggestions for further improvement were presented to the Company X and the received feedback was overall positive. The recommended measures and actions will either be implemented or considered for introduction in the future, depending on the complexity of the process approval and organizational implementation.

The changes that can be applied to the supervisory level in the local unit are the easiest for actual implementation. These include updating the operational instructions on user access management for the team, adjusting the initial onboarding training plan for the newcomers, introducing a work tool for password management, taking a new approach to monthly scheduling for the team and including a quick inspection of generated credentials in the quality checks. Among the suggested organizational changes that require approval by the upper management are adjustments to the content of the Information Security Awareness Training, overlooking the approach and development of repeated phishing simulation campaigns, an improvement of the organizational process for issuing temporary visitor badges, performing audits of visitor badges, monitoring security cameras for security violations, and increasing the number of employees recruited for the team. The need for additional hiring has already been brought up and confirmed, and the team will be expanded.

Potential future implementation of the Human Factors Analysis Classification System could be considered for introduction to the information security incident management and response process. The HFACS model is a powerful tool and could possibly be applied for investigation of security incidents. The system is clear to use and gives a broad outlook on the analysed scenarios.

# 6 Conclusion

The purpose of this thesis was to determine a set of practically applicable suggestions for minimizing existing human failure in information security within an organization. There were several risky cyber security behaviours and errors spotted within a team of employees in the Company X. These behaviours might result in actual security incidents. The goal was to identify root causes of undesired behaviours and understand what could be done for improvement and to minimize human error in the future.

The theoretical part of this paper includes analysis of literature and previous studies on the matter in the fields of information security and human behaviour analysis. It includes explaining the significance of human error in cyber security nowadays, a brief overview of various approaches and models for analysing and managing human failure and, specifically, the HFACS model. The overview of the HFACS model shows the major benefits of its implementation in the root cause analysis process. Previous studies imply that the model can be successfully applied in various industries. Adaptation of the HFACS model included evaluating a set of possible contributory factors from the HFACS that were relevant to the analysed scenarios and therefore incorporated as a structural basis for the interviews.

The practical contribution of the thesis is represented by qualitative research in a focus group of employees in a real organization and evaluating areas of improvement to mitigate human failure based on the analysis. The DoD HFACS guide was used as a basis for the conducted interviews. The interviews with employees of the Company X covered actual risky security behaviours in password security, phishing identification, and physical security. Considering the outcome of the interviews, possible causative factors of errors were determined, and corresponding areas of improvement needed to be addressed were identified.

Identified factors for risky behaviours included among others Pace of Ops-tempo/Workload, Failure to Provide Proper Training, Failure to Provide Appropriate Policy/Guidance, Failure to Identify/Correct Risky or Unsafe Practices, Fatigue, Distraction, Not Paying Attention, Emotional State, Technical or Procedural Knowledge Not Retained After Training, Improper Role-modelling, Deficient Command & Control Resources and Inadequate Procedural Guidance or Publications.

Corresponding areas of improvement included staff shortages, gaps in the local training and operational instructions, insufficient supervision, chaotic schedule, random timing of the Information Security Awareness Training, flaws in the organizational procedures and a lack of monitoring for security violations.

Based on the conducted qualitative research and the root cause analysis, a set of reasoned suggestions was introduced to the Company X to help minimize human failure in cyber security in the future. Offered suggestions include updating the operational instructions on user access management for the team, adjusting the initial onboarding training plan for the newcomers, introducing a work tool for password management, taking a new approach to monthly scheduling for the team, increasing the number of employees recruited for the team, an improvement of the organisational process for issuing temporary visitor badges, minor adjustments to the content of the Information Security Awareness Training, monitoring security cameras for violations on a regular basis and consistent audits of visitor badges.

Feedback from the Company X on the provided recommendations was overall positive and suggested actions are either carried out or considered for future implementation.

# References


[1] Nobles, C. (2018). *Botching Human Factors in Cybersecurity in Business Organizations.* HOLISTICA, Vol. 9, Issue 3.

[2] IBM. *Cost of a Data Breach Report 2022.* https://www.ibm.com/reports/data-breach [Accessed 12 February 2023]

[3] Verizon. *2022 Data Breach Investigations Report.* https://www.verizon.com/business/resources/reports/dbir/ [Accessed 12 February 2023]

[4] HFACS, Inc. *The HFACS Framework.* https://www.hfacs.com/hfacs-framework.html [Accessed 16 January 2023]

[5] The Air Force Safety Center. *DoD HFACS 7.0 Guide.* https://www.safety.af.mil/Divisions/Human-Factors-Division/HFACS/ [Accessed 18 February 2023]

[6] Unisys. *2021 Unisys Security Index.* https://www.unisys.com/unisys-security-index/ [Accessed 12 February 2023]

[7] Karanikas, N., Chionis, D., & Plioutsias, A. (May 2020). *"Old" and "New" Safety Thinking: Perspectives of Aviation Safety Investigators.* Safety Science.

[8] Igene, O. O., & Johnson, C. (2020). *To Computerised Provider Order Entry system: A comparison of ECF, HFACS, STAMP and AcciMap approaches.* Health Informatics Journal, Vol. 26(2), 1017–1042.

[9] HSE. *Introduction to human factors.* https://www.hse.gov.uk/humanfactors/introduction.htm [Accessed 18 February 2023]

[10] HSE. *Human factors: Managing human failures.* https://www.hse.gov.uk/humanfactors/topics/humanfail.htm [Accessed 18 February 2023]

[11] Pollock, T. (2017). *Reducing human error in cyber security using the Human Factor Analysis Classification System (HFACS).* Kennesaw: Kennesaw State University.

[12] SKYbrary. *Human Factors Analysis and Classification System (HFACS).* https://www.skybrary.aero/articles/human-factors-analysis-and-classification-system-hfacs [Accessed 19 February 2023]

[13] Small, A. (2020). *Human factors analysis and classification system (HFACS): As applied to Asiana Airlines flight 214.* Journal of Purdue Undergraduate Research, 10, 69–77.

[14] Widyanti, A., & Reyhannisa, A. (2020). *Human Factor Analysis and Classification System (HFACS) in the Evaluation of Outpatient Medication Errors.* International Journal of Technology, 11(1), 167-179.

[15] Mirzaei Aliabadi, M., Askaripoor, T., Ghamari, F., & Aghaei, H. (2020). *An investigation of the relationship between human and organizational factors in occupational accidents using Bayesian network approach: A case study in mining accidents.* Iran Occupational Health, 17(1), 990-1001.

[16] Ye, G., Tan, Q., Gong, X., Xiang, Q., Wang, Y., & Liu, Q. (2018). *Improved HFACS on Human Factors of Construction Accidents: A China Perspective.* Advances in Civil Engineering, vol. 2018, Article ID 4398345, 15 pages.
[17] Moser, A., & Korstjens, I. (2018). *Series: Practical guidance to qualitative research. Part 3: Sampling, data collection and analysis.* The European Journal of General Practice, 24(1), 9-18.
[18] Serrat, O. (2017). *The Five Whys Technique.* In: Knowledge Solutions. Springer, Singapore. doi: https://doi.org/10.1007/978-981-10-0983-9_32

# Appendix 1 – Non-exclusive licence for reproduction and publication of a graduation thesis[1]

I Elina Kurr

1. Grant Tallinn University of Technology free licence (non-exclusive licence) for my thesis “Application of HFACS Model for Minimizing Human Error in Cyber Security”, supervised by Kaido Kikkas
   1.1. to be reproduced for the purposes of preservation and electronic publication of the graduation thesis, incl. to be entered in the digital collection of the library of Tallinn University of Technology until expiry of the term of copyright;
   1.2. to be published via the web of Tallinn University of Technology, incl. to be entered in the digital collection of the library of Tallinn University of Technology until expiry of the term of copyright.
2. I am aware that the author also retains the rights specified in clause 1 of the non-exclusive licence.
3. I confirm that granting the non-exclusive licence does not infringe other persons' intellectual property rights, the rights arising from the Personal Data Protection Act or rights arising from other legislation.

22.04.2023

1 The non-exclusive licence is not valid during the validity of access restriction indicated in the student's application for restriction on access to the graduation thesis that has been signed by the school's dean, except in case of the university's right to reproduce the thesis for preservation purposes only. If a graduation thesis is based on the joint creative activity of two or more persons and the co-author(s) has/have not granted, by the set deadline, the student defending his/her graduation thesis consent to reproduce and publish the graduation thesis in compliance with clauses 1.1 and 1.2 of the non-exclusive licence, the non-exclusive license shall not be valid for the period.

# Appendix 2 – The HFACS Framework

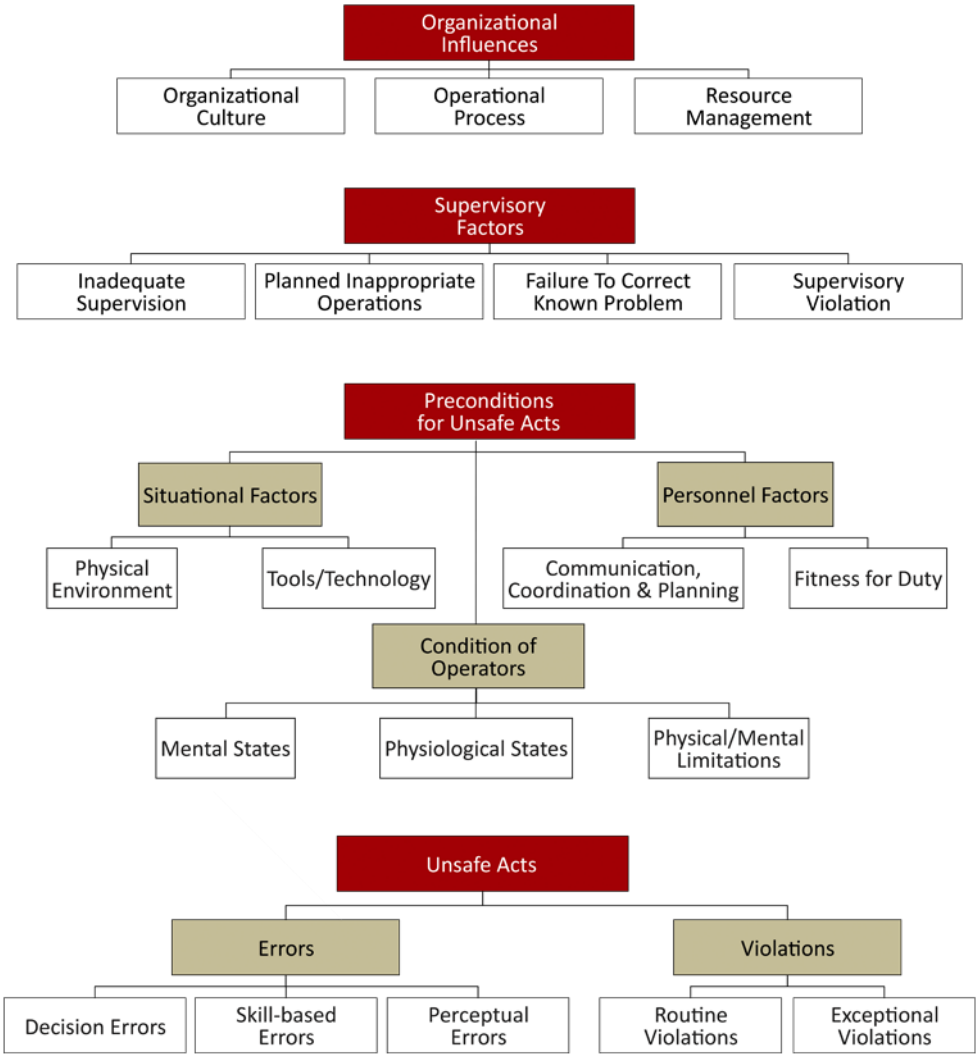


Figure 10. The HFACS Framework. [4]

# Appendix 3 – Questions after adaptation

1. Did the behaviour/error occur because known instructions/procedures were not followed correctly? (AE103) If yes, explain.
   Behaviour 1[1], Behaviour 2[2], Behaviour 3[3].
2. Did the behaviour/error occur because initially correct actions were performed too quickly or too slowly? (AE107) If yes, explain.
   Behaviour 2.
3. Did the behaviour/error occur because the employee did not recognize the risks? (AE201) If yes, explain.
   Behaviour 1, Behaviour 2, Behaviour 3.
4. Was the behaviour/error influenced/caused by incorrect prioritization of tasks? (AE202) If yes, explain.
   Behaviour 1, Behaviour 2.
5. Was there a caution/warning that was ignored?
   (AE205) If yes, explain.
   Behaviour 3.
6. Was the behaviour/error influenced/caused by an incorrect plan/choice of actions? (AE206) If yes, explain.
   Behaviour 1, Behaviour 2, Behaviour 3.
7. Was the behaviour/error a workaround solution?
   (AV001) If yes, explain.
   Behaviour 1, Behaviour 3.
8. Was the behaviour/error widespread among employees?
   (AV002) If yes, explain.
   Behaviour 1, Behaviour 2, Behaviour 3.
9. Was the behaviour/error influenced/caused by a lack of discipline?
   (AV003) If yes, explain.
   Behaviour 1, Behaviour 2, Behaviour 3.
10. Was the behaviour/error influenced/caused by substance effects?
    (PC302) If yes, explain.
    Behaviour 1, Behaviour 2, Behaviour 3.
11. Was the behaviour/error influenced/caused by a loss of consciousness?
    (PC304) If yes, explain.
    Behaviour 2.
12. Was the behaviour/error influenced/caused by fatigue/poor sleep habits?
    (PC307) If yes, explain.
    Behaviour 1, Behaviour 2, Behaviour 3.
13. Was the behaviour/error influenced/caused by poor nutrition/diet/hunger?
    (PC319) If yes, explain.
    Behaviour 2, Behaviour 3.
14. Was the behaviour/error influenced/caused by psychological state/problem?
    (PC202) If yes, explain.

---

1 Checked for risky behaviour in password security (generating credentials).

2 Checked for risky behaviour in phishing identification (simulations).

3 Checked for risky behaviour in physical security (tailgating).

Behaviour 1, Behaviour 2, Behaviour 3.

15. Was the behaviour/error influenced/caused by stress? (PC203) If yes, explain.
    Behaviour 1, Behaviour 2, Behaviour 3.
16. Was the behaviour/error influenced/caused by a positive or negative emotion? (PC204) If yes, explain.
    Behaviour 1, Behaviour 2, Behaviour 3.
17. Was the behaviour/error influenced/caused by impulsivity or submissiveness? (PC205) If yes, explain.
    Behaviour 1, Behaviour 2, Behaviour 3.
18. Did the behaviour/error occur because the employee overestimated personal capabilities? (PC206) If yes, explain.
    Behaviour 1, Behaviour 2.
19. Did the behaviour/error occur because the employee had a false sense of security? (PC208) If yes, explain.
    Behaviour 1, Behaviour 2, Behaviour 3.
20. Was the behaviour/error influenced/caused by motivational issues? (PC209) If yes, explain.
    Behaviour 1, Behaviour 2, Behaviour 3.
21. Was the behaviour/error influenced/caused by burnout? (PC215) If yes, explain.
    Behaviour 1, Behaviour 2, Behaviour 3.
22. Did the behaviour/error occur because the employee was not paying attention? (PC101) If yes, explain.
    Behaviour 1, Behaviour 2, Behaviour 3.
23. Did the behaviour/error occur because the employee was fixated on a limited number of cues? (PC102) If yes, explain.
    Behaviour 1, Behaviour 2, Behaviour 3.
24. Was the behaviour/error influenced/caused by the quantity of information? (PC103) If yes, explain.
    Behaviour 1, Behaviour 2, Behaviour 3.
25. Was the behaviour/error influenced/caused by a sense of confusion? (PC104) If yes, explain.
    Behaviour 1, Behaviour 2, Behaviour 3.
26. Was the behaviour/error influenced/caused by a working habit? (PC105) If yes, explain.
    Behaviour 1, Behaviour 2, Behaviour 3.
27. Was the behaviour/error influenced/caused by distraction? (PC106) If yes, explain.
    Behaviour 1, Behaviour 2, Behaviour 3.
28. Did the behaviour/error occur because the employee was interrupted? (PC108) If yes, explain.
    Behaviour 1, Behaviour 2, Behaviour 3.
29. Was the employee not able to recall the knowledge after the training? (PC109) If yes, explain.
    Behaviour 1, Behaviour 2, Behaviour 3.
30. Was the behaviour/error influenced/caused by an improper team climate? (PP101) If yes, explain.
    Behaviour 1, Behaviour 2, Behaviour 3.

31. Was the behaviour/error influenced/caused by unequal distribution of tasks? (PP103) If yes, explain.
    Behaviour 1, Behaviour 2.
32. Did the behaviour/error occur because the employee was intimidated by an authority? (PP104) If yes, explain.
    Behaviour 1, Behaviour 2, Behaviour 3.
33. Did the behaviour/error occur because critical information was not communicated with persistence/confidence? (PP105) If yes, explain.
    Behaviour 1, Behaviour 3.
34. Was the behaviour/error caused by a lack of timely communication among peers? (PP106) If yes, explain.
    Behaviour 1, Behaviour 3.
35. Was the behaviour/error caused by a lack of effective communication among peers? (PP108) If yes, explain.
    Behaviour 1, Behaviour 3.
36. Did the behaviour/error occur because the rules were not enforced? (SV001) If yes, explain.
    Behaviour 1, Behaviour 3.
37. Did the behaviour/error occur because it was allowed and seemed standard? (SV002) If yes, explain.
    Behaviour 1, Behaviour 2, Behaviour 3.
38. Did the behaviour/error occur because the supervisor directed to violate regulations? (SV003) If yes, explain.
    Behaviour 1, Behaviour 2, Behaviour 3.
39. Did the behaviour/error occur because the supervisor allowed the employee to perform a task unprepared? (SV004) If yes, explain.
    Behaviour 1, Behaviour 2.
40. Did the behaviour/error occur because the supervisor directed to perform a task beyond the skill level of the employee? (SP001) If yes, explain.
    Behaviour 1, Behaviour 2.
41. Did the behaviour/error occur because the employee lacked appropriate experience for the task? (SP003) If yes, explain.
    Behaviour 1, Behaviour 2.
42. Did the behaviour/error occur because the supervisor did not evaluate risks? (SP006) If yes, explain.
    Behaviour 1, Behaviour 3. Checked separately with the supervisor.
43. Was the behaviour/error influenced/caused by an example/behaviour of the supervisor? (SI002) If yes, explain.
    Behaviour 1, Behaviour 2, Behaviour 3.
44. Was the behaviour/error influenced/caused by misleading/a lack of local training? (SI003) If yes, explain.
    Behaviour 1.
45. Was the behaviour/error influenced/caused by misleading/a lack of local guidance/instructions? (SI004) If yes, explain.
    Behaviour 1.
46. Was the behaviour/error influenced/caused by a conflict with the supervisor? (SI005) If yes, explain.
    Behaviour 1, Behaviour 2, Behaviour 3.
47. Did the behaviour/error occur because the supervisor did not act upon the critical information that was provided? (SI006) If yes, explain.

Behaviour 1, Behaviour 3. Checked separately with the supervisor.

48. Did the behaviour/error occur because it was not identified/corrected? (SI007) If yes, explain.
    Behaviour 1, Behaviour 3.
49. Was the behaviour/error influenced/caused by insufficient organizational control? (OR001) If yes, explain.
    Behaviour 1, Behaviour 3. Checked separately with the supervisor.
50. Was the behaviour/error influenced/caused by missing infrastructure for dining/leisure-time? (OR003) If yes, explain.
    Behaviour 2, Behaviour 3. Checked if yes in the Question 13.
51. Did the behaviour/error occur because inadequate equipment (a security badge) was not timely removed/replaced? (OR005) If yes, explain.
    Behaviour 3.
52. Was the behaviour/error caused by inadequate organizational information resources? (OR008) If yes, explain.
    Behaviour 1, Behaviour 3. Checked separately with the supervisor.
53. Was employee screening during recruitment adequate/inadequate? (OS001) If yes, explain.
    Checked separately with the supervisor.
54. Was the behaviour/error influenced/caused by pace of ops-tempo/workload? (OP001) If yes, explain.
    Behaviour 1, Behaviour 2, Behaviour 3.
55. Was the behaviour/error influenced by incomplete/inadequate procedural guidance on the organizational level? (OP003) If yes, explain.
    Behaviour 1, Behaviour 3. Checked separately with the supervisor.
56. Was the behaviour/error influenced/caused by inadequate organizational training? (OP004) If yes, explain.
    Behaviour 1, Behaviour 2, Behaviour 3. Re-watched separately.
57. Was the behaviour/error influenced by poorly designed/unsuitable equipment (a security badge)? (OP007) If yes, explain.
    Behaviour 3.
58. Was the behaviour/error influenced/caused by organizational culture? (OC001) If yes, explain.
    Behaviour 1, Behaviour 2, Behaviour 3. Training on organizational culture and values checked separately.