Security in Organisations (SIO)

Assignment 3 - 2021-2022

Goals:

- Understanding the requirements that are needed in an organizational information security policy.
- Acquiring hands-on experience by drafting a security policy.

Instructions:

- This assignment must be completed by a team of two students.
- The assignment must be written with the Times New Roman font, in size 12pt, with normal spacing. The subtitles are in bold, and the margins must be all of size 2.5cm.
- The original numbering of the questions must be indicated for each answer.
- State your answers in a succinct and clear manner.

Deadline:

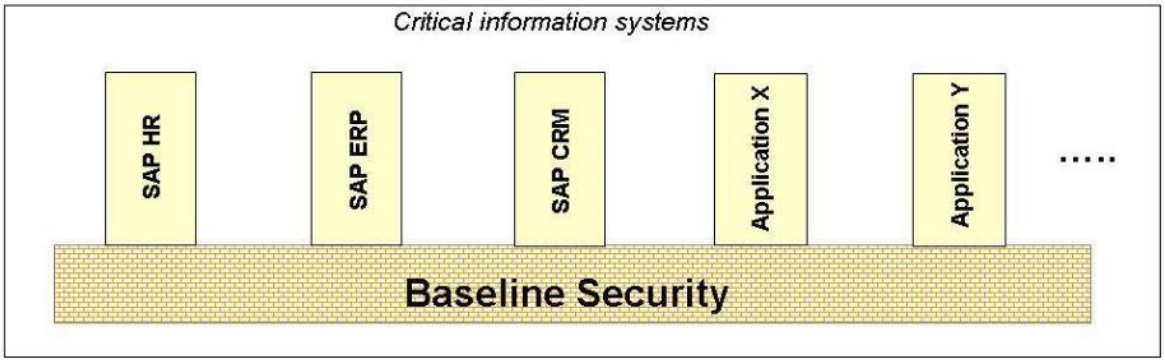
- Submit the assignment in a PDF document through Brightspace before **2021/12/17 23:59.**

If and only if you do not have a Brightspace access, you can submit your assignment by email to Anna Guinet (see SIO website) in a PDF document.

You were recently hired as the Chief Security Officer of the Faculty of Science at Radboud University. Your first task is to draft an information security policy according to the ISO 27001/27002 for the Faculty of Science (and not for the whole Radboud University)[1]. Use the 'combined approach' for this policy which is explained in the lectures, and:

- Compile an information security policy for the Faculty of Science as outlined below and whereby following the instructions/questions. This should result in a fictive information security policy of the Faculty of Science, and not in a list of explicit answers on the questions raised.
- As part of the information security, describe your own role as Chief Security Officer of the Faculty of Science. If you think that additional staff members are needed, like Security Officers, describe their role in the information security policy.

[1] In earlier years, TUE students could write a similar information security policy for the TUE only. However, the relevant information is easier to found for the FNWI than for the TUE which make it difficult to consistently grade the assignment. This is why we ask to write an information security policy for FNWI only.



1. **Introduction**.
   - *Describe the types of 'core business processes' that take place in the Faculty of Science and how there are organized, with an organization chart. Show the difference between core and supporting departments.*
   - *Indicate if the Faculty of Science depends on external parties. And if it does, how?*
2. **Definition of information security**
   - *Provide a definition of information security (e.g., from ISO 27001).*
   - *Relate this definition with the core business processes of the Faculty of Science which you have described in Section 1 ('Introduction').*
3. **Management approval**
   - *Describe the management layers within the Faculty of Science, and make an informed choice of a person or a committee that should approve this policy.*
   - *Describe how, and how often, the policy should be reviewed.*
4. **Security objectives**
   - *From the perspective of information security, what is important for the Faculty of Science?*
   - *Mention some possible threats.*
   - *Mention the relevant regulations, legislation and contracts that you need to adhere to.*
   - *Mention the relations with external parties.*
5. **Scope**
   - *What is the scope of this policy, i.e., what falls under it? Make sure that this scope is absolutely clear, including from a physical perspective.*
6. **Approach**

   Describe the combined approach in a comprehensive manner even for non-experts, e.g. senior management, that explains how:

   a) *the baselines should be developed based on the ISO 27002 (see Appendix I),*
   b) *all information systems should be inventoried,*
   c) *all information systems should be linked to an owner,*
   d) *high level risk assessments (Business Impact Assessment, see Appendix II) are conducted,*
   e) *detailed risk assessments should be conducted on security critical systems (you can refer to ISO27005, without specifying any further),*

f) *baseline and additional controls from risk assessments should be implemented,*
g) *information security should be reviewed,*
h) *management review of information security should be performed.*

7. Organization of information security

- *Relate all the processes a-h you answered in Section 6 ('Approach') to responsibilities that are set below. You have the possibility to add extra roles/ responsibilities.*

7.1 End-responsibility

7.2 (Line) management

7.3 Support departments

7.4 ICT department

7.5 Internal audit department

7.6 Corporate security officer

7.7 Employees

Appendix I - Baselines

Review all the ISO 27002 (2013 version) controls and guidelines and categorize them in two selections:

1. the controls that are not relevant for the Faculty of Science at all, and motivate why, and
2. the controls that are relevant for the Faculty of Science. Describe to which extent the Faculty should implement them, i.e., describe with keywords the parts of these controls that the Faculty of Science should implement as a baseline. This is preferable that you limit yourself to the controls that you understand rather than implementing all of them. In addition, be aware that in practice, organizations do not have the budget to implement all the controls.

Please, use the format below. Be aware that some formulations in the ISO27002 can be unclear, and this is your task to interpret it.

Statement of Applicability and status of information security controls			
#	**Title**	**Selected Y/N**	**Motivation**
A5	Information security policies		
A5.1	Management direction for information security		
A5.1.1	Policies for information security		
A5.1.2	Review of the policies for information security		
A6	Organization of information security		
A6.1	Internal organization		
A6.1.1	Information security roles and responsibilities		
A6.1.2	Segregation of duties		
A6.1.3	Contact with authorities		
A6.1.4	Contact with special interest groups		
A6.1.5	Information security in project management		
…	…		

Appendix II - Business Impact Assessment forms

For each of the confidentiality, integrity and availability aspects, define five questions to be answered by the system owners within the Facility of Science. The aim is to determine whether their systems are security critical for the Facility of Science.

Use the format below, and fill in the yellow parts.

Do not use questions that can be related to vulnerabilities, but rather write questions that can indicate the value of the information for the organization.

Classification of Confidentiality

Business consequences of unintended or unauthorized disclosure of information (worst case)					
Ref	**Question**	**Impact** (circle the right answer)			**Motivation**
C01	How privacy-sensitive is the information?[2]	Public	Basic (membership, subscription related, employee related)	High (medical, financial, sexual inclination)	
C02					
C03					
C04					
C05					
Result (check one of the three boxes)		Low	Medium	High	

Classification of Integrity

Business Consequences of errors in information or of deliberate manipulation of information to perpetrate or conceal fraud (worst case)					
Ref	**Question**	**Impact** (circle the right answer)			**Motivation**
I01					
I02					
I03					

[2] Simplification of ‘Achtergrondstudies en Verkenningen 23’, College Bescherming Persoonsgegevens, 2001.

I04					
I05					
Result (check one of the three boxes)		Low	Medium	High	

Classification of Availability

Business Consequences of a prolonged outage of the system (worst case)					
Ref	**Question**	**Impact** (circle the right answer)			**Motivation**
A01					
A02					
A03					
A04					
A05					
Result (check one of the three boxes)		Low	Medium	High	

CALCULATION OF THE GRADES	
Question	Max. points
A. Introduction	0,5
B. Definition of information security	1
C. Management approval	1,5
D. Security objectives E. Scope	1,5
F. Combined approach G. Responsibilities	1,5
Appendix I: Baselines	1
Appendix II: Business Impact Assessment forms	1,5
Overall impression	0,5
SUM	**9**
Grade = (1 + sum_of_points) rounded to the nearest 0,5 point	