Universitatea Tehnică a Moldovei

Facultatea Calculatoare Informatică şi Microelectronică

Departamentul Ingineria Software și Automatică

**RAPORT**

Lucrarea de laborator nr. 4

# La disciplina „Managementul și Auditul Securitații Informaționale”

Tema: “Evaluarea conformității sistemului de securitate informațională cu recomandările ISO 27001 si GDPR . Domeniile ISO 27002”

A efectuat: st. gr. SI-211 S. Chirița

A verificat: E. Nemerenco

Chișinău – 2024

## Find out your level of compliance with ISO 27001

Introducere:

În domeniul Managementului Securității Informațiilor, respectarea standardelor recunoscute este esențială pentru a asigura confidențialitatea, integritatea și disponibilitatea informațiilor sensibile. Organizația Internațională pentru Standardizare (ISO) a dezvoltat standardul ISO/IEC 27001, care oferă un cadru pentru stabilirea, implementarea, menținerea și îmbunătățirea continuă a unui Sistem de Management al Securității Informațiilor (SMSI).

Acest set de întrebări servește ca un instrument de evaluare pentru a evalua conformitatea unei organizații cu standardul ISO/IEC 27001. Fiecare întrebare este concepută pentru a investiga aspecte specifice ale practicilor de securitate a informațiilor ale organizației, acoperind domenii precum contextul organizațional, angajamentul conducerii, gestionarea riscurilor, evaluarea performanței și îmbunătățirea continuă.

Răspunsurile la aceste întrebări, care pot fi date cu "Da" sau "Nu", oferă perspective asupra nivelului de pregătire al organizației, respectarea politicilor și procedurilor stabilite și eficacitatea generală a măsurilor sale de securitate a informațiilor.

Prin analizarea sistematică a fiecărei întrebări și a răspunsului său corespunzător, părțile interesate pot obține o înțelegere cuprinzătoare a maturității SMSI-ului organizației și pot identifica domenii pentru îmbunătățiri sau remedieri. Acest proces de evaluare ajută la consolidarea posturii de securitate a informațiilor a organizației, la atenuarea riscurilor și la promovarea unei culturi a îmbunătățirii continue în protejarea activelor de informații sensibile.

Să explorăm procesul de evaluare prin analizarea fiecărei întrebări și a considerațiilor asociate în evaluarea conformității cu ISO/IEC 27001.

### REPORT ON ISO 27001 COMPLIANCE ASSESSMENT

#### 4.0 CONTEXT OF THE ORGANIZATION

##### 4.1 UNDERSTANDING THE ORGANIZATION AND ITS CONTEXT

1. Did the organization determine the purpose(s) of the ISMS?
   * Yes
2. Did the organization determine the internal and external issues that are relevant to the ISMS purpose?
   * Yes
3. Did the organization determine how internal and external issues could influence the ISMS ability to achieve its intended outcomes?
   * Yes

#### 4.2 UNDERSTANDING THE NEEDS AND EXPECTATIONS OF INTERESTED PARTIES

1. Did the organization determine interested parties?
   * Yes
2. Does the list of all of interested parties’ requirements exist?
   * Yes

##### 4.3 DETERMINING THE SCOPE OF THE INFORMATION SECURITY MANAGEMENT SYSTEM

1. Is the scope documented with clearly defined boundaries and applicability?
   * Yes

#### 4.4 INFORMATION SECURITY MANAGEMENT SYSTEM

1. Have you established, documented, implemented, maintained, and continually improved an information security management system, including needed processes and interactions, per ISO 27001 requirements?
   * Yes

### 5.0 LEADERSHIP

#### 5.1 LEADERSHIP AND COMMITMENT

1. Are the general ISMS objectives compatible with the strategic direction?
   * Yes
2. Does management ensure the necessary ISMS resources are available as needed?
   * Yes
3. Does management ensure that ISMS achieves its intended outcomes?
   * Yes

#### 5.2 POLICY

1. Does an Information Security Policy exist with included objectives or a framework for setting objectives?
   * Yes
2. Is the Information Security Policy documented and communicated within the company and to other interested parties?
   * No

#### 5.3 ORGANIZATIONAL ROLES, RESPONSIBILITIES AND AUTHORITIES

1. Are roles, responsibilities, and authorities for information security assigned and communicated?
   * Yes

### 6.0 PLANNING

#### 6.1 ACTIONS TO ADDRESS RISKS AND OPPORTUNITIES

1. Are internal and external issues, as well as interested parties' requirements, considered while addressing risks and opportunities?
   * Yes
2. Is there a documented process to identify information security risks, including the risk acceptance criteria and criteria for risk assessment?
   * Yes
3. Is the risk treatment process documented, including the risk treatment options and how to create a Statement of Applicability?
   * Yes

#### 6.2 INFORMATION SECURITY OBJECTIVES AND PLANNING TO ACHIEVE THEM

1. Are information security objectives and targets established at relevant functions of the organization, measured and monitored where practical, and consistent with the information security policy?
   * Yes
2. Is there a plan, or group of plans, in place to achieve the information security objectives and targets including designated responsibility, evaluation method, and the means & timeframe for the plan(s)?
   * Yes

#### 6.3 PLANNING OF CHANGES

1. Are changes in the ISMS done in a planned manner?
   * Yes

### 7.0 SUPPORT

#### 7.1 RESOURCES

1. Are adequate resources provided for all the elements of the ISMS?
   * Yes

#### 7.2 COMPETENCE

1. Is appropriate competence assessed, and training provided where needed, for personnel doing tasks that can affect the information security? Are records of competences maintained?
   * Yes

#### 7.3 AWARENESS

1. Is the personnel aware of the Information Security Policy, of their role, and consequences of not complying with the rules?
   * Yes

#### 7.4 COMMUNICATION

1. Are there identified needs for communication related to information security, including the responsibilities and what to communicate, to whom and when?
   * Yes

#### 7.5 DOCUMENTED INFORMATION

1. Does the documentation of the ISMS include the Information Security Policy, objectives & targets, the scope of the ISMS, the main elements and their interaction, documents and records of ISO 27001 and those identified by the company?
   * Yes
2. Is it ensured that managing of documents and records exists, including who reviews and approves documents, and where and how they are published, stored, and protected?
   * Yes
3. Is documented information of external origin controlled?
   * No

8.0 OPERATION

#### 8.1 OPERATIONAL PLANNING AND CONTROL

1. Does the organization have established criteria for processes, and has it implemented controls over them according to these criteria?
   * Yes
2. Does the organization have the necessary documented information to be confident that its processes are being carried out as planned?
   * Yes
3. Are planned changes controlled? Are consequences of unplanned changes reviewed to identify mitigation actions if necessary?
   * Yes
4. Are outsourced processes identified and controlled?
   * Yes

#### 8.2 INFORMATION SECURITY RISK ASSESSMENT

1. Are the risks, their owners, likelihood, consequences, and the level of risk identified? Are these results documented?
   * Yes

#### 8.3 INFORMATION RISK TREATMENT

1. Does a risk treatment plan exist, approved by risk owners?
   * Yes
2. Is there a documented list with all controls deemed as necessary, with proper justification and implementation status?
   * Yes

### 9.0 PERFORMANCE EVALUATION

#### 9.1 MONITORING, MEASUREMENT, ANALYSIS AND EVALUATION

1. Is it defined what needs to be measured, by which method, who is responsible, who will analyze and evaluate the results?
   * Yes
2. Are the results of measurement documented, analyzed, and evaluated by responsible persons?
   * Yes

#### 9.2 INTERNAL AUDIT

1. Does an audit program exist that defines the timing, responsibilities, reporting, audit criteria, and scope?
   * Yes
2. Are internal audits performed according to an audit program, results reported through an internal audit report, and relevant corrective actions raised?
   * Yes

#### 9.3 MANAGEMENT REVIEW

1. Is management review regularly performed, and are the results documented in minutes of the meeting?
   * Yes
2. Did management decide on all the crucial issues important for the success of the ISMS?
   * Yes

### 10.0 IMPROVEMENT

#### 10.1 CONTINUAL IMPROVEMENT

1. Is the ISMS continuously adjusted to maintain its suitability, adequacy, and effectiveness?
   * Yes

#### 10.2 NONCONFORMITY AND CORRECTIVE ACTION

1. Does the organization react to every nonconformity?
   * Yes
2. Does the organization consider eliminating the cause of the nonconformity and, where appropriate, take corrective action?
   * Yes
3. Are all nonconformities recorded, together with corrective actions?
   * Yes

### REQUIREMENTS READINESS:

### ANNEX A. (Note: only the controls marked as applicable in the Statement of Applicability must be implemented.)

#### A.5 ORGANIZATIONAL CONTROLS

1. Are there published policies, approved by management, reviewed, and updated to support information security?
   * Yes
2. Are all information security responsibilities defined?
   * Yes
3. Are duties and responsibilities properly segregated considering situations of conflict of interest?
   * Yes
4. Is management actively requiring all employees and contractors to comply with information security rules?
   * Yes
5. Are contacts with relevant authorities defined?
   * Yes
6. Are contacts with special interest groups or professional associations defined?
   * Yes
7. Is information related to information security threats collected and analyzed to produce threat intelligence?
   * Yes
8. Do projects consider information security aspects?
   * Yes
9. Does an Inventory of Assets exist, and does every asset in the inventory have a designated owner?
   * Yes
10. Are rules and procedures for handling of information and other associated assets defined?
    * Yes
11. Are company assets returned by employees and contractors when their employment is terminated?
    * Yes
12. Are criteria to classify information defined?
    * Yes
13. Are there procedures which define how to label and handle classified information?
    * Yes
14. Is the information transfer properly protected?
    * Yes
15. Is there an Access Control Policy, and do users have access only to the resources they are allowed to use?
    * Yes
16. Are access rights provided via a formal registration process?
    * Yes
17. Are there rules for passwords and other secret authentication information to be provided in a secure way, as well as for password management systems, and users, on how to manage and protect them?
    * Yes
18. Is there a formal access management process to handle, review, and update access to information systems and users' access rights?
    * Yes
19. Is there a policy on how to treat the risks related to suppliers and partners?
    * Yes
20. Are relevant security requirements included in the agreements with the suppliers and partners?
    * Yes
21. Do the agreements with providers and suppliers include security requirements?
    * Yes
22. Are suppliers regularly monitored, and are changes involving arrangements and contracts with suppliers and partners taking into account risks and existing processes?
    * Yes
23. Are cloud services acquired, used, managed, and canceled according to information security requirements?
    * Yes
24. Are incidents managed properly?
    * Yes
25. Are security events assessed and classified properly?
    * Yes
26. Are procedures on how to respond to incidents documented?
    * Yes
27. Are security incidents analyzed properly?
    * Yes
28. Do procedures exist which define how to collect evidence?
    * Yes
29. Are requirements for continuity of information security defined, implemented, exercised, and tested?
    * Yes
30. Is ICT readiness managed according to business continuity objectives and ICT requirements?
    * Yes
31. Are legislative, regulatory, contractual, and other security requirements listed?
    * Yes
32. Do procedures exist to protect intellectual property rights?
    * Yes
33. Are records protected properly?
    * Yes
34. Is personally identifiable information protected properly?
    * Yes
35. Is information security regularly reviewed by an independent auditor?
    * Yes
36. Do the managers regularly review if the security policies and procedures are performed properly in their areas of responsibility, and that information systems are in compliance with the information security policies and standards?
    * Yes
37. Are operating procedures for IT processes documented?
    * Yes

### A.6 PEOPLES CONTROLS

1. Does the organization perform background checks on candidates for employment or for contractors?
   * Yes
2. Are there agreements with employees and contractors that specify information security responsibilities?
   * Yes
3. Do employees and contractors attend trainings to better perform their security duties, and do the awareness programs exist?
   * Yes
4. Does the organization have a formal disciplinary process?
   * Yes
5. Are there agreements covering information security responsibilities that remain valid after the termination of employment?
   * Yes
6. Does the organization list all the confidentiality clauses that need to be included in agreements with third parties?
   * Yes

### A.8 TECHNOLOGICAL CONTROLS

1. Are rules for the secure handling of mobile devices, and for protecting equipment when not in the physical possession of its users, defined? - Yes
2. Are privileged access rights managed with special care? - Yes
3. Is the access to information in systems restricted according to the access control policy? - Yes
4. Is the access to source code restricted to authorized persons? - Yes
5. Is secure log-on required on systems according to the Access Control Policy? - Yes
6. Are resources monitored and plans made to ensure their capacity to fulfill users' demands? - Yes
7. Are anti-virus software, and other software for malware protection installed and properly used? - Yes
8. Is information about vulnerabilities properly managed, and are information systems regularly reviewed to check their compliance with the information security policies and standards? - Yes
9. Are configurations of relevant IT assets properly handled? - Yes
10. Is data that is no longer required properly disposed of? - Yes
11. Is data masking applied according to applicable requirements? - Yes
12. Do systems, networks, and devices include data leakage prevention measures? - Yes
13. Is a backup policy defined and performed properly? - Yes
14. Does IT infrastructure have redundancy (e.g.: secondary location) included in its planning and operation? - Yes
15. Are relevant events from IT systems logged periodically, and are logs protected properly? - Yes
16. Are systems, networks, and applications monitored, and proper actions taken when anomalous behaviors are found? - Yes
17. Are clocks on all IT systems synchronized? - Yes
18. Is the use of utility tools controlled and limited to specific employees? - Yes
19. Is installation of software strictly controlled? - Yes
20. Are the networks controlled to protect information in systems and applications? - Yes
21. Are security requirements for network services defined, and included in agreements? - Yes
22. Are the networks segregated considering risks and assets classification? - Yes
23. Is access to external websites controlled? - Yes
24. Does a policy to regulate encryption and other cryptographic controls exist? - Yes
25. Are rules for the secure development of software and systems defined? - Yes
26. Is application information, including transaction information, transferred through public networks appropriately protected? - Yes
27. Are principles for engineering secure systems applied to the organization system's development process? - Yes
28. Is software code developed according to defined principles? - No
29. Is the implementation of security requirements tested during system development, and are the criteria for accepting the systems defined? - Yes
30. Is the outsourced development of systems monitored? - Yes
31. Are development, testing, and production environments separated and properly secured? - Yes
32. Are changes that could affect the information security of new or existing systems properly controlled and tested? - Yes
33. Are test data carefully selected and protected? - Yes
34. Are audits of production systems planned and executed properly? - Yes

**Analiza Conformității cu Regulamentul General de Protecție a Datelor (GDPR)**

Scopul acestui raport este de a evalua în ce măsură organizația respectă prevederile Regulamentului General de Protecție a Datelor (GDPR) în ceea ce privește prelucrarea datelor cu caracter personal. GDPR reprezintă un cadru legislativ crucial pentru protejarea vieții private a indivizilor și pentru asigurarea unei prelucrări corecte și transparente a datelor cu caracter personal.

Întrebările și răspunsurile asociate vor oferi o imagine de ansamblu asupra modului în care organizația gestionează datele cu caracter personal, respectând drepturile subiecților datelor și aplicând principiile de bază ale GDPR. Acestea includ aspecte precum documentarea bazelor legale pentru prelucrare, asigurarea consimțământului adecvat al subiecților datelor, furnizarea de notificări privind confidențialitatea, raportarea incidentelor de securitate și evaluarea impactului asupra protecției datelor.

Prin evaluarea acestor aspecte cheie, organizația poate identifica zonele în care trebuie să își îmbunătățească practicile de gestionare a datelor și să se asigure că respectă cerințele GDPR, contribuind astfel la construirea încrederii și respectului în rândul clienților și partenerilor săi.

**PRINCIPLES RELATED TO PROCESSING OF PERSONAL DATA**

1. **Is the legal basis for each processing activity documented?**
   * Response: Yes
2. **Is the purpose for each processing activity documented?**
   * Response: Yes
3. **Will the personal data be processed for a purpose other than what was intended at the time of collection?**
   * Response: Yes
4. **Do consent-collecting mechanisms require some action (e.g., ticking a box) or affirmative statement by the data subject?**
   * Response: Yes
5. **Where processing involving special categories of data is based on consent, is explicit consent obtained from the data subject?**
   * Response: Yes

**RIGHTS OF THE DATA SUBJECTS WHILE PROCESSING AND ACCESSING THEIR INFORMATION**

1. **Is a process in place to respond to requests for access to information held about a data subject?**
   * Response: Yes
2. **Is a process in place to rectify/delete information about a data subject pursuant to a request?**
   * Response: Yes
3. **Is a process in place to communicate updates of personal data to third parties who have received the data?**
   * Response: Yes
4. **Is there a process in place to allow a data subject to revoke consent for a particular processing activity at any time?**
   * Response: Yes
5. **When consent for a particular processing activity is revoked, are there processes in place to ensure processing is stopped, including any processing by third parties?**
   * Response: Yes
6. **Is there a process in place to comply with requests to restrict the processing of data if requested by a data subject, including any processing by third parties?**
   * Response: Yes
7. **Is a process in place to comply with requests from a data subject to have their personal data transferred directly to another controller, if technically possible?**
   * Response: Yes
8. **Is a process in place to stop processing for direct marketing purposes when an objection is received?**
   * Response: Yes
9. **If engaged in automated decision making, including profiling, is there a process by which a data subject may request a manual review of the decision or profiling activity?**
   * Response: Yes
10. **Has a representative within the European Union been designated?**
    * Response: Yes

**TRANSFERS OF DATA TO THIRD PARTIES**

1. **Do contracts with third parties specify that the third party, and any subcontractor that may be utilised, must have data protection and security protection clauses/annexes in place?**
   * Response: Yes
2. **Are records kept of all processing activities your company engages in?**
   * Response: Yes
3. **Are all data transfers documented, including cross-border transfers?**
   * Response: Yes
4. **Is a data transfer mechanism in place in the event that personal data is to be transferred to a third country or international organisation?**
   * Response: Yes

**PRIVACY NOTICES**

1. **Is a Privacy Notice provided to data subjects no later than at the time information is collected from those data subjects?**
   * Response: Yes
2. **Is a Privacy Notice provided to data subjects at every point of collection?**
   * Response: Yes
3. **If data is to be processed for a secondary purpose, are data subjects notified of the new purpose prior to processing?**
   * Response: Yes
4. **Does the Privacy Notice clearly specify how data subjects can exercise their rights under the GDPR?**
   * Response: Yes

**DATA BREACHES**

1. **Is a process in place to ensure the appropriate Supervisory Authority is notified within 72 hours of a confirmed data breach?**
   * Response: Yes
2. **Do agreements/contracts with third parties specify that the third party has to notify you (the controller) without undue delay after becoming aware of a data breach or potential data breach involving personal data?**
   * Response: Yes
3. **Are internal policies in place defining what is considered to be a data breach and when and if notification to data subjects or Supervisory Authorities is required?**
   * Response: Yes
4. **Is a log kept of all data breaches that occur, along with the effects and remedial actions taken?**
   * Response: Yes
5. **Are assessments of processing activities conducted by the relevant personnel to determine the data protection measures that should be in place, proportionate to the risks involved with the processing activity?**
   * Response: Yes
6. **Is privacy assessed at the beginning stages of development of any processing activity?**
   * Response: Yes
7. **Are measures such as data minimisation and pseudonymisation implemented across all applicable organisational units?**
   * Response: Yes

**DATA PROTECTION IMPACT ASSESSMENT (DPIA)**

1. **Are Data Protection Impact Assessments (DPIAs) completed for processing activities involving special categories of information, automated decision making, or profiling?**
   * Response: Yes
2. **Are DPIAs completed prior to implementing new technologies, processes, or projects?**
   * Response: Yes

Concluzie: În concluzie, evaluarea conformității organizației noastre cu cerințele GDPR a relevat atât aspecte pozitive, cât și zone care necesită îmbunătățiri. În ansamblu, există un nivel satisfăcător de conștientizare și documentare a practicilor de protecție a datelor. Cu toate acestea, identificarea și implementarea unor procese mai eficiente pentru obținerea consimțământului și gestionarea cererilor subiecților datelor ar putea consolida respectarea normelor GDPR și ar putea contribui la întărirea încrederii clienților în organizație.