Schweizerische Eidgenossenschaft
Confédération suisse
Confederazione Svizzera
Confederaziun svizra

Federal Department of Defence, Civil Protection and Sport DDPS

National Cyber Security Centre NCSC
Analysis and Prevention

2 July 2025

Technology brief

Information security management and ISMS

1 Introduction

In today's information society, information is vital to the operations of organisations and companies. It is usually stored, processed and transmitted electronically in the form of data. Because of its importance, this data must be protected to meet specific security objectives – such as confidentiality, integrity (or authenticity), and availability. Ensuring this protection is a demanding management task, often referred to as *information security management*, and is ideally supported by an *information security management system (ISMS)*.

This technology brief explores what exactly an ISMS is, what it is designed to do, and how it can best support those responsible for ensuring information security. It also examines what (cyber) risks are and how to manage them effectively as part of an information security management process or ISMS. Many of the ideas discussed also apply to other types of management systems. It is important to note that any management system should be considered within a broader management model, which may distinguish between political, strategic, tactical, and operational levels, for example. The integration of an ISMS (or other management systems) into such a model will not be addressed further in this brief.

2 Definition of terms

Due to its broad scope, the term 'ISMS' is defined in various ways in literature. According to DIN EN ISO/IEC 27000, an ISMS includes the policies, procedures, guidelines, resources and activities used by an organisation to protect its information assets. It provides a systematic framework for establishing, implementing, operating, monitoring, reviewing, maintaining and improving information security in line with business objectives.[1] A more narrowly focused definition found on Wikipedia describes an ISMS as the set of internal procedures and rules that an organisation uses to define, manage, monitor, maintain, and continuously improve its information security over time.[2] Building on this definition, the National Cyber Security Centre (NCSC) uses the following practical definition as a basis for its work:

[1] German version of ISO/IEC 27000:2016: *Informationstechnik – Sicherheitsverfahren – Informationssicherheits-Managementsysteme – Überblick und Terminologie*.

[2] https://de.wikipedia.org/wiki/Information_Security_Management_System

'An ISMS is a system made up of procedures and rules that can be implemented within an organisation or company to ensure information security – that is, to define concrete information security objectives, and to plan, manage, and ensure their achievement.'

Although this definition states that an ISMS is a system consisting of procedures and rules designed to achieve defined information security objectives, the concept of 'system' itself remains undefined. In the simplest case, an ISMS may consist only of a set of instructions presented as procedures and rules, or even just a list of recurring activities to be carried out. In addition, an ISMS may include tools and resources that support the person or team responsible for managing information security. These tools can vary widely in complexity. Unfortunately, the importance of tools is often exaggerated, and in some cases, the term 'ISMS' is equated with one or more tools. Following the saying 'a fool with a tool is still a fool,' some argue that an ISMS should be defined independently of any tools, and that it has nothing to do with tools by default.[3] Once a suitable ISMS has been defined, the question arises as to which tool or combination of tools might best support its implementation. However, this question should neither dictate the specification of the ISMS nor influence its content. In other words, the ISMS defines the requirements that tools must meet, not the other way around.

In addition to being independent of any specific tools, the NCSC identifies another key factor for the practical implementation of an ISMS as being an understanding of risks and how to deal with them. Typically, risk assessments focus on risks stemming from external and internal threats (i.e. threat-based risks). Another approach is to view risks purely in terms of their potential impact. In the case of data loss, for example, it is the loss itself that matters most. The cause of the loss (human error, technical failure or malware) is secondary when assessing the risk posed by such an event. Regardless of the cause, this kind of risk must always be mitigated – the underlying threat is irrelevant. Based on this idea, it is possible to develop an information security management approach that focuses solely on impact-based risks. However, before doing so, it is useful to take a closer look at how risks are currently handled.

3 Dealing with risks

In everyday use, the term 'risk' refers to a situation involving potential danger or harm. It is a broad concept, and people often perceive the same risk in very different ways – even when the risk is objectively measurable. Take the risk of a plane crash:[4] while statistically low, some people board flights without a second thought, while others develop a fear of flying. The actual risk is the same, but how it is perceived and assessed varies from person to person.

Even though people perceive risks differently, the general view in cybersecurity – and in information security management in particular – is that risks can be quantified and that decisions can be based on these figures. This is commonly referred to as a 'risk-based' approach. It typically involves selecting a set of defined threats and calculating the individual

[3] The origin of the saying is unclear, but it is most commonly attributed to the American computer scientist Grady Booch. To emphasise this point further, some have suggested a more pointed version: 'A fool with a tool is a more foolish fool.' A quote often attributed to Abraham Maslow makes a similar point: 'If all you have is a hammer, everything looks like a nail' – suggesting that no single tool is suitable for every problem.

[4] The risk of a plane crash can be quantified, for example, by dividing the number of plane crashes by the number of flights (per unit of time and per airline).

risk for each one – usually by multiplying the likelihood of an event by the potential impact of the resulting damage. The overall risk is then estimated as the sum of all individual risks.

This simple risk formula has shaped discussions in information security management, including in the context of ISMS, for a long time, and continues to dominate to this day. A common argument in favour of a risk-based approach is that the insurance industry has long been successful in quantifying risks and has built a business model around them. This approach is effective for everyday risks for which statistically meaningful data is available, particularly with regard to likelihood and potential impact. Examples include theft or accident insurance. However, insuring against a given risk becomes much more difficult when no reliable statistical data is available. In such cases, insurers sometimes launch provisional products and adapt them gradually based on real-world experience. Over time, this can lead to viable insurance solutions, even when it was initially unclear how to assess the risk or design a suitable product. This is exactly what is currently happening in the field of cybersecurity. Potential customers need to carefully assess proposed insurance offers on a case-by-case basis. These can vary significantly in terms of what they cover in the event of damage and the support services they provide. Having a cyber insurance policy does not necessarily mean that all potential risks in this area are well understood or can be reliably quantified. Where robust data is lacking, assumptions are made, and the data foundation is gradually built up over time.

From the NCSC's perspective, a risk-focused approach is fundamentally sound. However, the way cyber risks are assessed and managed needs to be reconsidered. Firstly, there is no 'defined set of threats' in cyberspace. And even if such a set did exist, the individual components of those threats are neither clearly defined nor exhaustively identifiable. As a result, it is not possible to define a meaningful probability space – that is, a structured basis for assigning probabilities to possible outcomes.[5] This means that probability theory can't really be applied, and calculating likelihoods becomes essentially arbitrary [1].[6]

Even aside from this formal difficulty, estimating the likelihood of threats in cyberspace is nearly impossible due to a lack of statistical data and the constantly evolving and complex nature of the environment. Consider, for instance, the probability of a data leak – how could that be meaningfully assessed? Almost any value could be chosen and justified. The same applies to estimating potential damage: virtually any amount could be justified, particularly if indirect or follow-on effects are considered. A buggy software update, for example, might have only a negligible impact in some cases. In others – such as the 2024 CrowdStrike incident – the damage could run into the billions, with estimates for that event alone differing by several billion. Because it is so challenging to estimate both the probability of occurrence and the potential extent of damage, the aforementioned simple risk formula is either unusable or must be revised or expanded. Unfortunately, no such revision or expansion has yet been made, meaning that the formula is impractical and, to some extent, unrealistic.

In reality, risks are often dealt with heuristically instead of formally [2, 3]. A useful analogy is the way a general practitioner works. When assessing the health of a patient, a doctor doesn't work through a fixed list of possible illnesses or rely on probabilities and estimated levels of harm. Instead, he or she draws on background knowledge and carries out targeted examinations or tests to assess the patient's condition as accurately as possible, then proposes a suitable treatment based on experience and heuristics. Additionally, the doctor

---

[5] Formally, a probability space consists of a set of possible events and a probability measure that assigns each event a value between 0 and 1, in line with the three Kolmogorov axioms.

[6] One possible workaround would be to define a separate, single-event probability space for each threat. But to satisfy Kolmogorov's axioms, each of those events would have to be assigned a probability of 1 – which calls the usefulness of the entire approach into question.

may provide general health advice (such as recommendations for a healthy diet and regular physical activity) that applies regardless of the patient's current condition. A similar approach can be applied to cybersecurity, specifically to information security management and the design and operation of an ISMS: combining a baseline level of protection with targeted enhancements.

4 Conclusions and outlook

An ISMS should provide the best possible support to the person or team responsible for managing information security. Although its support function may give the impression that an ISMS is primarily a tool, this is not its defining characteristic. At its core, an ISMS consists of procedures and rules. These can be implemented using tools, but this is not a requirement. Therefore, the emphasis should be placed on procedures and rules rather than tools. It also makes sense to move away from risk calculations in information security management and cyber risk handling, and adopt heuristic approaches instead. Just as human health is too complex for simple formulas, so too is cybersecurity – making heuristics a better fit to handle its complexity.

Based on these findings, the NCSC is currently developing a structured method to strengthen cybersecurity and resilience. This method will be publicly available and can be used by organisations of any size and in any sector to prepare for relevant threats, as well as to develop and implement an ISMS in line with the recommendations set out in this document. Naturally, it will be possible to expand and further develop such an ISMS over time.

References

[1] Andreas Grünert, James Bret Michael, Rolf Oppliger and Ruedi Rytz, Why Probabilities Cannot Be Used in Cyber Risk Management, *IEEE Computer*, Vol. 57, No. 10, October 2024, pages 86–89

[2] Rolf Oppliger and Andreas Grünert, How to Manage Cyber Risks: Lessons Learnt from Medical Science, *IEEE Computer*, Vol. 56, No. 1, January 2023, pages 117–119

[3] Rolf Oppliger and Andreas Grünert, How to Measure Cybersecurity and Why Heuristics Matter, *IEEE Computer*, Vol. 57, No. 2, February 2024, pages 111–115