
AI Support for Establishing and Operating an Information Security Management System (ISMS)

Florian Großimlinghaus, Marko Schuba, Tim Höner, Sacha Hack, and Georg Neugebauer

Aachen University of Applied Sciences, Aachen, Germany

ABSTRACT

The increasing complexity of information security threats and ever more stringent legal requirements mean that more and more organizations are setting themselves the goal of implementing an effective and efficient information security management system (ISMS). This paper examines the ways in which artificial intelligence (AI) in the form of a chatbot can support the development and operation of an ISMS. In particular, it evaluates how a chatbot can be integrated into standard setup and operating processes within an ISMS. In addition, various possible applications are shown and advantages, disadvantages and limitations are discussed. It turns out that the use of a chatbot as a supporting tool has many advantages and, in the hands of specialist personnel, offers a useful addition to established methods. Consequently, chatbots open up the possibility for organizations to optimize their organizational and operational processes.

Keywords: Information security management systems, ISMS, AI, Chatbot, Implementation, Operation

INTRODUCTION

The area of information security has become increasingly important in recent years. Reasons for this include the numerous cyberattacks that have affected organizations and companies of various industries and sizes, as well as the public sector. In addition, these topics are also increasingly gaining political attention, for example through the NIS2 Directive in the EU (European Parliament, 2023). One way to systematically strengthen information security is to introduce an information security management system (ISMS) with corresponding policies and controls (ICS2, 2023; BSI Annual Report, 2023; NIS Investments, 2023; BSI NIS2, 2024; EU NIS2, 2024; FBI Internet Crime, 2023). However, this requires extensive expertise or specialists in the field of cybersecurity, which is currently lacking worldwide (ICS2, 2023). In view of this problem, methods to increase efficiency in the introduction of ISMSs are not only helpful, but necessary.

One approach that promises to increase efficiency in many areas of information processing is the use of artificial intelligence (AI). AI-based software solutions are already providing support for many everyday and

specialized tasks, for example in the form of chatbots. This raises the question of the extent to which AI in the form of chatbots can be used to support the implementation and operation of an ISMS. The aim of this article is therefore to work out possible procedural integrations of chatbots in the ISMS context and to highlight advantages, disadvantages and limitations.

BACKGROUND

Information Security Management Systems

Management systems refer to a documented way within an organization to bundle activities, tools and methods for the organization and use them to achieve objectives for the underlying scope of application (see ISO 9000, 2015 sections 3.3.3, 3.5.1, and 3.5.3). There are various management system standards that specialize in different thematic areas. The certification of a management system offers the opportunity to provide proof of conformity with the requirements of the corresponding standard. Examples of management systems include quality management systems, energy management systems, occupational health and safety management systems and information security management systems. This article focuses on information security management systems and their implementation and operation with the help of a chatbot.

Management systems are often based on a process for continuous improvement, such as the well-known Plan-Do-Check-Act (PDCA) cycle (see ISO 9001, 2015). This means that a management system is constantly evolving as a central component and reacts to changes within and outside the organization. A management system is therefore never finished, but is regularly evaluated and, if necessary, adapted in a controlled manner.

The introduction and correct handling of an information security management system, or ISMS, offers organizations an opportunity to systematically and demonstrably increase the level of information security in the organization. When setting up an ISMS, a list of controls is checked for their applicability to the organization. These controls include policies, processes and potential technical measures. They also include controls for monitoring success. In order to be able to implement the selected controls in a sufficient manner, the organization's management needs to provide the necessary resources and to establish a suitable security organization. Afterwards, the details of the ISMS can be worked out, implemented and put in operation. However, the information security management system can only be effective if it is actually implemented systematically within the organization and actively lived by all those involved.

Chatbots

Chatbots based on Large Language Models (LLMs) offer the possibility of answering questions and performing other tasks such as generating source code, images or other content. The basic application of the chatbot acts as a kind of interactive assistant that interacts directly with the user or provides additional functionalities such as an API. At the core of the basic

application is the integrated LLM, which has been trained in advance with very large amounts of data, processes the actual request and returns the result (Kumar et al., 2024).

In addition, there are LLMs that can be integrated in different ways for basic applications. These have either been trained very generally or sometimes specifically with regard to resource usage and area of application. This gives the user the opportunity to select a language model that is optimal for their purpose and based on the available resources, and even to use and exchange it with the same base application. The structure of the basic application often remains similar or, in extreme cases, even unchanged. Application examples include the general answering of knowledge questions, the generation and optimization of source code, the creation of summaries and the text-based generation of images and videos (Hugging Face, 2024; Yan, 2024).

There are numerous commercial and non-commercial basic applications. These offer different functionalities such as operation via a local installation, the integration of local documents (extension of the LLM), training or the so-called “fine tuning” of your own LLM and the provision of the chatbot via API or web server (ChatGPT, 2024; PrivateGPT, 2024; GPT4All, 2024).

It can therefore be said that interactive chatbots offer a way to bundle many different functionalities of differently specialized LLM and AI solutions. This makes the supportive integration of interactive chatbots in everyday commercial and non-commercial life interesting.

RELATED WORK

At present, the authors are not aware of any work that systematically evaluates the support provided by a chatbot for the implementation and operation of an ISMS. In general, little research has been carried out in neighboring areas, such as “A Chatbot for Information Security” (Hamad and Yeferny, 2020) or “Chatbots: A Framework for Improving Information Security Behaviors using ChatGPT” (Gundu, 2023). Hamad and Yeferny propose AI to support users by acting as an advisor for general information security questions, while Gundu focuses on the usage of AI for cybersecurity training and awareness.

However, the lack of relevant literature is not surprising, as AI solutions such as ChatGPT were only presented in Nov 2022 (OpenAI, 2022) and the breadth of possible applications in science and business is only just beginning. The use in the field of information security and especially in the field of ISMS is only one of many options for the use of chatbots. This paper aims to address and partially close the current gap in the systematic application of AI in the field of ISMS.

CONSIDERATIONS ON THE USE OF CHATBOTS FOR ISMS

Fields of Application in the Area of ISMS

ISO 27001 was chosen as the basis for the ISMS implementation because it is a widely used standard, enables normative certification and can therefore be considered a very realistic choice for an ISMS (ISO 27001, 2022). In order

to assess the usefulness of chatbots for the development and operation of an ISO 27001 ISMS, possible areas of application in which a chatbot could be used on a trial basis were first defined. These areas have been structured as work packages that relate to initial tasks when implementing an ISMS as well as its subsequent regular operation. It should be noted that the grouping of work packages is an exemplary breakdown of some of the core activities involved in setting up and operating an ISMS. It is possible to create further work packages and differentiate between them.

The work packages include the creation of an information security policy, other required policies, the mandatory statement of applicability, the implementation and operation of risk management as well as asset management, the controls from the catalogue in Annex A of ISO 27001, the continuous improvement process, the announcement to interested parties and the associated communication processes.

Chatbot Requirements

The selection of a suitable basic application and a suitable language model, which will later serve as a chatbot for interaction with the user, depends on numerous technical, organizational and legal criteria. Not every basic application and not every language model is equally suitable as a solution. Depending on the context of the organization, there may be other criteria that need to be considered when selecting a suitable chatbot.

The technical selection criteria include expandability in the context of open source projects, the national language in which the LLM is trained or specialized, the hardware requirements for operating the chatbot, subsequent scalability after initial commissioning, the integration of local documents or other content to expand the knowledge base and context, the available protocols and APIs for comprehensive human-machine and machine-machine communication and the integrability of different LLMs into the basic application.

As part of the organizational criteria, the economic efficiency of the support provided by the chatbot, the maintainability of the required infrastructure, the ability to integrate into existing processes, the requirements for user interaction and the up-to-dateness of the LLM's database are considered.

The legal criteria include the licensing of the components used, the copyright status of the generated content and compliance with other organization- or country-specific regulations and laws.

CHATBOT TEST SETUP

PrivateGPT (PrivateGPT, 2024) and GPT4All (GPT4All, 2024) were selected as basic applications for the test setup. All previously defined selection criteria for the basic application are sufficiently fulfilled by PrivateGPT and GPT4All. Two basic applications were selected for the test setup as they have two different unique selling points. While PrivateGPT is a Python-based basic application that is highly extensible and customizable through the use of the

API and further scripting, GPT4All is a so-called plug-and-play solution that is ready for use within a very short time thanks to its installation software.

Meta's "LLMA 3.1 8B Instruct" was used as the integrated LLM for the test scenarios. This LLM offers sufficient accuracy for the test purposes within the test setup while at the same time meeting acceptable hardware requirements. For larger production environments in an organizational context, other versions such as the "LLMA 3.1 70B" or the "LLMA 3.1 405B" are available, which place significantly higher demands on the hardware, but also tend to deliver higher quality results (LLAMA, 2024).

The data sets of the chatbots have been expanded using the integrated functionality of the GPT4All and PrivateGPT basic applications. As soon as documents are stored and integrated as a context, they are taken into account for requests to the chatbot. Alternatively, individual specific content can be provided as context for the requests at the start of each request. The documents that are stored to expand the data set can be very diverse and their integration should be weighed up depending on the expected purpose. While it may make sense to provide an employee who is responsible for the implementation and operation of the ISMS with extensive documentation on the context of the organization, contractual and legal documents, policies, ISMS documentation and other relevant documents, it should be carefully weighed up whether this content may be disclosed externally if the chatbot is intended to be used for a purpose where external interested parties can also access the content of the documents.

CHATBOT TEST RESULTS

All work packages described in the earlier "Considerations" section were tested, evaluated and assessed. For each of these work packages, a standard process - without the use of a chatbot - has been enhanced with chatbot specific extensions. Please note that such processes should be considered as simplified process examples, which will vary from organization to organization and could become more complex if desired. In the following sections, two exemplary applications of chatbots for work packages are given.

Exemplary Integration of the Chatbot for Policy Generation

The following is an example of the procedural integration of the chatbot for the second work package (creating and maintaining required policies, cf. Fig. 1).

The chatbot enhanced process for creating and maintaining the policies contains a useful extension for the use of the chatbot in almost all steps, which can also be transferred to most other work packages. Only the final enactment of the policy in point (7) remains a completely manual task, which could at best be supported in the subsequent communication with the stakeholders. The chatbot is used here as a knowledge base to be used systematically, as a tool to support the creation of the document structure and as a tool for reviewing the policy. While its use as a knowledge base is particularly evident in points (4) and (8), the focus on supporting the creation

of documents becomes clear in points (2), (3) and (5). In point (1), the chatbot is used both as a knowledge base and as a tool for creating an overarching document structure to determine which types of policies are needed and which controls should be included in which policy. A general review of the information security policy as well as a possible compliance check takes place primarily in point (6).

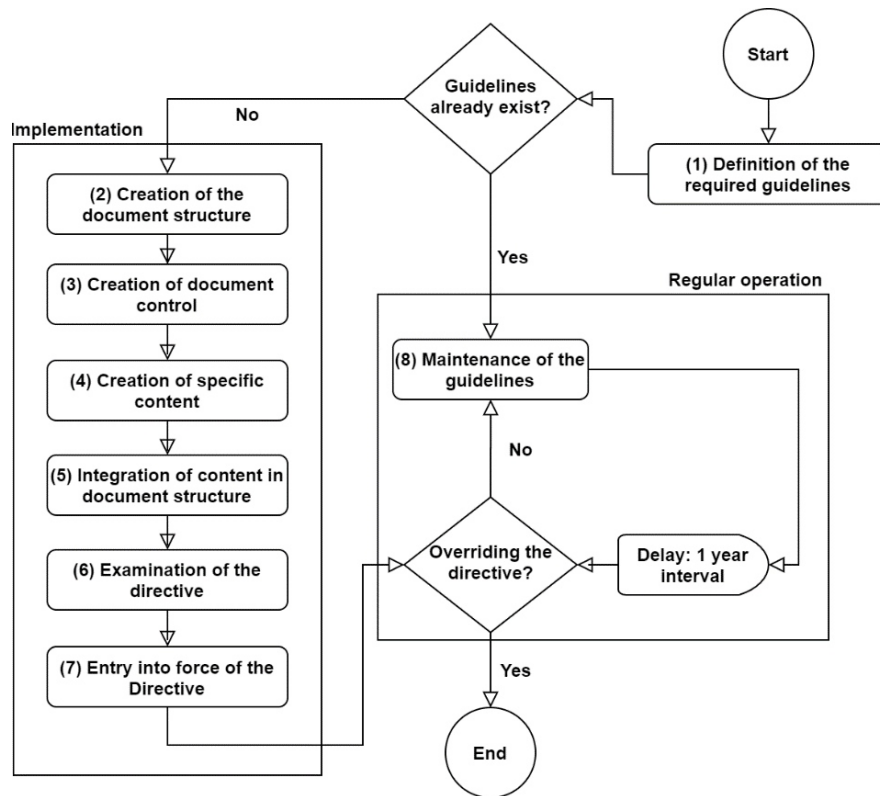


Figure 1: Standard (non-chatbot) process for creating and maintaining ISMS policies.

In order to evaluate the advantages and disadvantages of integrating a chatbot into the policy creation and maintenance process, various topic-specific requests were sent to the chatbot to check the effectiveness of integrating a chatbot into the example process shown. The requests are sent to the chatbot immediately before or during the respective process step of the standard process.

During the initial generation of the document structure in point (2) of the process flow, initial ideas for the respective policies can already be collected. This is followed by the document control (3) which includes metadata such as the document properties, the document and release status as well as a document history that precedes the actual content, and more metadata like the effective date of the document and the signature at its end. Document control metadata can be generated on the basis of frequently encountered metadata common in the document control sections of existing

ISMS documents (see BSI example information security policy, BSI Guideline 2020). It is advisable to generate the chapters individually from the previously created document structure of the respective policy, as this tends to make them more detailed and allows to limit the effects of changes in the request to just one chapter.

For more details on how an individual process step works, the chatbot request to generate the technical content for a password policy for a specific organization (step (4) of the overall process) is illustrated in Figure 2. The chatbot answer in the same figure shows that the chatbot can provide relevant technical and organizational standards, recommendations and information matching the desired policy. Depending on the type of request, the chapters can either be generated together based on the previously generated document structure or the chapters can be generated individually and then manually inserted into the structure.

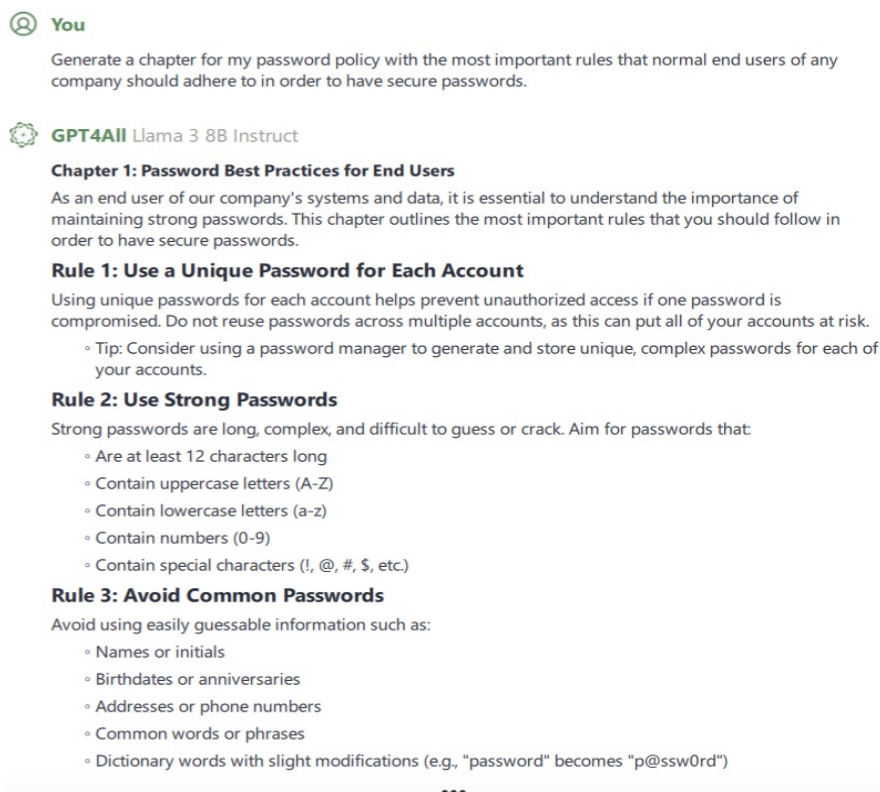


Figure 2: Request for generating the content of a password policy (output clipped).


To check the respective policies after the integration of the individual chapters in point (6), chapters or even the entire document can be transferred and checked for optimizations or errors. In the test scenario, for example, the generated minimum password requirements from point (4) were manipulated and passed to the chatbot for checking. During the transfer, some content, such as specific technical and organizational requirements, was removed and

the chatbot was instructed to check the minimum password requirements. The chatbot recognized these and pointed out gaps in the minimum technical and organizational requirements. In addition, further optimization points were identified. As soon as the policies have come into force and are transferred to regular operation, a regular check for changes can be carried out in the same way as point (6). This takes place in regular operation via a delayed maintenance loop in point (8). Over the years, new laws and standards may become established, for example, which will be taken into account by the chatbot in future revisions.


Exemplary Integration of the Chatbot for SoA Creation

When creating an ISMS in accordance with ISO 27001:2022, a Statement of Applicability (SoA) has to be created for the individual Annex A controls. ISO 27001 Annex A is a central collection of 93 security controls to help organizations strengthen their information security. It serves as a toolbox from which to select applicable controls that are relevant to the organization, depending on its needs and the scope of its ISMS. The standardized controls help to effectively protect information assets and minimize risks.

To simplify implementation for an organization, the chatbot can be used to generate an exemplary SoA document structure at different levels of granularity (cf. Fig. 3 for an example). This enables the organization to implement the SoA for the first time in an efficient manner and to orient itself on effective examples.

 You

I need a Statement of Applicability (SoA) for my ISO 27001 certification. Create a complete tabular document structure for the structure as it is usual for a SoA. This should be compliant with ISO 27001. As a minimum, there should be columns for the control ID of Annex A, the title of the control, the applicability status, the associated justification and the implementation status. Suggest further useful columns. Give me suitable examples.

 GPT4o | Llama 3 8B Instruct

Here is a complete tabular document structure for the Statement of Applicability (SoA) as per ISO 27001:

Statement of Applicability

Control ID (Annex A)	Title of Control	Applicability Status	Associated Justification	Implementation Status
A.4.1	Information Security Policy	Applicable	The organization has a formal information security policy that outlines its commitment to protecting sensitive data and ensures all employees are aware of their responsibilities in this regard.	Implemented
A.5.2.1	Access Control Policies - User Authentication	Not Applicable	The organization does not have any physical or logical access controls, as it is a small team with minimal sensitive information.	N/A
A.6.1.3	User Registration and De-provisioning - Account Management	Partially Applicable	All employees are required to register their accounts upon joining the organization, but de-provisioning process needs improvement.	In Progress
...

Additional Columns:

- **Implementation Date:** The date when the control was implemented or is planned to be implemented.
• Example: A.4.1 - Information Security Policy (Implemented on 01/02/2023)
- **Responsible Person/Team:** The individual or team responsible for implementing and maintaining each control.
• Example: A.6.1.3 - User Registration and De-provisioning - Account Management (John Smith, IT Department)
- **Review Frequency:** The frequency at which each control will be reviewed and updated (e.g., annually, quarterly).
• Example: A.4.2 - Risk Assessment (Reviewed every 12 months)
- **Next Review Due Date:** The date by which the next review of each control is due.
• Example: A.5.1.3 - Cryptographic Controls (Due for review on 31/03/2024)

...

Figure 3: Request for generating an initial statement of applicability (output clipped).

When analyzing the chatbot answer of Fig. 3 advantages and drawbacks of the solution become obvious. While the output delivers a useful initial SoA document structure, the mistakes in the above output might only be detected by experts in the field: the Control IDs (left column) are not correct, as they neither match any of the IDs used in the latest 2022 version of the standard nor are they correct for earlier versions. A solution to this could be a manual correction of the IDs in the output or an improvement of the LLM by providing a better learning data set.

Recommendations for Chatbot Usage in the Context of ISMSs

The two integration examples of the chatbot for policy or SoA generation described above are only two of several tested use cases. Similar promising applications of chatbots were identified for other ISMS work packages. These include the creation of the information security policy in the organizational context, establishment and operation of suitable risk management, implementation of other controls from Annex A of ISO 27001, implementation and operation of asset management for information and other related assets, continuous improvement process, and communication to internal and external interested parties.

In general, it should be noted that the more organizational context is provided and the more detailed and precise the requirements are described in the chatbot request, the better the results tend to be. The question in Fig. 3, for example, is very general and brief in order to assume a simple scenario in which not much preparatory work has been invested in the ISMS and a low level of knowledge on the part of the user is assumed.

CONCLUSION

Numerous possible applications for the meaningful use of a chatbot in the development and operation of an ISMS were identified. For various application options it could be shown – for one example explicitly in this paper – that a chatbot is demonstrably a useful support tool in the hands of suitable specialist personnel. Despite the many advantages and support options, current chatbots are not yet technologically advanced enough to take on tasks independently and unsupervised. According to the current state of the art, a chatbot is to be regarded as a medium that is a powerful tool in the hands of trained specialist staff. However, trained specialist personnel must interpret the results correctly, check them and correct them if necessary. In the case of untrained personnel, chatbots run the risk of inconsistent or incorrect results being accepted without verification, which can have severe consequences for information security.

The advantages, disadvantages and limitations that could be identified overall and generally for all work packages are extensive and very diverse. For example, it was found that the advantages include the generation of a structural framework, the generation of examples, the preparatory work for researching, analyzing and evaluating content, knowledge generation, information processing, the generation of requirements, the generation of implementation plans, the answering of specific questions and the

automation of recurring tasks. However, at this stage, some global and general drawbacks and limitations have also been identified, including the strong dependence on the timeliness of the database, the need for context checking, the occurrence of hallucinations, the output of inconsistent or incomplete results and the potentially large differences in results depending on the LLM used. These disadvantages and limitations require an almost constant review of the results by trained professionals.

With the vast development of LLMs and other AI solutions in recent years it is to be expected that the quality and accuracy of query processing and result generation will further increase as the performance of LLMs and other AI solutions improves. It can also be assumed that the variety of applications and the accuracy of the current application possibilities will continue to improve. The use of chatbots will therefore remain a highly relevant topic for ISMS in the future.

REFERENCES

- BSI Annual Report. (2023). Die Lage der IT-Sicherheit in Deutschland 2023 (in German). Bundesamt für Sicherheit in der Informationstechnik. Website: <https://www.bsi.bund.de/SharedDocs/Downloads/DE/BSI/Publikationen/Lageberichte/Lagebericht2023.pdf> (accessed on Nov 20, 2024).
- BSI Guideline. (2020) Leitlinie zur Informationssicherheit der RECPLAST GmbH (in German). Bundesamt für Sicherheit in der Informationstechnik. Website: https://www.bsi.bund.de/SharedDocs/Downloads/DE/BSI/Grundschutz/Hilfsmittel/Recplast/A01_Sicherheitsleitlinie.pdf (accessed on Nov 20, 2024).
- BSI NIS2. (2024) EU-Richtlinien zur Netzwerk- und Informationssicherheit - Nationale Umsetzung und Rolle des BSI. Bundesamt für Sicherheit in der Informationstechnik (in German). Website: https://www.bsi.bund.de/DE/Das-BSI/Auftrag/Gesetze-und-Verordnungen/NIS-Richtlinien/nis-richtlinie_node.html (accessed on Nov 20, 2024).
- ChatGPT. (2024) ChatGPT. OpenAI Inc. <https://openai.com/chatgpt/> (accessed on Nov 20, 2024).
- EU NIS2. (2024) Directive on measures for a high common level of cybersecurity across the Union (NIS2 Directive). European Commission. Website: <https://digital-strategy.ec.europa.eu/de/policies/nis2-directive> (accessed on Nov 20, 2024).
- European Parliament. (2023) The NIS2 Directive - A high common level of cybersecurity in the EU. Website: [https://www.europarl.europa.eu/thinktank/en/document/EPRS_BRI\(2021\)689333](https://www.europarl.europa.eu/thinktank/en/document/EPRS_BRI(2021)689333) (accessed on Nov 20, 2024).
- FBI Internet Crime. (2023) Internet Crime Report 2023. Federal Bureau of Investigation. https://www.ic3.gov/Media/PDF/AnnualReport/2023_IC3Report.pdf (accessed on Nov 20, 2024).
- GPT4All. (2024) GPT4All. GitHub Inc. Website: <https://github.com/nomic-ai/gpt4all> (accessed on Nov 20, 2024).
- Gundu, Tapiwa. (2023) Chatbots: A framework for improving information security behaviours using chatgpt. In: Furnell, S., Clarke, N. (eds) Human Aspects of Information Security and Assurance. HAISA 2023. IFIP Advances in Information and Communication Technology, vol. 674. Springer, Cham. https://doi.org/10.1007/978-3-031-38530-8_33
- Hamad, Sofian and Yeferny, Taoufik. (2020) A Chatbot for Information Security. IJCSNS International Journal of Computer Science and Network Security, Vol. 20 No. 4, April 2020. <https://doi.org/10.48550/arXiv.2012.00826>

- Hugging Face. (2024) Models. Hugging Face Inc. Website: <https://huggingface.co/models> (accessed on Nov 20, 2024).
- ICS2. (2023) Cybersecurity Workforce Study, Website: https://media.isc2.org/-/media/Project/ISC2/Main/Media/documents/research/ISC2_Cybersecurity_Workforce_Study_2023.pdf?rev=28b46de71ce24e6ab7705f6e3da8637e (accessed on Nov 20, 2024).
- ISO 27001. (2022) ISO/IEC 27001:2022 Information security, cybersecurity and privacy protection - Information security management systems – Requirements. <https://www.iso.org/standard/27001> (accessed on Nov 20, 2024).
- ISO 9000. (2015) ISO 9000:2015(en) Quality management systems — Fundamentals and vocabulary. Website: <https://www.iso.org/standard/62085.html> (accessed on Nov 20, 2024).
- ISO 9001. (2015) ISO 9001:2015 Quality management systems — Requirements. Website: <https://www.iso.org/obp/ui/#iso:std:iso:9000:ed-4:v1:en> (accessed on Nov 20, 2024).
- Kumar, Vimal. Srivastava, Priyam and Dwivedi Ashay. (2024) Large-Language-Models (LLM)-Based AI Chatbots: Architecture, In-Depth Analysis and Their Performance Evaluation. In: Santosh, K., et al. Recent Trends in Image Processing and Pattern Recognition. RTIP2R 2023. Communications in Computer and Information Science, vol. 2027. Springer, Cham. https://doi.org/10.1007/978-3-031-53085-2_20
- LLAMA. (2024) Llama 3.1 Requirements. Llama 3 AI. Website: <https://llamaimodel.com/requirements/> (accessed on Nov 20, 2024).
- NIS Investments. (2023) NIS Investments Report 2023. European Union Agency for Cybersecurity. Website: <https://www.enisa.europa.eu/publications/nis-investments-2023> (accessed on Nov 20, 2024).
- OpenAI. (2022) Introducing ChatGPT. Introducing ChatGPT. Website: <https://openai.com/index/chatgpt/> (accessed on Nov 20, 2024).
- PrivateGPT. (2024) PrivateGPT. GitHub Inc. Website: <https://github.com/zylon-ai/private-gpt> (accessed on Nov 20, 2024).
- Yan, Eugene. (2024) A list of open LLMs available for commercial use. GitHub Inc. Website: <https://github.com/eugeneyan/open-llms> (accessed on Nov 20, 2024).