Statement of Applicability (SoA) Compliance Report

The report was generated on: 11:32:37 2024/05/02.

Contents

Questionnaire: ISMS questionnaire 2022

5. Policies for information security

- Best Practice
- Risk evaluated

Reason of choice

As a cybersecurity company, information security is essential for business operations. Employees should be aware and well informed.

5.1. Information security roles and responsibili-ties

- Best Practice
- Risk evaluated

5.1.a. Reason of choice

Governance of information security can enhance business operations and make sure that security tasks are well performed within CSIS.

5.1. Segregation of duties

- Best Practice
- Risk evaluated

5.1.a. Reason of choice

CSIS needs to make sure that company records are not altered due to lack of proper access control, segregation of duties and supervision.

5.2. Management responsibilities

- Best Practice
- Risk evaluated

5.2.a. Reason of choice

For business operations, personnel has to know their tasks and responsibilities communicated by management. Probable areas: access control, assets, incident response, etc...

5.3. Contact with authorities

- Best Practice
- Legal requirement

5.3.a. Reason of choice

As a company in EU, GDPR and other, for example, tax related legislations require the contact with authorities.

5.3.b. Legal requirements and directives

- Personal Data Legislation

5.4. Contact with special interest groups

- Best Practice
- Legal requirement
- Risk evaluated

5.4.a. Reason of choice

Based on GDPR, CSIS is responsible to reach out to private persons if they are subject to data breach.

5.4.b. Legal requirements and directives

- Personal Data Legislation

5.5. Threat intelligence

- Best Practice
- Risk evaluated

5.5.a. Reason of choice

Since CSIS' operations are based on sensitive customer data, threats and vulnerabilities of the system have to be monitored, analysed and mitigated.

5.6. Information security in project management

- Best Practice
- Risk evaluated

5.6.a. Reason of choice

Since CSIS internal projects might involve sensitive and confidential data, information security risks have to be addressed and managed.

5.7. Inventory of information and other associated assets

- Best Practice
- Risk evaluated

5.7.a. Reason of choice

At CSIS, due to sensitive and confidential data, governance and ownership is important to preserve information security and prevent unauthorizes access.

5.8. Acceptable use of information and other associated assets

- Risk evaluated
- Best Practice
- Contractual requirement

5.8.a. Reason of choice

At CSIS, we handle sensitive and confidential customer data and information accessible through company assets has to be protected.

5.9. Return of assets

- Risk evaluated

5.9.a. Reason of choice

Necessary in order to avoid data breech and unauthorized access.

5.10. Classification of information

- Best Practice
- Risk evaluated

5.10.a. Reason of choice

Since CSIS' business operations are highly dependent on information obtained by customers, classification of this information is needed for secure and effective operations.

5.11. Labelling of information

- Best Practice

5.11.a. Reason of choice

CSIS operates with personal and confidential information.

5.12. Information transfer

- Best Practice
- Risk evaluated
- Legal requirement

5.12.a. Reason of choice

CSIS has to comply with EU data protection regulations and maintain integrity towards customers through secure data handling.

5.12.b. Legal requirements and directives

- Personal Data Legislation

5.13. Access control

- Best Practice
- Risk evaluated

5.13.a. Reason of choice

Important for everyday operations.

5.14. Identity management

- Best Practice
- Risk evaluated

5.14.a. Reason of choice

Necessary for effective access control since CSIS handles sensitive and confidential data.

5.15. Authentication information

- Risk evaluated

5.15.a. Reason of choice

Important for effective access control because of confidential company and customer data.

5.16. Access rights

- Best Practice
- Risk evaluated

5.16.a. Reason of choice

CSIS has to make sure that company and customer information is only accessed by authorized personnel.

5.17. Information security in supplier relationships

- Best Practice
- Risk evaluated
- Contractual requirement

5.17.a. Reason of choice

At CSIS it is important that our suppliers maintain security measurements and do not jeopardize CSIS security level.

5.18. Addressing information security within supplier agreements

- Best Practice
- Risk evaluated
- Contractual requirement

5.18.a. Reason of choice

CSIS acknowledges different supplier relations and emphasizes the importance of supplier agreements to ensure that both parties know their information security obligations.

5.19. Managing information security in the ICT supply chain

- Best Practice

5.19.a. Reason of choice

Information security within the ICT supply chain at CSIS is essential to protect company and customer data and maintain high level of information security within the company.

5.20. Monitoring, review and change management of supplier services

- Contractual requirement
- Best Practice

5.20.a. Reason of choice

At CSIS, the maintained and constant information security is important when it comes to supplier services. Changes within these services must be managed.

5.21. Information security for use of cloud services

- Best Practice
- Risk evaluated

5.21.a. Reason of choice

CSIS uses cloud services, hence, the information security related to these services is essential to maintain information security within CSIS as well.

5.22. Information security incident management planning and preparation

- Best Practice
- Risk evaluated
- Legal requirement

5.22.a. Reason of choice

CSIS has implemented various controls to detect and take actions against the threat actors with malicious intent. These controls aim to reduce the likelihood of both internal and external actors successfully committing a malicious act undetected.

5.22.b. Legal requirements and directives

- Personal Data Legislation

5.23. Assessment and decision on information security events

- Best Practice
- Risk evaluated

5.23.a. Reason of choice

CSIS aims to create a well-defined incident response plan in place to minimize the damage caused by a successful attack and quickly identify and take actions against the attackers. This includes the categorization and prioritization of security events.

5.24. Response to information security incidents

- Risk evaluated

5.24.a. Reason of choice

CSIS has an incident response plan in place to ensure quick and effective response to any security incidents. This plan must be followed for consistent efficiency.

5.25. Learning from information security incidents

- Best Practice

5.25.a. Reason of choice

AT CSIS it is important that we keep up to date and strengthen the information security system by learning from previous incidents.

5.26. Collection of evidence

- Best Practice
- Legal requirement

5.26.a. Reason of choice

Evidence-collection is important to comply with legal obligations and apply best practices.

5.26.b. Legal requirements and directives

- Personal Data Legislation

- Bookkeeping Act
- Financial Business Act

5.27. Information security during disruption

- Best Practice
- Risk evaluated
- Contractual requirement

5.27.a. Reason of choice

CSIS should have a plan for information security during disruption since the company handles sensitive information.

5.28. ICT readiness for business continuity

- Best Practice
- Risk evaluated

5.28.a. Reason of choice

Since CSIS uses ICTs, the maintenance and testing of these technologies is important to maintain business continuity in case of disruption.

5.29. Legal, statutory, regulatory and contractual requirements

- Best Practice
- Risk evaluated
- Contractual requirement
- Legal requirement

5.29.a. Reason of choice

CSIS handles sensitive information, therefore, the company has to make sure that it complies with customer and supplier contracts, legal obligations, and that personnel is well-trained to do so.

5.29.b. Legal requirements and directives

- Personal Data Legislation

5.30. Intellectual property rights

- Best Practice
- Legal requirement

5.30.a. Reason of choice

The company needs to make sure that software used by employees are legally acquired and that employees are well-aware of how to protect intellectual property rights of CSIS and its customers.

5.30.b. Legal requirements and directives

- Personal Data Legislation

5.31. Protection of records

- Best Practice
- Risk evaluated
- Contractual requirement
- Legal requirement

5.31.a. Reason of choice

As a cybersecurity company, the protection of company records are essential.

5.31.b. Legal requirements and directives

- Financial Business Act
- Personal Data Legislation

5.32. Privacy and protection of PII (personally identifiable information)

- Best Practice
- Risk evaluated
- Contractual requirement
- Legal requirement

5.32.a. Reason of choice

As a company that operates in the EU and UK, compliance with privacy and data protection regulations is essential.

5.32.b. Legal requirements and directives

- Personal Data Legislation

5.33. Independent review of information security

- Best Practice
- Legal requirement

5.33.a. Reason of choice

CSIS introduces independent internal audits for business continuity, and make sure that the company standards are up to date with CSIS' information security objectives, and changed where necessary.

5.33.b. Legal requirements and directives

- Financial Business Act

5.34. Compliance with policies, rules and standards for information security

- Best Practice
- Risk evaluated

5.34.a. Reason of choice

CSIS aims to make sure that employees and systems are compliant with policies, regulations and standards.

5.35. Documented operating procedures

- Best Practice
- Risk evaluated

5.35.a. Reason of choice

Governance of information security controls and other company procedures needs to be effective and clear.

6. Screening

- Risk evaluated
- Best Practice
- Contractual requirement

6.1.a. Reason of choice

Employees handle confidential and sensitive information and hence have to be suitable for the job. Moreover, some customer contracts require us to have repeated verification checks on personnel with a critical role.

6.2. Terms and conditions of employment

- Best Practice
- Risk evaluated
- Contractual requirement

6.2.a. Reason of choice

To avoid data breach and unlawful use of company data and assets.

6.3. Information security awareness, education and training

- Best Practice
- Risk evaluated

6.3.a. Reason of choice

Employees should be up to date about information security policies and procedures since they are handling sensitive data.

6.4. Disciplinary process

- Best Practice
- Risk evaluated

6.4.a. Reason of choice

Because of handling protected and sensitive data, all parties should be aware of the importance and consequences of violation.

6.5. Responsibilities after termination or change of employment

- Risk evaluated

6.5.a. Reason of choice

This is a control that assists CSIS to protect against data breach and unlawful use of company and client information.

6.6. Confidentiality or non-disclosure agreements

- Best Practice
- Risk evaluated
- Contractual requirement

6.6.a. Reason of choice

To make sure that CSIS' NDA is up to date and clear about confidential information handled by the company.

6.7. Remote working

- Best Practice
- Risk evaluated

6.7.a. Reason of choice

Essential for everyday operations within CSIS, since employees are allowed to work remotely.

6.8. Information security event reporting

- Best Practice
- Risk evaluated

6.8.a. Reason of choice

Roles should be assigned and personnel should be able to easily report to IT Operations to minimize the incident effect.

7. Physical security perimeters

- Best Practice
- Risk evaluated

7.1.a. Reason of choice

Because CSIS has an office where company assets are stored, the physical access should be controlled.

7.2. Physical entry

- Best Practice
- Risk evaluated

7.2.a. Reason of choice

Access to CSIS office and other premises should be restricted and visitors should be signed in and out.

7.3. Securing offices, rooms and facilities

- Best Practice
- Risk evaluated

7.3.a. Reason of choice

Access to CSIS office and other premises should be controlled and public persons should be signed in and out.

7.4. Physical security monitoring

- Best Practice
- Risk evaluated

7.4.a. Reason of choice

CSIS aim to monitor access to the office to ensure physical security.

7.5. Protecting against physical and environmental threats

- Best Practice

7.5.a. Reason of choice

CSIS would like to ensure physical security for employees and the information and assets handles and owned by the company.

7.6. Working in secure areas

- Best Practice
- Risk evaluated

7.6.a. Reason of choice

CSIS needs to ensure that it operates in a secure way for client satisfaction and protection. This includes secure office and training of personnel about how to maintain it.

7.7. Clear desk and clear screen

- Best Practice
- Risk evaluated

7.7.a. Reason of choice

Since employees handle confidential and sensitive information, the company has to make sure that data breech does not happen through physical access.

7.8. Equipment siting and protection

- Best Practice
- Risk evaluated

7.8.a. Reason of choice

Since CSIS has information and physical assets, there should be a protection mechanism.

7.9. Security of assets off-premises

- Risk evaluated
- Best Practice

7.9.a. Reason of choice

Since CSIS has consultants and other third-parties temporary employees, the asset and information security should apply to them as well.

7.10. Storage media

- Best Practice
- Risk evaluated

7.10.a. Reason of choice

Since CSIS has hard copy documents and other physical assets, the management of these is essential to avoid unauthorized access.

7.11. Supporting utilities

- Best Practice
- Risk evaluated

7.11.a. Reason of choice

Since CSIS offers 24/7 services, electricity and other supporting utilities should be backed up.

7.12. Cabling security

- Best Practice

7.12.a. Reason of choice

Since CSIS uses cabling in it physical environment, the security of such is important for business availability and operations.

7.13. Equipment maintenance

- Best Practice
- Risk evaluated

7.13.a. Reason of choice

Overall equipment maintenance is necessary for continuous, effective and secure operations within CSIS.

7.14. Secure disposal or re-use of equipment

- Best Practice
- Risk evaluated

7.14.a. Reason of choice

Since CSIS provides company computers and phones, these should be securely disposed and re-used to avoid unauthorized access.

8. User endpoint devices

- Best Practice
- Risk evaluated

8.1.a. Reason of choice

Since remote working is allowed for CSIS employees, the protection of information available through user endpoint devices such as company laptops is essential for CSIS.

8.2. Privileged access rights

- Best Practice
- Risk evaluated

8.2.a. Reason of choice

Since the company handles confidential and sensitive information, access to these should be governed and managed to avoid unauthorized access.

8.3. Information access restriction

- Best Practice
- Risk evaluated

8.3.a. Reason of choice

Access to confidential information and other assets has to be controlled to avoid data breech and loss.

8.4. Access to source code

- Best Practice
- Contractual requirement

8.4.a. Reason of choice

Least Access Privilege is the principle for every system, including access to source code.

8.5. Secure authentication

- Best Practice
- Contractual requirement

8.5.a. Reason of choice

Access control to Github is performed by SSO/MFA and conditional access policies in Azure.

8.6. Capacity management

- Best Practice
- Risk evaluated

8.6.a. Reason of choice

Cost control, data control, best business practice.

8.7. Protection against malware

- Best Practice
- Contractual requirement

8.7.a. Reason of choice

As a cybersecurity company we cannot imagine NOT having such protection. We have Microsoft defender on every company enrolled device.

8.8. Management of technical vulnerabilities

- Best Practice
- Risk evaluated
- Contractual requirement

8.8.a. Reason of choice

We have several systems scanning our environment for vulnerabilities - Tenable, Darktrace, Sentinel.

8.8.b. Configuration management

- Best Practice
- Risk evaluated

8.8.c. Reason of choice

Configuration of key systems is well documented and information reviewed regularly. Best business practice and nature of our company dictates that we maintain that vigorously.

8.9. Information deletion

- Legal requirement
- Best Practice
- Contractual requirement

8.9.a. Reason of choice

As a company operating in the EU we are obliged to delete data that is no longer used. Sometimes contractual regulations dictate that we even do so in a stricter nature

8.9.b. Legal requirements and directives

- Freedom of Information Act
- Personal Data Legislation

8.10. Data masking

- Best Practice
- Risk evaluated
- Contractual requirement
- Legal requirement

8.10.a. Reason of choice

Data masking is essential to control information and asset access. It can also be part of a contractual obligation towards customers and legislations can be applied for safe data storing and handling.

8.10.b. Legal requirements and directives

- Freedom of Information Act
- Personal Data Legislation

8.11. Data leakage prevention

- Best Practice
- Risk evaluated
- Contractual requirement
- Legal requirement

8.11.a. Reason of choice

GDPR and other legislations can be applied. Contractual obligations to protect customer and employee data. Important for company integrity.

8.11.b. Legal requirements and directives

- Freedom of Information Act
- Personal Data Legislation

8.12. Information backup

- Best Practice
- Risk evaluated
- Contractual requirement

8.12.a. Reason of choice

Essential for company integrity and continuous workflow. Possible contractual obligations towards customers to keep up the service we provide.

8.13. Redundancy of information processing facilities

- Best Practice
- Contractual requirement

8.13.a. Reason of choice

Essential for company integrity and continuous operations to provide our services.

8.14. Logging

- Risk evaluated
- Best Practice

8.14.a. Reason of choice

CSIS has to protect against data breach and unauthorized access to information and assets. It is important for company integrity and business continuity.

8.15. Monitoring activities

- Best Practice
- Risk evaluated
- Legal requirement

8.15.a. Reason of choice

It is important for company integrity and business continuity. Moreover, laws and regulations about business and information security are considered.

8.15.b. Legal requirements and directives

- Freedom of Information Act
- Personal Data Legislation

8.16. Clock synchronisation

- Best Practice

8.16.a. Reason of choice

During creation of systems or onboarding so that the time zone is set since CSIS operates in UK and Copenhagen and Romania.

8.17. Use of privileged utility programs

- Best Practice
- Risk evaluated

8.17.a. Reason of choice

Least Access Privilege principle is followed. The access is given based not only on least access privilege but also on time spent in the company and needs.

8.18. Installation of software on operational systems

- Best Practice
- Contractual requirement

8.18.a. Reason of choice

Out of date operating systems are prompt to security threats.

8.19. Networks security

- Best Practice
- Risk evaluated
- Contractual requirement
- Legal requirement

8.19.a. Reason of choice

The company can keep up business integrity and prevent info processing facilities from getting compromised. Possible contractual obligations towards customers and their data. Legislations applicable about information and data security.

8.19.b. Legal requirements and directives

- Freedom of Information Act
- Personal Data Legislation

8.20. Security of network services

- Risk evaluated
- Best Practice

8.20.a. Reason of choice

Needs to be in place to prevent data breech and unauthorized access.

8.21. Segregation in networks

- Best Practice
- Risk evaluated

8.21.a. Reason of choice

Segregation needs to be implemented to prevent internal and external unauthorized information access and for business continuity.

8.22. Web filtering

- Best Practice
- Risk evaluated

8.22.a. Reason of choice

Web filtering is essential for CSIS to maintain internal information security.

8.23. Use of cryptography

- Best Practice
- Risk evaluated
- Contractual requirement
- Legal requirement

8.23.a. Reason of choice

CSIS handles sensitive customer data hence it is essential for contractual obligations towards employees and customers. Also, legal obligations of data and information protection.

8.23.b. Legal requirements and directives

- Freedom of Information Act
- Personal Data Legislation

8.24. Secure development life cycle

- Risk evaluated
- Best Practice

8.24.a. Reason of choice

CSIS develops software, hence it is important to maintain a secure development life cycle.

8.25. Application security requirements

- Best Practice
- Risk evaluated
- Legal requirement

8.25.a. Reason of choice

Our vendors should be compliant with cybersecurity and data protection regulations.

8.25.b. Legal requirements and directives

- Freedom of Information Act
- Personal Data Legislation
- Other legislation

8.25.c. Legal requirements and directives

NIS2

8.26. Secure system architecture and engineering principles

- Best Practice
- Risk evaluated
- Contractual requirement

8.26.a. Reason of choice

CSIS develops software and applications for customer use.

8.27. Secure coding

- Best Practice
- Risk evaluated

8.27.a. Reason of choice

Since CSIS develops software, secure coding is important to reduce potential information security vulnerabilities.

8.28. Security testing in development and acceptance

- Best Practice
- Risk evaluated

8.28.a. Reason of choice

This is necessary for CSIS to validate if information security requirements are met.

8.29. Outsourced development

- Best Practice
- Risk evaluated
- Contractual requirement

8.29.a. Reason of choice

CSIS outsourcing development and hence, this control is essential to maintain information security.

8.30. Separation of development, test and production environments

- Best Practice
- Risk evaluated

8.30.a. Reason of choice

It is important at CSIS to protect data from compromise, development and test activities should be separated to non-production and production sites.

8.31. Change management

- Best Practice

8.31.a. Reason of choice

Because CSIS can change systems, the accurate implementation of the new systems is crucial for secure operations.

8.32. Test information

- Best Practice
- Risk evaluated
- Contractual requirement

8.32.a. Reason of choice

During internal audits, test information has to be protected and carefully chosen through the internal audit schedule applied by CSIS. It is also contractual because some customers do not want CSIS to use their data.

8.33. Protection of information systems during audit testing

- Best Practice
- Risk evaluated

8.33.a. Reason of choice

CSIS needs to ensure business continuity during internal audit tests and ensure that all parties are well informed about the procedure.