Implementing Information Security Management System (ISMS) for OT environments within multinational organizations

Turvallisuusjohtamisen koulutusohjelma – TJK 18

Lopputyöraportti

Robert Valkama

Fortum Corporation

Loviisa 12.3.2024

Aalto University Executive Education and Professional Development

Tiivistelmä

Lainsäädännölliset muutokset edellyttävät kriittisen infrastruktuurin toimijat huomioimaan teollisuusautomaatiojärjestelmien (OT) tietoturvallisuus entistä paremmin ja määrämuotoisemmin toiminnassaan. Kansallisia eroja lainsäädännön vaatimuksissa löytyy, mutta tästä huolimatta velvoitteet voi tiivistää siten että on määriteltävä roolit ja vastuut, toteutettava riskien arviointi ja hallinta liiketoiminnan edellyttämällä tavalla, varmistaa kyvykkyyttä tietoturvallisuuspoikkeamien hallintaan sekä tuottaa tapahtumista raportteja vastuu viranomaiselle. Vaatimustenmukaisuuden osoittaminen edellyttää prosessimaista lähestymistapaa tietoturvallisuuden hallinnalle, missä prosessien eri vaiheessa toteuttavat tehtävät tuottavat todistusaineistoa tapahtuneesta minkä avulla vaatimustenmukaisuutta voidaan jälkeenpäin osoittaa. Tämän toteuttamiseksi auttaa tietoturvallisuuden hallintajärjestelmän (ISMS) käyttöönottaminen.

Perinteiset tietoturvallisuuden hallintajärjestelmät ovat luotu tietojen luottamuksellisuuden, eheyden ja käytettävyyden varmistamiseksi. Nämä periaatteelliset tavoitteet ovat sovellettavissa myös teollisuusautomaatiojärjestelmille, on tietoturvallisuuden hallintajärjestelmän toteuttamisessa huomioitava näiden ympäristöjen ja hallintamallien erityispiirteet, kuten se, että teollisuusautomaatiojärjestelmän tehtävä on tukea ja ohjata fyysistä tuotantoprosessia, se ei itsenäisesti toteuta sitä. Organisatorisesti on myös huomioitava se, että vastuu teollisuusautomaatiojärjestelmien tietoturvallisuudesta ei voi erottaa tuotantolaitoksen prosessiturvallisuus- tai tuotantovastuista.

Teollisuusympäristöissä on yleisesti olemassa jonkunlainen johtamisjärjestelmä mihin toiminnan turvallisen ja laadullisen operointiin tarvittavat kriittiset prosessit ovat kuvattu. Tietoturvallisuuden hallintajärjestelmä ei tulisi kilpailla näiden olemassa olevien johtamisjärjestelmien kanssa, vaan rakentua sen päälle. Esim. OT ympäristön riskienhallinnan pohjaksi on hyvä hyödyntää olemassa olevia prosessiturvallisuus analyysejä kuten esim. HAZOP ja LOPA.

Abstract

Legislative changes require critical infrastructure operators to consider the cybersecurity of operational technology (OT) more thoroughly and formally in their operations. While there are national differences in legal requirements, the obligations can be summarized to; defining roles and responsibilities, conducting risk assessments and management in line with business needs, ensuring the capability to manage cybersecurity incidents, and producing reports on events for competent authorities. Demonstrating compliance requires a process-oriented approach to cybersecurity management, where the tasks performed at different stages produces records which can be used to show compliance. Implementing an Information Security Management System (ISMS) helps achieve this.

Traditional information security management systems are designed to ensure the confidentiality, integrity, and availability of data. These fundamental objectives are also applicable to industrial automation systems. However, when implementing a cybersecurity management system, the specific characteristics of these environments and management models must be considered, such as the fact that the role of an OT system is to support and control a physical production process, it does not independently produce it. On an organizational level it is also needed acknowledge that in industrial operations, the accountability for the cybersecurity of the OT systems cannot be separated from the accountability for process safety or production responsibilities.

There is usually some form of management system established within industrial environments, where the processes critical for safe and quality operations are described. The ISMS should not compete with these existing management systems, instead it should build upon them. As an example, risk management in OT environments should utilize existing process safety analyses, such as HAZOP and LOPA.

Table of Contents

1 Introduction

Operational Technology (OT) environments are increasingly using digital components and software to monitor and control industrial processes. This is a change that has happened slowly over time starting in the 1970's with the first widely used digital controllers. Since then, the development has taken us towards more general industrial components that can be programmed to suit a large variety of applications while still running on standardized hardware. The physical panels in control rooms have been replaced with Commercial off-the-shelf (COTS) IT hardware running applications allowing control of the industrial process. The development is currently taking industrial control applications towards big data and machine learning based calculations for optimization and to increase the autonomous operation of industrial applications. I.e., the computer is doing more of the tasks that humans used to manually do before.

As a biproduct of this transition there have been tremendous changes in the span of control. Where in the "analog" era it was possible to follow a cable from the actuator to the panel in the control room, exactly knowing how the function operated, in the "digital" era that is replaced with cables terminated into I/O at the factory floor and process values and control signals transmitted as data packages to the IT system used for controlling the process. While this has enabled many new features and possibilities, it has also made it possible to have a large span of control over multiple processes from one single point. Hence, increasing the possibilities for something to go wrong on the control pane, and creating attractive points for malicious activities.

In analog environments it was sufficient to have good physical configuration management in place. One did not have to take into consideration that the value of a resistor changed from 100 ohm to 1 Mohm during the operation phase, which could have changed the alarming or triggering level of an event/action, as this was not possible. In digital OT environments this risk is

one that needs to be considered, not the change of the hardware value, but the systems allow to change setpoints and application codes during operation changing the way the control of the industrial environment reacts or works.

This is where a well specified ISMS comes into use. It sets up a management system designed to take these types of digital risks into consideration to identify potential weak practices and continuously improve them to meet the expected level of safe and secure operation. It can also be used to help show compliance to regulatory requirements on cyber security in OT environments but utmost, it is to help ensure that the organization considers cyber security sufficiently, just like any other business management domain.

2 Background

2.1 Defining Operational Technology

Operational Technology is not a universally understood term. There are many different terms and abbreviations used to describe it depending on the level of detail that is discussed. As an example, Instrumentation and Automation Control Systems (IACS), Industrial Control Systems (ICS), Safety Instrumented Systems (SIS), Basic Process Control Systems (BPCS) and Cyber-physical system to name a few.

Krotofil [1] gives a more practical example of a cyber-physical system in her whitepaper "*(CPS): systems where the events in the physical world are managed with the help of modern advances in computation and control. Complex machines such as aircraft or robots, building automation systems, smart cities and smart grids, railways and agricultural systems, medical devices and industrial infrastructures, in general, are examples of cyber-physical systems."*

OT is defined in the glossary by Bochman and Freeman[2] as *"Operational Technology (OT) refers to any technology used to manage industrial operations. ICS is a subset of OT. The term cyber-physical system is also roughly synonymous"*. This shows the immaturity in the terminology within this field and the need to define the terminology. In this paper, the term Operational Technology (OT) will describe all different types of digital systems used to control an industrial process.

---

[1] M. Krotofil, Industrial Control Systems: Engineering Foundations and Cyber-Physical Attack Lifecycle, Technical Whitepaper May 2023 (Cyber-physical security | ICS security (cyberphysicalsecurity.info))

[2] A. Bochman and S. Freeman, Countering cyber sabotage: introducing consequence-driven, cyber-informed engineering (CCE). CRC Press 2021 ISBN 9780367491154

2.2 Defining OT Cyber Security

On a principal level OT Cyber Security does not differ from the general understanding of Information Security. It is the practice to protect the Confidentiality, Availability, and Integrity (CIA) of the environment or as ISO27000[3] defines Information Security, "*preservation of confidentiality (3.10), integrity (3.36) and availability (3.7) of information*".

The difference for OT Cyber Security, compared to IT, does not come from the technology itself, but from how the technology is used. IT Cyber Security (or Information Security) purpose is to protect information, whereas OT Cyber Security purpose is to protect the correct operation of a cyber-physical function. I.e., OT Cyber Security purpose is to ensure that the control functions of a cyber-physical operation execute as designed, when needed and within the expected time limit while providing the operator with sufficient insight to the process status (operational monitoring). Therefore, the actual CS priorities in OT environments depend on the characteristics of the physical process it controls or interacts with. In practice this usually means *a)* to ensure safety (incl. Health, Safety and Environment) and *b*) to ensure availability of the physical process.

While managing OT Cyber security using the CIA priorities, as in IT, is possible, there is a risk that the security practices defined are not suitable for OT. Meaning that the controls defined may be too restricted or ineffective in OT environments potentially causing harm than good to the production process. Do not get it wrong, the Confidentiality, Availability and Integrity are still principles that can be applied, but as such they do not resonate with OT management practices as there the focus is not only on protecting the information, but the function using or producing the information.

Due to the differences in between IT and OT cyber security practices it is recommended to consider OT Cyber Security as a separate area of expertise and keep some separation between the two.

[3] ISO/IEC 27000:2018(en) Information technology — Security techniques — Information security management systems — Overview and vocabulary

2.3 Regulatory environment for CI operators in Europe

The Cyber Security regulatory environment for Critical Infrastructure (CI) operators in Europe began to change with the publication of the first *NIS (Network and Information Systems) Directive* [4] as the first attempt to create EU (European Union) wide common cyber security regulation. Before this, there was sector specific regulation in place for specific industries like the financial sector or nuclear energy production, but with the release of the *NIS Directive* it was the first attempt to have a holistic societal view of Cyber Security which extended the scope of security regulation to new industries, which had not been subject to regulation before.

As the *NIS Directive* is a Directive issued by the European Parliament and the council of the European union, it is to be implemented through national laws, which gave the member states the freedom to do it as they saw fit. While this can be seen as a benefit from a national perspective (easier to include in the existing regulatory framework) there is another side to the coin. Individual (national) implementations of the same directive results in variations on the union level. With the NIS Directive this could be seen as some countries adopted very prescriptive (how to do it) legislation while others implemented more descriptive (what to achieve) legislation. There is also a difference in how it was implemented, some countries (like Finland) implemented the Directive by changing the sector laws, where others created a more general cyber security law.

As such, one is not better than the other, but for corporations operating in multiple countries, this causes some degree of additional work to align the corporate wide operations as the compliance is to be achieved on national level. To support this work, the ISMS with clear compliance management practices are essential.

Since the publication of the *NIS Directive* there was identified a need to update it and the *NIS 2 Directive* [5] was published in December 2022 starting the

[4] Directive (EU) 2016/1148 of the European Parliament and of the Council of 6 July 2016 concerning measures for a high common level of security of network and information systems across the Union, (https://eur-lex.europa.eu/eli/dir/2016/1148/oj)

[5] Directive (EU) 2022/2555 of the European Parliament and of the Council of 14 December 2022 on measures for a high common level of cybersecurity across the Union, amending Regulation (EU) No 910/2014 and Directive (EU) 2018/1972,

21-month implementation period. The NIS2 Directive extended the scope of sectors in scope in addition to introducing stronger means for the authorities to enforce implementation at the entities in scope. The implementation of this Directive into the member state legislation is ongoing during the time of writing.

In addition to the *NIS 2 Directive*, there are additional security related regulations affecting security in force and as ongoing initiatives both on EU level but also on member state national level. To name a few, but not going into details.

- Resilience of critical entities (CER Directive) [6]
- Cybersecurity Act [7]
- Cyber Resilience Act[8]

In addition to the obvious security legislation, there are other legislations that are closely related to security, without specifically defining it. This is because most operations today are controlled by or with the help of digital systems. Therefore, legislation related to, as an example, safety, preparedness, or quality also need to be considered from the security (especially Cyber Security) perspective to ensure compliance.

To summarize the content of the most relevant security legislations aimed at critical infrastructure operators, they contain the following elements:

- Define the responsibilities for addressing security and management responsibility (Governance)
- Know your risks and take proportionate actions (Risk management)

---

and repealing Directive (EU) 2016/1148 (NIS 2 Directive) (Text with EEA relevance) (https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX%3A32022L2555)

[6] Directive (EU) 2022/2557 of the European Parliament and of the Council of 14 December 2022 on the resilience of critical entities and repealing Council Directive 2008/114/EC (Text with EEA relevance) (https://eur-lex.europa.eu/eli/dir/2022/2557/oj)

[7] Regulation (EU) 2019/881 of the European Parliament and of the Council of 17 April 2019 on ENISA (the European Union Agency for Cybersecurity) and on information and communications technology cybersecurity certification and repealing Regulation (EU) No 526/2013 (Cybersecurity Act) (Text with EEA relevance) (https://eur-lex.europa.eu/eli/reg/2019/881/oj)

[8]Proposal for a REGULATION OF THE EUROPEAN PARLIAMENT AND OF THE COUNCIL on horizontal cybersecurity requirements for products with digital elements and amending Regulation (EU) 2019/1020 (https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=celex:52022PC0454)

- Identify incidents and prepare to manage them (Incident management)
- Report to the relevant authorities (Reporting)

In other words, the existing and upcoming regulation for critical infrastructure operators requires the affected entities to set up a (cyber/information) security management system or governance model which is to be used to ensure sufficient security actions have been taken to protect and ensure the continuity of the service which is essential for the society. As the legislation includes the right to audit by competent authorities, the governance model and security activities done need to be auditable, meaning that they need to be executed in a documented manner. This is where an ISMS can be utilized to help meet the expected goals.

2.4 ISMS Briefly

ISO27000[9] defines an ISMS the following way "*An ISMS consists of the policies, procedures, guidelines, and associated resources and activities, collectively managed by an organization, in the pursuit of protecting its information assets. An ISMS is a systematic approach for establishing, implementing, operating, monitoring, reviewing, maintaining and improving an organization's information security to achieve business objectives. It is based on a risk assessment and the organization's risk acceptance levels designed to effectively treat and manage risks. Analysing requirements for the protection of information assets and applying appropriate controls to ensure the protection of these information assets, as required, contributes to the successful implementation of an ISMS."*

An Information Security Management System is a documented and approved governance model set up by the organization to ensure that the targets set (based on business objectives) for information security are achieved. It is not different to any other management system, except it focuses on information security and the reference controls are aimed at information security.

[9] Chapter 4.2.1

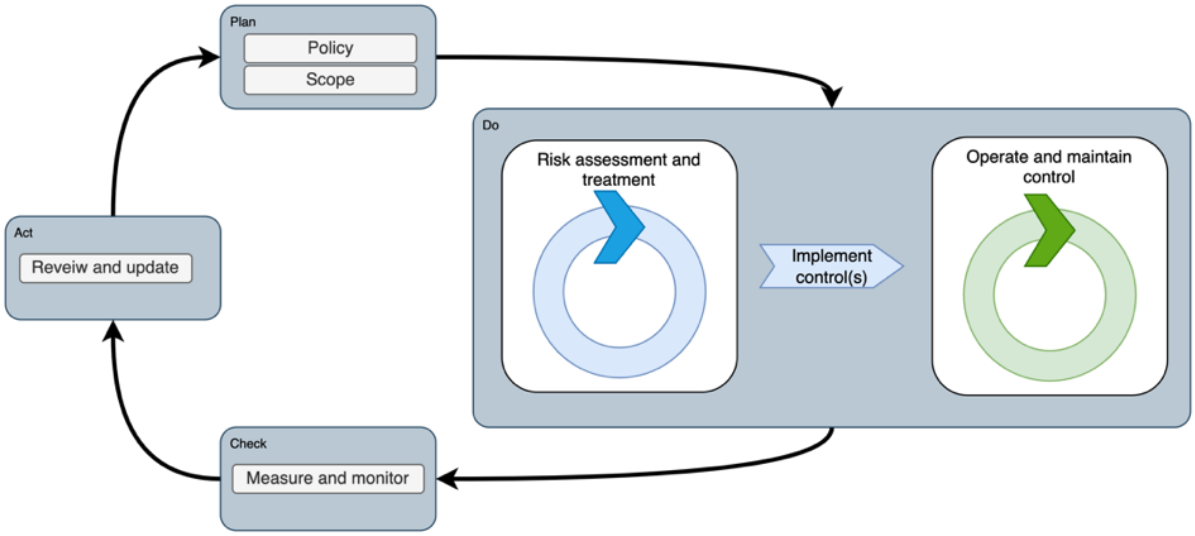

Figure 1: ISMS process in PDCA context.

3 Considerations in OT environments

3.1 IT vs. OT environments and ISMS

On a fundamental level, there is no difference if an ISMS is implemented for ensuring security of an enterprise IT (Information Technology) or for OT (the why). The differences arise in the details, i.e., how, and especially what activities are included.

The difference here originates from the purpose of the different technologies and what their business value or function is. In enterprise IT, the purpose is to ensure the availability, confidentiality, and integrity of information and in OT to ensure the safety, availability, and quality of the production process it controls.

The separation of the purposes of the systems also impacts the way these systems are managed. Enterprise IT is mostly centrally managed and operated, and major parts of it is outsources to various partner(s), aiming for a more cost-efficient way to get the wide expertise needed, but also because IT is seen as a function which is not a core activity of the company (except if you are an IT service provider).

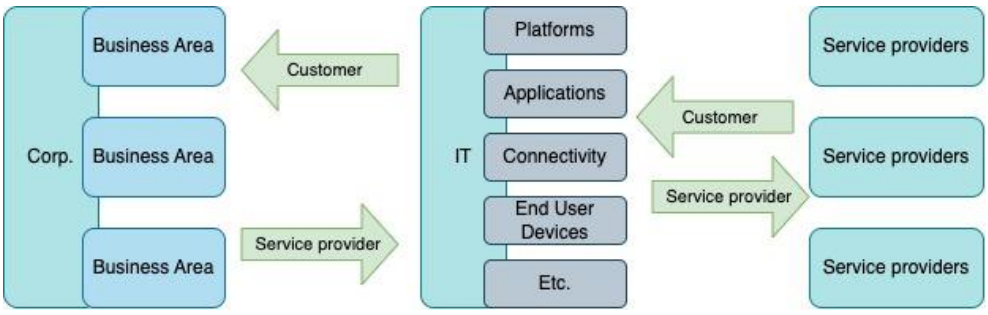

Figure 2: Enterprise IT management architecture (simplified)

In OT, the management of the environments are de-centralized or distributed. This is primarily due to two reasons 1) safety and 2) operational performance. These have nothing to do with the technical aspects of the OT environments,

but the responsibility of it. By legislation (Nordics), the production manager is responsible for the safety of the production site. If that site utilizes digital controllers to perform the safety functions, then the digital components used for this can be manipulated to impact the production facility safety (in a digital environment there is no safety without security). Even if the responsibility to execute specific tasks can be, and are, outsourced to third parties, the accountability of safety can never be transferred.

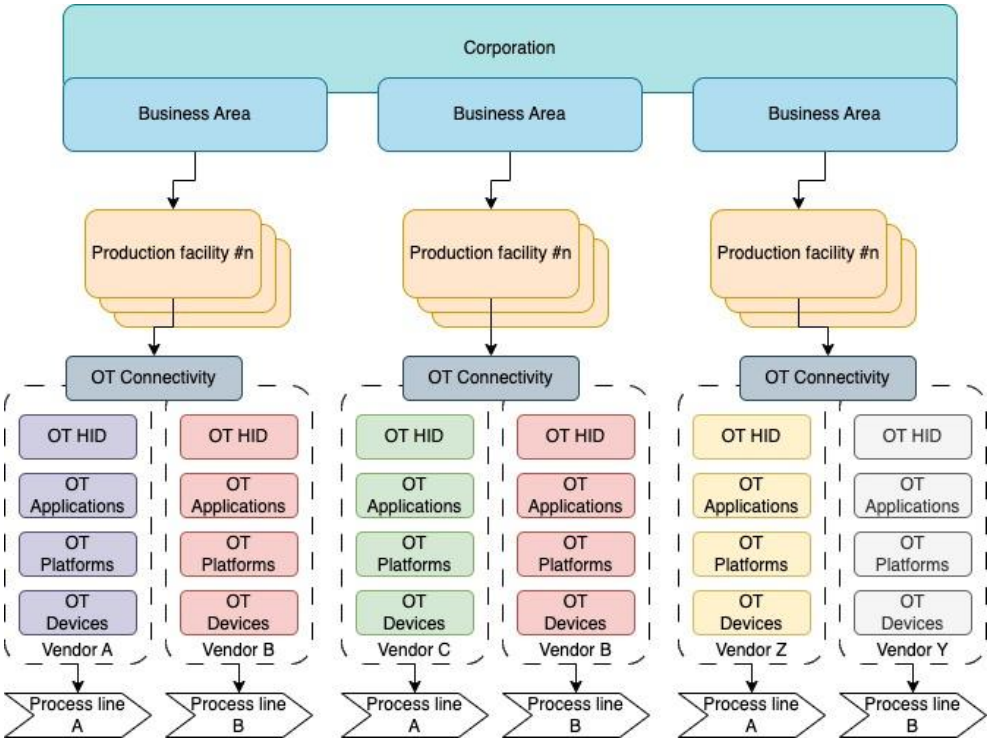

Figure 3: OT Management model (simplified)

OT systems are also connected to the production facility's operational performance, i.e., quality and quantity. This is where process control knowledge and security knowledge need to be combined. The execution of good quality risk assessments requires good knowledge of how the process would react in specific situations, and what controls (process) are in place to restrict the consequences. This knowledge is also needed when designing security controls (the how and what) for the environment.

As a simple example, in IT the control for losing the integrity of some data can be backup and recovery, in OT the loosing of integrity of some data may result in equipment failures and prolonged production down-time, hence backup and restore activity may not be sufficient to mitigate the risk.

Thus, it is not impossible to manage OT environments with similar organizational setup as IT environments (central and/or outsourced), the magnitude of the potential consequences of disruptions in OT in combination with potential legal actions require a strict and formal management control (supplier management if outsourced) of the activities, usually makes it easier to keep it inhouse or localized to the sites.

3.1.2 Management frameworks

Security is not an independent function that is executed in vacuum from the "real operations", but something that needs to be integrated to the overall management processes of the function itself. E.g., IT is usually managed with the help of some IT Service Management process (ITSM) where OT is managed through some type of Industrial (or Integrated) Management System (IMS), where various engineering disciplines are integrated to support the control of the industrial process. It is not uncommon that the IMS is based upon Quality Management standards such as ISO 9001[10].

Figure 4: General quality management process (ISO9001)

[10] ISO 9001 Quality management systems - Requirements

3.2 Available standards and frameworks

There are a variety of information security standards and frameworks available that can be used to support the implementation of an ISMS in OT environments. There are both national standardization bodies like National Institute of Standards and Technology (NIST) in the US and international standardization bodies like International Organization for Standardization (ISO) and International Electrotechnical Commission (IEC). All of these provide both standards and guidelines or frameworks, and the major difference between these is the possibility to certify the operations towards it or not.

3.2.1 ISO 27000 standard family

The most used and well-known information security standard series is the ISO/IEC 27000 family on Information security management. This information security management standard is not as such built for OT environments but on a management level the processes are fully adoptable to meet the needs for OT. The ISO/IEC 27000 is a family of documents where the ISO/IEC27001 (Information security, cybersecurity and privacy protection — Information security management systems — Requirements) is the fundamental standard document setting the requirement and which entities can certify their management system towards. The requirement document is then supported by additional documents to help organizations implement the management system. The most relevant ones are ISO/IEC27002 (Information security, cybersecurity and privacy protection — Information security controls) and ISO/IEC27005 (Information security, cybersecurity and privacy protection — Guidance on managing information security risks).

While the controls defined in ISO/IEC 27002 are not designed for OT environments there are sector specific adaptations made for this. As an example, the ISO/IEC 27019 (Information technology, Security techniques, Information security controls for the energy utility industry). The management requirements as defined in ISO/IEC 27001 are adaptable to OT environments. However standard ISO27002 controls can be adapted to be suitable for OT environments, but this requires some effort from the organization performing the implementation.

3.2.2 ISA/IEC 62443 standard family

The ISA/IEC62443 standard family has become the prominent and most used standard family for Industrial Automation and Control Systems (IACS) or OT. The standard standards and it is actively being developed and extended with new documents. The standard family is organized into four levels of 1. General, 2. Policies and Procedures, 3. System Requirements and 4. Component Requirements. The most relevant document in this family in respect to the ISMS is the ISA/IEC 62443 2-1 (Industrial communication networks - Network and system security - Part 2-1: Establishing an industrial automation and control system security program) which describes what is required to define and implement a cyber security management system for IACS.

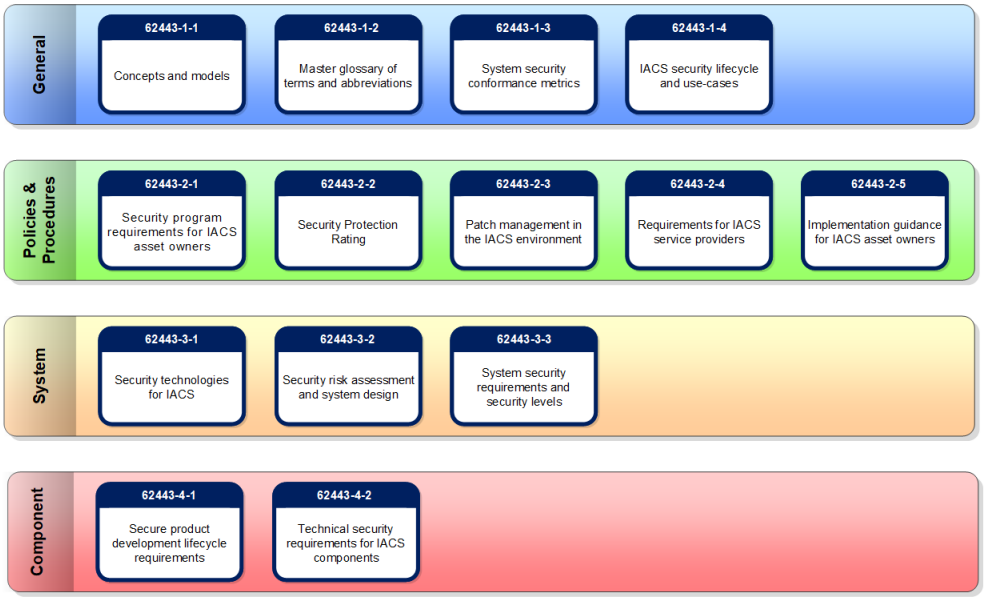

Figure 5: ISA/IEC 62443 standard family[11]

The benefit with ISA/IEC62443 2-1 standard is that it is specifically developed for setting up a cyber security management system (CSMS) for OT environments and therefore focuses on the specific topics that are important in these environments, and with a bit more detail than in ISO27001. The CSMS is also supported by other more detailed documents like system and service requirements which can be helpful when discussing cyber security topics with solution and service vendors.

[11] ISA Global Security Alliance (https://gca.isa.org/blog/structuring-the-isa-iec-62443-standards)

3.2.3 NIST Cybersecurity framework and SP 800-82

The National Institute of Standards and Technology have published a cyber-security framework (CSF)[12] and an additional guide for OT Security (SP 800-82[13]) which describes in detail how cyber security can be implemented into OT environments as well as customized controls and discussion points for OT related to the controls described in the NIST CSF.

The NIST CSF is a national standard, developed for the United States focusing on operators of critical infrastructure within the US. However, as the framework is publicly available, it can be used by anyone as such or as a supplement to the existing security program.

The CSF is built up like all other frameworks, starting with risk assessments and identifying the business needs for security. There is no certification or audit process available for the NIST CSF, meaning that an operator cannot certify their operations against it to show compliance. The NIST CSF or its core controls can be integrated into an ISO27001 ISMS.

Figure 6: NIST CSF

3.2.4 ISF Standard of Good Practice

The Information Security Forum Ltd (ISF) is a forum where companies can join to gain access to resources, tools, and peer organizations to help with

[12] NIST Framework for Improving Critical Infrastructure Cyber Security v.1.1 2018, https://nvlpubs.nist.gov/nistpubs/CSWP/NIST.CSWP.04162018.pdf
[13] NIST Special Publication 800-82r3, Guide to Operational Technology (OT) Security (https://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-82r3.pdf)

their cyber security activities. All the ISF resources are limited to the members and therefore not available publicly.

The ISF has developed an information security management framework and associated tools that its members can utilize to help them with their cyber security management activities. As a tool supporting this, the Standard of Good Practices (SOGP) has been developed. The SOGP is a control catalogue developed for IT operations, or the protection of information, but some developments into the OT or ICS sector are ongoing.

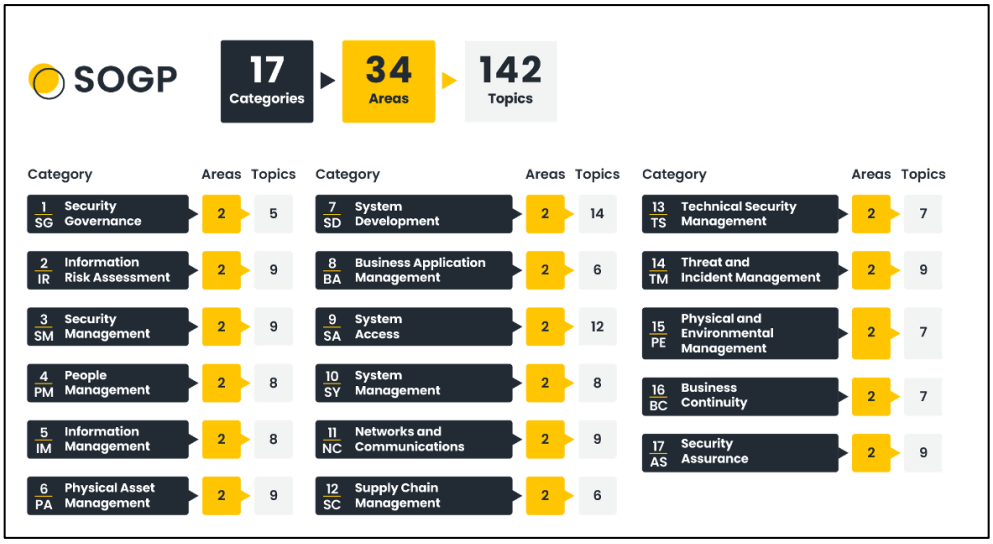

Figure 7: ISF SOGP 2022 structure[14]

The SOGP governance and management related controls are applicable to OT, but the more technology focused controls are not customized for OT and the use of the framework will require efforts by the organization to ensure that the desired outcome is achieved.

3.3 Choosing the suitable framework

Choosing the most suitable framework for your organization should be done consciously as it may have an impact on the success of the implementation. The different frameworks do contain the same cyber security activities to be done, the differentiating factors are the level of detail (towards what they are done for), and terminology used to describe the activities. There are primarily two things to consider when making the decision on the framework.

[14] Information Security Forum Standard of good practice for information security (www.securityforum.org)

Compliance to regulation or standard, if the industry the organization is in have specific standard ways of working of sector specific regulation that mandate the use of a specific framework, this makes the decision trivial.

The organizational management model is recommended to be the directing factor when choosing the framework for the ISMS in OT. The reasoning behind this is that if cyber security is created as a separate function with its own terminology and processes it can be more challenging for the business leadership to understand it and have it considered as something separate from the actual business processes. The ISMS should not compete with other management systems within a business organization but complement it to ensure that cyber security is sufficiently covered when making business decisions. In this sense, the ISMS is a set of formal processes developed to communicate cyber security aspects for the business context. This is why utilizing the existing management system model and adopting to its terminology can be considered more important than the detail of the content.

3.4 Multinationalism

As discussed earlier, OT is often managed on production facility (local) level even if the company owning the facility operates in multiple countries. This can be both a challenge and opportunity when implementing an ISMS. Challenging in a sense that there may be missing one single line operation through which the ISMS practices can be implemented, requiring more efforts on composing the enterprise level ISMS practices and agreeing on the interface points and resourcing, and an opportunity as there may be more mature management practices within the production facility base that can move more quickly and act as example organizations for others.

Multinationalism also sets some requirements on the ISMS implementation, the biggest one being national legislation and the difference between the countries of operation. In general, cyber security can be presented in many ways and frameworks, but the actual activities are fundamentally the same. However, local regulation can have considerable differences in i.e., expected level of assurance, reporting to authorities and processing of information considered important for national security (usually impacts critical infrastructure operators). As these types of legislative requirements are sensible and understandable, their implementation expectations may not as such support the most cost-efficient multinational operation and can even require overlapping

functions to be operated in various countries. One of the major challenges for corporations operating regulated business in multiple countries is the interpretation and alignment of regulatory requirements. The national legislation takes rarely into consideration multinational operations, and especially in the security domain, the legislation tends to be leaning more towards protectionism than supporting multinational operations.

Knowing the legislations of the operating countries is the first items to master when defining the ISMS implantation strategy for OT environments and one of the most important topics to understand is if there is a requirement (or practical expectation) for a certified ISMS or security management system. The requirement to certify the ISMS will require more detailed documentation of the activities, which as such is not a negative thing when expected to show compliance, but it will require more time and resources to do. However, the bigger risk is the scope of the ISMS and the certification. If the ISMS is defined in a way that all enterprise operations are in the scope of one single ISMS, then there is a risk that inadequate procedures on one production facility causes the certification to be lost, potentially making another production facility non-compliant to local regulations, even if that production facility itself applies adequate procedures.

3.4.1 Implementation models

When starting with the design of an ISMS the most critical topic to address is the scope of the management system i.e., what are the Physical, Logical and Organizational boundaries for the ISMS. There is no difference in this stage for OT in comparison to implementing or designing an ISMS for any other service or organization. This is also where the actual implementation model is decided, as the scoping of the ISMS is what defines this in practice.

There are generally three different implementation models for a governance framework[15]. The first is a distributed (or decentralized) model, where each production facility defines and creates its own ISMS without any synergies between the functions or business lines and limited alignment with corporate

[15] D. Blum, Rational Cybersecurity for Business, The security leaders' guide to Business Alignment, Apress Open

operations. This can be compared to holding companies, where each individual company within the holding company portfolio operates as an independent entity.

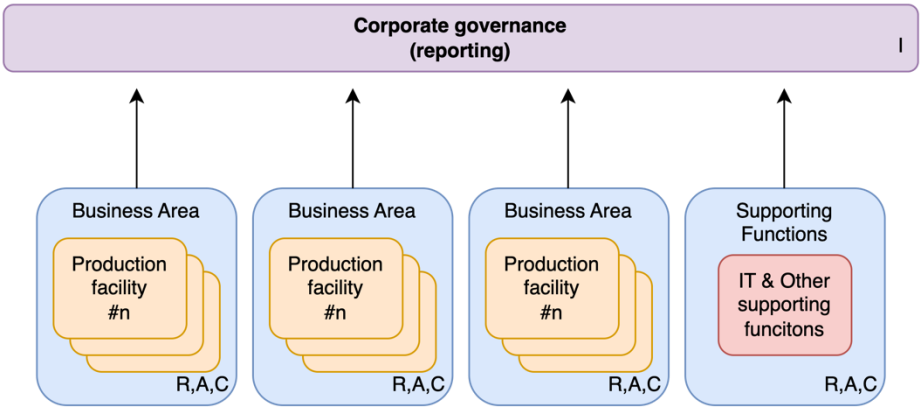

Figure 8: Distributed ISMS

The second type is a centralized model where the ISMS is defined for the whole corporation and all the individual production facilities and supporting functions are part of the ISMS scope. This can be a very well-functioning model especially if the production facilities are similar in type or are part of the same production chain where all have similar or the same business objectives.

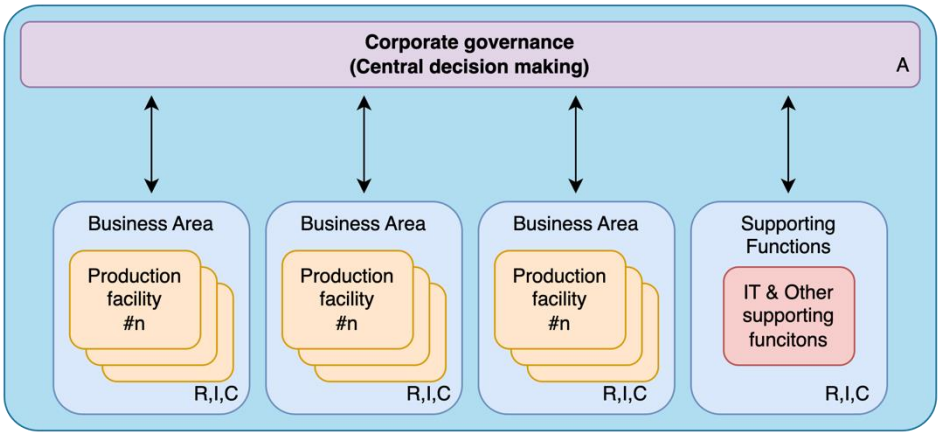

Figure 9: Centralized ISMS

The third is a hybrid (or matrixed) model where corporate oversight and governance is applied but each production facility or business is responsible for setting up their own ISMS. This is useful for corporations where there are different business lines with individual business goals and risk appetites, while enabling strategic governance from corporate.

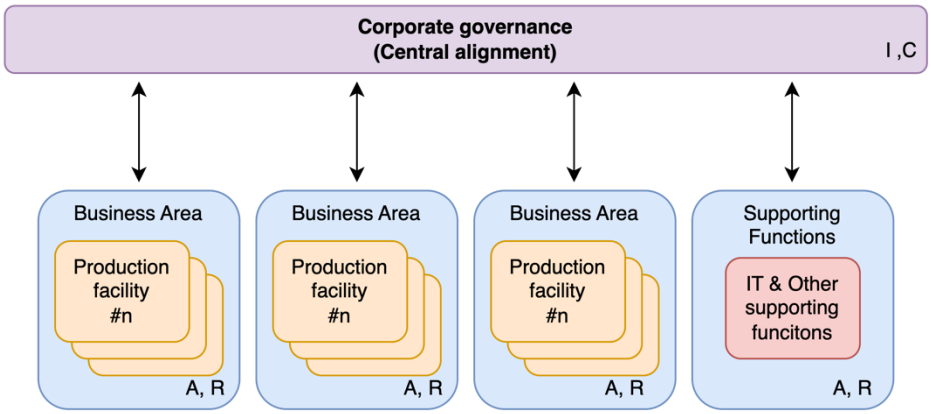

Figure 10: Hybrid ISMS

It is noteworthy that all these models have different benefits and drawbacks, but the key is to ensure the accountability and responsibilities are well known and understood according to the operating model. Especially in OT, where security knowledge or skills may be less mature, implementing a distributed governance model may not have the best results as the drive or accountability does not come naturally.

3.4.2 Defining the control catalogue

The control catalogue defines what is to be done and depending on the environment, also the how. For regulated multinational corporations this can be challenging as the controls may be defined, or heavily influenced, by the national legislation (especially the ones implementing prescriptive regulations). Another challenge is that OT systems are usually very heterogeneous both in technology type but also from a lifecycle view. One way to address this challenge is by defining the controls on relatively high level and allowing for target specific implementation variations. There are however some caveats that need to be addressed with this approach, the biggest being lack of cyber security skills resulting in inadequate implementation and hence potentially providing a false sense of security. By allowing the target personnel to define how to achieve the control target requires that the expectation level is well defined and supportive material is available. This can for example be achieved by defining control specific implementation guidelines which describes what needs to be taken into consideration when implementing it.

4 Key processes

The boiled down purpose of an ISMS is to maintain situational awareness and to have the capability to make business informed decisions on security management. I.e., what is needed and where to make the most of the available resources (in other words, most effort with minimal cost).

The drivers to implement security controls can come from various sources. As discussed earlier, regulation is one of these but not the only one. Other drivers for implementation of controls are risk mitigation, policy decision or contractual obligations. In general, these can be grouped into two main drivers, business driven control implementation and compliance driven control implementation.

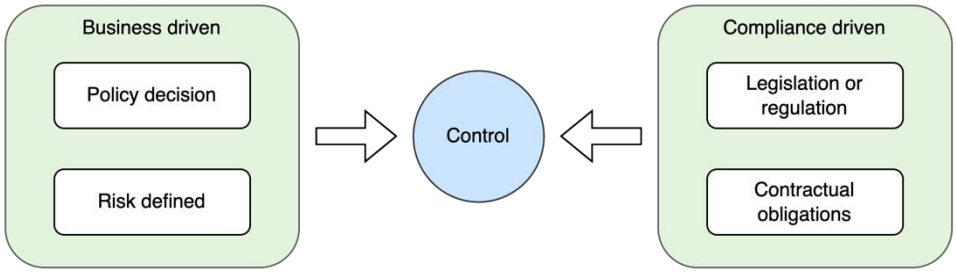

Figure 11: Control implementation drivers

To manage these there are two key processes that need to be in place in the ISMS, the risk management process, and the compliance management process. These will not by themselves constitute as an ISMS, but they are the fundamental activities that the management system can be built upon.

4.1 Risk management process

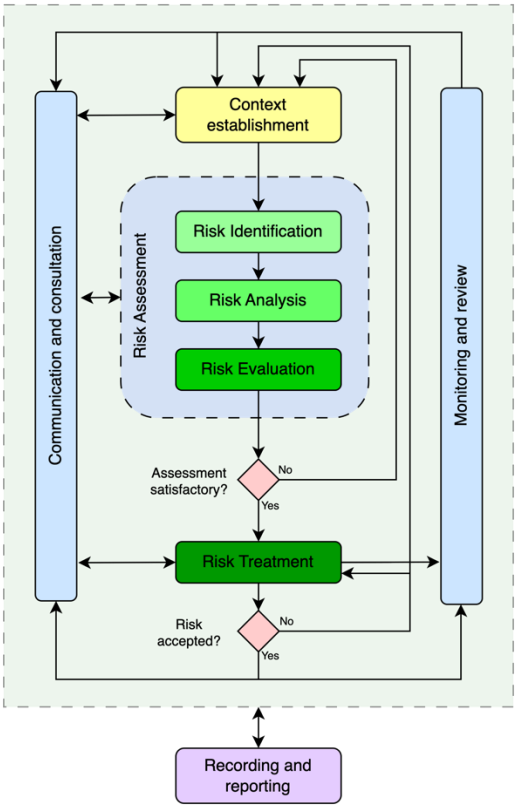

Figure 12: ISO27005 Risk management process[16]

The Risk management process for OT does not have to be different from the general risk management process. In fact, it is beneficial to have the OT Cyber Security Risk management process integrated into the overall or general risk management process of the production facility. This will emphasize that Cyber Security risks (or digital risks) is just one more domain to consider, as any other risk at the facility.

However, there are differences in the attributes used for cyber security risk assessment and general risk assessment. Especially on the concept of likelihood where this is a factor of a threat and the availability of a vulnerability that the threat can utilize. Even if these attributes sum up to the same likelihood calculation that is used for determining the risk, they are important to have identified to allow detailed analysis of the overall risk profile. Vulnerability information is also a key item to understand, and address when wanting to minimize the likelihood of a risk to actualize.

[16] ISO/IEC27005:2022 Information security, cybersecurity and privacy protection — Guidance on managing information security risks

The risk management process is not different for OT CS Risk management. however, there are some specific OT considerations when establishing the context and executing the risk assessment phase of the risk management process.

A common mistake when establishing the context for the risk assessment in OT is to either oversimplify the environment (by assuming all is the same) resulting in a very wide scope with minimal details, another is chopping the target into too small pieces, causing lots of work and all identified risks to be very low probability or impact as the assessment is only looking at a specific detail or sub control area.

Ideally, when determining the scope of a risk assessment, one should have the data flow diagram, detailed architecture, and network diagrams, process diagrams and business continuity plans at hand. Unfortunately, it is rare that all this information is available to support scoping. The challenge is that it is getting increasingly difficult to define what the control boundaries of a specific system are, without this information.

An alternative way to determine the context or scope of an assessment in OT environments is by addressing it from a functionality aspect. I.e., what are the functions the process requires to operate correctly. There are generally, two main functions, ensuring safety (process, environmental or health) and normal operation (i.e., the production of the site). A safe approach to start executing CS Risk Assessments is by addressing the safety functions first, as these will have the potential for the most critical impacts. The Hazard and Operability study (HAZOP[17]) and Layers of Protection analysis (LOPA[18]) are process safety analyses usually done at industrial sites. From these analyses it can be determined which components and system are required from a process safety perspective, and how their failures may impact the process itself. Cyber Security or intentional malicious activity is usually not included in HAZOP or LOPA analyses.

[17] Hazard and operability study (Wikipedia: https://en.wikipedia.org/wiki/Hazard_and_operability_study)
[18] Layers of protection analysis (Wikipedia: https://en.wikipedia.org/wiki/Layers_of_protection_analysis)

4.2 Compliance management

There are requirements and policies in most industries which the industrial operations need to be adhered to. The scope of these may also vary, meaning that it can be a small part of the industrial operations that is subject to regulatory oversight (i.e., the use of dangerous chemicals). Depending on the industrial operation's nature, the oversight of these rules and regulations differs. As an example, in industries where non-compliance can in the worst-case cause limited damage or impact to the surrounding environment (or customers), the oversight can be event based such that oversight activities are performed reactively if an incident have occurred. For high-impact industries where an incident can be high or catastrophic to the surroundings (i.e., deaths, severe environmental impacts etc.) the oversight is usually performed proactively.

Compliance requirements can also originate from contractual agreements or internal company policies. From a compliance management perspective, it does not matter where the requirement originates from, all need to be managed in a manner where their fulfillment can be proven if needed.

There are three activities that must be done to ensure compliance management.

1. Identify requirements.
2. Implement and document compliance.
3. Evaluate and monitor compliance.

Of these steps 2 and 3 are no different for OT than any other compliance management activity. But when focusing on cyber security compliance management the step for identifying requirements requires thorough analysis.

Normally, when thinking about cyber security compliance, the thoughts go towards security regulations or requirements. Which is correct, but not always sufficient in OT environments. In OT, identifying relevant regulatory requirements requires analysis of the regulations affecting the business operations. These need to be analyzed against the OT environment to identify the requirements set for the operations.

As an example, a water treatment plant has regulations on the availability of the supply and the quality of the water. None of these regulations are directly

security regulations. However, in this example, the water treatment plant is operated using digital systems (OT) which includes the normal process control and analytics of water quality. As the regulated topics are operated by digital components, they can also be influenced using digital means, hence setting indirect regulatory requirements on the Cyber Security of the operations even if it is not explicitly defined. To be fair, usually there are other additional quality processes implemented to ensure quality of the product, but experience have also shown that, after a while, if the digital system performs well and continuously produces valid results, businesses start to rely on it and cuts down on additional measures (unless specifically required by regulation) for cost savings.

The identification of these types of "indirect" regulations can be challenging, and the result very target dependent, making it more challenging to define an industry practice. The result of the regulatory impact is usually descriptive, i.e., setting a target level, which means that the operator of the installation needs to have the skills to define the actual Cyber Security requirements to be fulfilled to meet the regulation. This requires expertise of the industrial process and Cyber Security.

4.3 Performance and effectiveness monitoring

The purpose of performance monitoring is to have the capability to follow up and ensure that the cyber security performance is at the expected level. This is equally applicable to OT as to any other performance monitoring. Performance monitoring can be challenging to set up even in IT environments and one of the most common mistakes made with performance monitoring is to go "where least resistance" and use the technology data available without giving it a solid thought of what the measurement is all about. Another mistake is to mix statistics with performance monitoring. I.e., the number of alerts per month from the malware protection tool or number of thefts in a month are statistics and alone do not necessary provide any insight into the performance of the security operation. Activities also tend to lean towards what is measured, especially if personal incentives are based on them, and "you get what you measure". Therefore, a thorough consideration into what to measure is well spent time.

ISO27004[19] identifies two different types of measurements as following, *"a) performance measures: measures that express the planned results in terms of the characteristics of the planned activity, such as head counts, milestone accomplishment, or the degree to which information security controls have been implemented; b) effectiveness measures: measures that express the effect that realization of the planned activities has* on the organization's information security objectives.*"*

Both types are applicable to ISMS operations in OT, but there can be various practical challenges when implementing them. Performance measures in this situation could be to follow up on how the implementation of the ISMS procedures are progressing. Even if this type of measurement is quite straight forward, the challenge in OT comes from the management types and responsibilities, especially if the enterprise is a large multinational company. To make this measurement valid or meaningful, it needs to be ensured that all site responsible understand the expectations the same way and report the progress in a unified manner, which can be a time-consuming task for organizations implementing distributed or hybrid ISMS models.

4.3.1 Performance measure

As ISMS fundamentally is risk management, a practical example of a performance measure in OT could be measurement of performed risk assessments. This can be done as a direct calculation of number of risk assessments done for OT systems divided with total number of systems. This is, however, a measure with an end, i.e. at some point the organization will reach a stall point near 100% and after that point, this measure is not particularly useful. To make this measure longer term, it is recommended to turn towards the risk management policy or procedure. Risk management is a continuous activity that needs to be repeated (or evaluated) on regular basis. One way to do this is to set up time rules for risk assessments. As an example, if the policy stated, "All OT systems must have a risk assessment performed updated within the last 36 months". This would change the measurement to be a calculation of all systems with risk assessments done within the last 36 months divided in

[19] ISO27004:2016 Information technology. Security techniques. Information security management. Monitoring, measurement, analysis and evaluation

total number of systems. The result would be a floating % showing how well the organization is in line with the defined policy.

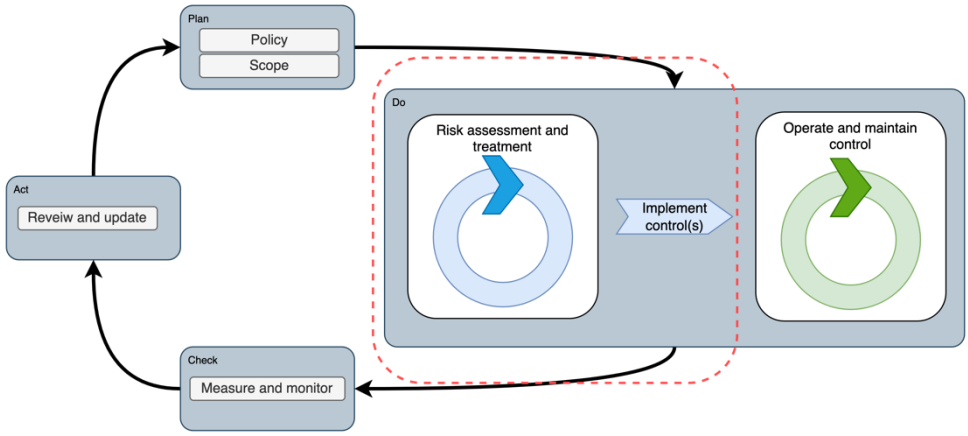

Figure 13: Typical scope of performance measure

4.3.2 Effectiveness measure

Effectiveness measures aim to show if the security controls applied provide the organizational value expected. I.e. do the implemented controls work as expected providing the defined value? Efficiency measures aim to reflect the return of the investment, even if it is not directly a monetary value.

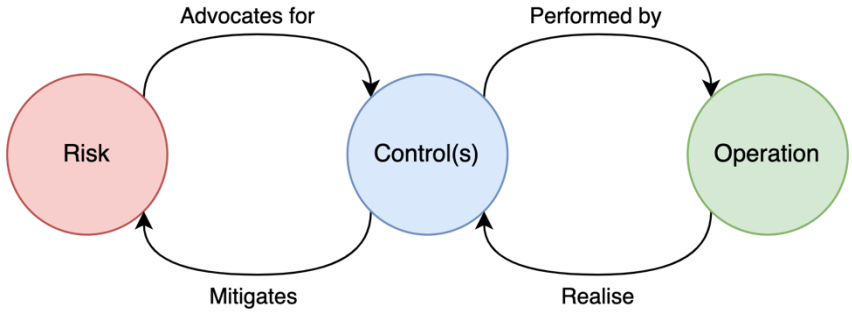

Figure 14: Risk to control to operation dependency

Taking network segmentation control as an example (commonly used in OT). A performance measure would measure if network segmentation has been applied (if deemed necessary by the risk assessment). Assuming a firewall has been procured and commissioned, this control can be set as “done” and the performance measure indicates “all good”. However, the efficiency measure focus on the value promised by the network segmentation control, which is to restrict unauthorized and unnecessary network communication to ensure operational stability. To ensure the correct and efficient operation of a fire-

wall you will, at least, need to ensure (and measure) that the firewall is commissioned correctly, the running ruleset is correct and that the firewall software is up to date.

Effectiveness measuring in OT environments is usually more challenging than in IT environments due to the technology diversity and fragmentation of the OT environments. The technological diversity causes efficiency problems when performing effectiveness measurements as effectiveness measurements usually require automatically collected technological data as source data. To make the data useful for measuring purposes it need to be comparable, and this makes this time consuming and expensive to do in diverse and fragmented environments.

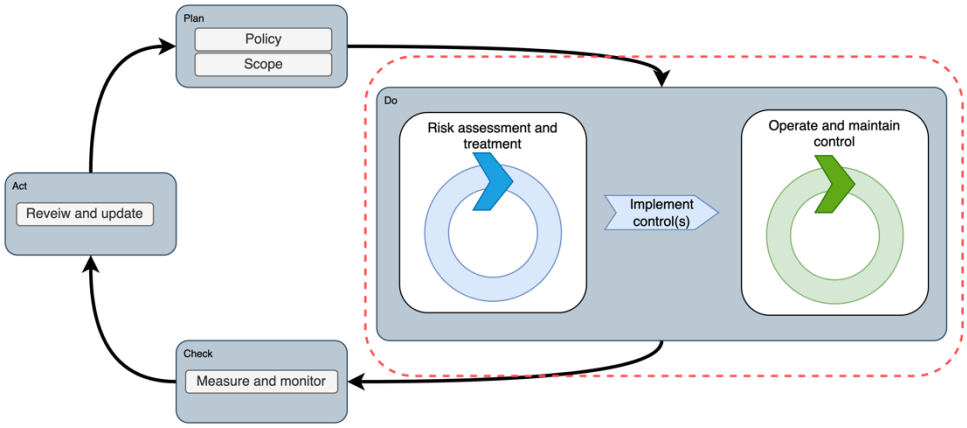

Figure 15: Typical scope of effectiveness measure

Another challenge with measuring the effectiveness of controls in OT is the use of compensating controls and how to map them into the efficiency measuring. A common example of this are controls related to Identity and access controls especially in control room environments where the ability to operate the system has precedence over the user identification. Control room operations may utilize shared credentials with autologin and never expiring sessions. While this would be a huge no-go in IT, this is common practice in OT, compensated with network segmentation and physical access restrictions into the control room itself.

4.3.3 Planning ISMS measures in OT

Measuring is important to be able to show progress or status, especially in the cyber security domain as the topic itself is intangible and can be hard to visualize or present in any other way.

There are many different options and methods available when measuring. This is also where thorough planning is to be done, as there are also many options to get it wrong. It is good to keep in mind that “you get what you measure”, therefore measures can even be counter effective if defined and implemented poorly.

A there are two common mistakes when measuring security, and they are especially valid for OT environments. These are the use of easy, available metrics (usually provided by some tool) or usage of technological statistic information available (like blocked network connection events in firewalls). Both have a common nominator in the technology used. I am not advocating that the usage of technology data is wrong, but rather that the data needs to be put into the business context and goals to have true value for the organization. At the same time, the organization must have the possibility to affect the measure outcome by adjusting their own actions, i.e. all measures need to be actionable.

Instead of going with the data easily available, the measures should be designed based on the organizational goals or the governance structure. Why are the organization investing in security? What are the items that matter? Is it the continuity of operation or the quality of the product, or transparency and traceability of it? By defining the value of security for the organization, more valid measurements can be defined and implemented, which in turn support achieving the organizational goals, not only security goals.

5 Conclusions and future considerations

Existing standards, frameworks and guides exist to support the implementation of security governance into OT environments. The foundational principles and procedures do not differ from practices applied in IT for decades and ISMS are possible to apply to OT. Despite this, OT has not been included in the ISMS scopes in organizations. The assumption is that this is due to differences in managerial responsibilities, but additional research into the area would clarify the root causes for this.

Regulatory requirements push especially critical infrastructure operators towards implementing ISMS in OT, not for the sake of existence, but to show sufficient risk management practices and evidence of such towards competent authorities responsible for performing the oversight. Implementing the ISMS in OT requires insight and considerations of the organizational structure, culture, and overall goals. The smaller the focus area of an ISMS is, the more straight forward its implementation process. This usually fits OT well, as the production lines and systems can be very independently operated, but implementing a very distributed ISMS may not fulfill the overall organizational goals and needs.

OT is highly diverse and built around specific operational (functional) needs. This results in highly specialized environments with specific vendor dependencies. This inevitably causes challenges for the operator to perform measurement of security performance and/or effectiveness. Hence this is an area which would benefit from an industry standard, making the security operations transparent and measurable both for the customer and the vendor.