RISK ASSESSMENT

THE RISK ASSESSMENT IS A PART OF THE PPHS CYBERSECURITY STANDARD FOR SMALL AND MEDIUM-SIZED ENTERPRISES AND PUBLIC INSTITUTION DEVELOPED BY THE POLISH PLATFORM FOR HOMELAND SECURITY.

TABLE OF CONTENTS

03

INTRODUCTORY INFORMATION:

- Risk assessment is a fundamental process that allows an organization to ensure the security of its information assets/ resources, at a level appropriate to the existing risk.
- There is no one-size-fits-all, universally accepted methodology for risk assessment. The choice of approach should be based on the specifics of the organization and take into account its characteristics. It is therefore possible to create your own methodology, or to adapt existing ones but it is important to remain consistent when using it. The results of the risk assessment should be comparable over time.
- The risk assessment should be performed on a regular basis in time units designated by appropriate persons in the organization. It should be also conducted after any major change, emergence of a new major threat, or the occurrence of a major incident.
- The risk assessment process should be continuously improved.

04

EXAMPLE METHODOLOGY:

NOTE:

A proposal of a two-stage approach[1].

Stage 1 It aims to increase the efficiency of the entire risk assessment process. It helps to identify priorities. Its application can significantly increase productivity, especially when an organization makes an assessment for the first time. These activities are recommended for SMEs by ENISA[2]. However, the process is not mandatory and can be skipped by going straight to step 2.

Stage 2 is the risk assessment as such[3].

1) The first stage is not described in the PPHS Standard because it is an optional operation.

2) ENISA ad hoc working group on risk assessment and risk management, Risk Assessment and Risk Management Methods: Information Packages for Small and Medium Sized Enterprises (SMEs), 30/03/2006.

3) The Standard uses the term "risk estimation" - the meaning is the same, those expressions are often used interchangeably, but it must be remembered that they will have to be used consistently and the difference between the whole process and the specific action carried out in Phase 2, Phase 3 (Phase 3: Evaluation of the analyzed risk) will have to be noticed.

05

WHAT STEPS SHOULD BE TAKEN TO CREATE A CLASSIFICATION?

STAGE 1

STEP 1
PROCESS IDENTIFICATION

STEP 2
EVALUATION OF PROCESS SIGNIFICANCE

STEP 3
DETERMINATION OF THE CRITICALITY ASSETS/RESOURCES ICT

STEP 4
ESTABLISHING PRIORITIES

STAGE 2

STEP 1
THREATS

STEP 2
RISK ANALYSIS

STEP 3
RISK ASSESSMENT

STEP 4
CHOICE AND IMPLEMENTATION OF THE RISK HANDLING STRATEGY

06

STAGE 1

Step 1 – identification of processes which are implemented in the organization.

The processes which are implemented in the organization should be identified. In practice, this can be done in working groups performing specific tasks in the organization. This step can be closely connected with the inventory of assets / information resources (Stage 1, Task 1 according to the PPHS framework). The identification of processes implemented in the company is closely linked to the assets/processes which already exist in the organization. E.g. email and collected CVs are directly related to the recruitment process which takes place in order to hire employees.

Step 2 – determining the significance of the identified processes.

TYPICAL PROCESSES IMPLEMENTED IN SMALL AND MEDIUM-SIZED COMPANIES:

- **Production:** understood as a process whose implementation serves the production of goods that the organization produces (and sells, offers), or the implementation of a service which it provides to recipients. The core of the organization's functioning.
- **Finance:** all financial operations carried out by the company (withdrawals, transfers for taxes, investments, etc.).
- **Human resources:** all processes related to employees, co-workers.
- **Sales, distribution, marketing:** servicing existing customers, acquiring new ones.

Afterwards, it is necessary to determine how important each process is to the organization in terms of its objectives. In other words, it is necessary to determine how important the processes are to achieve a given task and achieve the objectives.

07

STAGE 1

A three-step scale can be adopted: high, medium, low value. For example:

HIGH VALUE

- The most important processes for the organization, e.g. related to the most important service offered to the client.
- Disruption of these processes may have disastrous consequences for the organization (e.g. as for financial losses or damage to reputation).

MEDIUM VALUE

- Processes that play an important but not critical role for the organization. They are supplementary to its operation.
- Disruptions to these processes will cause problems and difficulties in functioning of the organization on the daily basis.

LOW VALUE

- Processes that are not very relevant to the organization.
- Disruptions to these processes may cause difficulties, but do not lead to serious consequences.

STAGE 1

Step 3 – Determine the criticality level of ICT assets/resources for the organization.

At first, it is necessary to determine how much the implementation of each of the identified processes depends on the proper functioning of individual ICT assets/resources. A three-step scale is proposed to determine the relation:

HIGH DEPENDENCE

- Malfunctioning of ICT assets/resources will severely disrupt or prevent the execution of a given process.

MEDIUM DEPENDENCE

- Malfunctioning of ICT assets/resources will lead to difficulties with the execution of the process. However, this is not a critical disruption.

LOW DEPENDENCE

- Malfunctioning of ICT assets/resources will make the process slightly more difficult.

09

STAGE 1

Criticality level of ICT assets/resources for an organization is determined by comparing the values of previously identified processes with the degree of their dependence on ICT systems.

NOTE

The same tool/system can be used for different processes and have different criticality levels. Ultimately, the highest criticality level should be considered.

TYPE OF PROCESS (e.g. recruitment)

IMPORTANTANCE OF THE PROCESS FOR THE ORGANISATION	DEPENDENCE OF THE PROCESS ON ICT ASSETS/RESOURCES		
	LOW DEPENDENCE	MEDIUM DEPENDENCE	HIGH DEPENDENCE
LOW VALUE	Very low criticality level	Very low criticality level	Low criticality level
MEDIUM VALUE	Very low criticality level	Low criticality level	Medium criticality level
HIGH VALUE	Low criticality level	Medium criticality level	Very high criticality level

Step 4 – Prioritization:

The result of determining the criticality of ICT assets/results for an organization clarifies which processes and ICT tools/systems used to implement them need a thorough risk assessment first. This can be done, for example, according to the methodology proposed below (Stage 2).

STAGE 2

Stage 2 is already the proper risk assessment, carried out in accordance with the chosen methodology (more: Stage 2 of the PPHS Framework). An exemplary methodology[4] can be found below.

The level of risk will result from calculating the product of three elements: probability of a given threat, vulnerability of the examined information asset/ resource and the consequence of the possible threat. Each of these three parameters will be considered in the context of a specific threat which may compromise the security of a specific information asset/resource.

Step 1 – Threats

The threats, which will pose risk, should be identified for a given information asset/resource associated with the analyzed process. It is recommended to create a list of threats, which will be continuously updated (in Annex 1 EXAMPLARY list of threats). Various methods can be used to create it. Analysis of existing sources (reports etc.), brainstorming, consultations with experts, surveys etc.).

It is worth focusing on several of the most important threats and subjecting them to more in-depth analysis. How to choose the key threats? It may be decided by the owner of the assets, it may be a result of the team voting.

4) Modified Procedure of Information Security Risk Assessment, Appendix to the Ordinance of the President of the City of Jastrzębie-Zdrój No. Or.IV.0050.635.2015 of 23 November 2015 on the introduction in the City Hall in Jastrzębie-Zdrój of "Procedure of Information Security Risk Assessment".

11

SELECTED DEFINITIONS

Threat - is any act, event that may negatively affect the information asset / resource needed to implement a given process.

Threats that should be considered when assessing risk are multidimensional and diverse, e.g.

- Environmental threats: flood, storm, earthquakes,
- Organizational threats: no specific procedures,
- Risks related to human error: accidental deletion of files, accidental sending of information to the wrong recipient,
- Risks related to technical error: hard disk failure, software failure, power failure,
- Threats with intentional hostile actions: eg hacker attack resulting in illegal database access, theft of databases.

Threats can be a risk for a resource only if there are the vulnerabilities.

Vulnerability - this is a weakness of the asset/resource that can be used by the threat.
Vulnerabilities may concern all assets/resources: e.g. IT assets (e.g. lack of updates).

STAGE 2

Step 2 – Risk analysis

In the context of any given risk, we analyze three elements: probability, vulnerability, consequences. One shall use the following tables for this analysis.

Examined criterion		Value
(P) Probability (possibility of danger)	**Low** – a threat is unlikely to materialize , similar incidents have occurred in the past in our organization (or in organizations of a similar type) very rarely (e.g. once every decade).	1
	Medium – there is a real chance that the incident will happen. The incident has occurred in our organization (or similar organizations) over the last five years.	2
	High- very real chances that the incident will happen. The incident occurred in our organization (or in organizations of a similar type) last year.	3

STAGE 2

Examined criterion		Value
(V) Vulnerability (vulnerability of the asset/resource)	There are no, or few weaknesses, effective safeguards.	1
	Weaknesses can be found, the safeguards are applied but their effectiveness is medium.	2
	There are many weaknesses, lack of safeguards or they are ineffective.	3

Examined criterion		Value
(C) Consequence (impact on the organization)	**The threat:** - will not obstruct the work of the organization for a long time, - will not damage the reputation (image) of the organization, - it will not bring financial losses.	1
	The threat: **-** will disrupt the operation of the organization, - will have a negative impact on the reputation (image) of the organization, - will bring financial costs, - there may be disciplinary consequences.	2
	The threat: - will cause a long-term downtime. It may even cause damage (to assets/resources), - will have serious negative impact on the reputation (image) of the company, - will result in large financial losses, - will have serious legal consequences.	3

STAGE 2

Then use the following formula:
R = P · V · C

P - Probability
V - Vulnerability
C- Consequence

We substitute the appropriate value measured in points according to the previously performed analysis into the formula.

Step 3 - Risk assessment[5]

We compare the result of the risk level with the scale. We use the table below (it contains the acceptable risk levels previously established in the organization).

The result obtained is the starting point for decisions on actions to be taken in relation to each risk.

5) The term "risk estimation" can be used to distinguish it from the name of the whole process.

STAGE 2

Category Class	Risk Category	Risk Value	Risk Acceptance Yes / No	Preventive actions
1	**Low**	1÷ 7	**YES**	Acceptable risk. It is not necessary to take action, it is recommended to keep the risk at the current level. Improvement measures can be taken.
2	**Medium**	8÷ 17	**NO**	Unacceptable risk. Action should be taken to reduce the level of risk.
3	**High**	18÷ 27	**NO**	Unacceptable risk. It is a priority to take actions which will reduce the risk level.

STAGE 2

Step 4 – Selection and implementation of risk management strategies.

A risk management strategy must be chosen and implemented. For unacceptable risks there are 3 possible decisions:

- Implementation of safeguards which will reduce the risk level (e.g. by eliminating vulnerability, reducing the consequences if the threat occurs),
- Transferring risk to other entities such as an insurer, supplier, business partner,
- Avoiding risk - e.g. not taking actions which may increase the risk level,
- Acceptance (retention)
- Sharing.

STAGE 2

Example – Legal chamber

Business process	Value for the business	Depndance on ICT	Criticality of ICT assests/ resources
Legal advice (Production)	**High value**	Case related database - high dependency	Very high criticality level
		Email - medium dependence	Medium criticality level
		IT infrastructure (hardware, operating system, network) - high dependency	Very high criticality level
		Time tracking application - low dependency	Low criticality level
Marketing	**Low value**	Website - medium dependence	Very low criticality level
		Social media – low dependence	Very low criticality level
Recruitment (Personnel)	**Medium value**	Database of candidates - low dependency	Very low criticality level
		Email – medium dependence	Low criticality level
		Recruitment portal - medium dependence	Low criticality level

NOTICE

As you can see in the example above, the same information asset/resource (e.g. email) can have different criticality levels for different processes. In such a situation the highest identified level should be applied.

STAGE 2

An in-depth risk analysis should be performed, first of all for the database encompassing data related to legal advice.One of the identified risks will be for example: - An attack leading to encryption of the database.
We start the risk analysis and substitute the data into the following formula:
R = P · V · C

P – probability – 2 – - Due to the nature of the organization, the importance of the processed information, and while observing incidents in similar entities, there is a real chance that the event will occur.
The event has occurred in our organization (or in similar organizations) in the last five years.

V – vulnerability - there are few weaknesses (e.g. frequent changes of employees who have access to the database), there are many safeguards - (e.g. regular backups) – 1

C – consequences - lack of access to the database may paralyze the operation of the legal chamber – 3

Result: 2x1x3 = 6 – low risk – acceptable.

ANNEX 1. EXAMPLES[6]:

EXAMPLES OF THREATS

1. Installation of malware through email leading to access to information assets/ resources
2. Installation of malware through email which leading to modification of information assets/ resources
3. Installation of malware through email leading to removal of information assets/ resources
4. Installation of malware through email leading to encryption of information assets/ resources
5. Installation of malware through a Website leading to access to information assets/ resources
6. Installation of malware through a Website leading to modification of information assets/ resources
7. Installation of malware through a Website leading to removal of information assets/ resources
8. Installation of malware through a Website leading to zaszyfrowania aktywów/zasobów informacyjnych
9. Installation of malware through external data carriers leading to access to information assets/ resources
10. Installation of malware through external data carriers leading to modification of information assets/ resources
11. Installation of malware through external data carriers leading to removal of information assets/ resources

6) Based on, among others, TZ-Consultans Tadeusz Zawistowski, “Metodyka oceny ryzyka do przygotowania sprawozdania za rok 2013”; Krzysztof Liderman, “Oszacowania jakościowe ryzyka dla potrzeb bezpieczeństwa teleinformatycznego”, “Biuletyn Instytutu Automatyki i Robotyki NR 19”, 2003; MC, “Metodyka zarządzania ryzykiem cyberprzestrzeni w systemach zarządzania bezpieczeństwem informacji podmiotów rządowych”, Warsaw 2015.

ANNEX 1. EXAMPLES[6]:

EXAMPLES OF THREATS

12. Installation of malware through external data carriers leading to encryption of information assets/ resources
13. Installation of malware in another software leading to access to information assets/ resources
14. Installation of malware in another software leading to modification of information assets/ resources
15. Installation of malware in another software leading to removal of information assets/ resources
16. Installation of malware in another software leading to encryption of information assets/ resources
17. Installation of malware during repair or servicing leading to access to information assets/ resources
18. Installation of malware during repair or servicing leading to modification to information assets/ resources
19. Installation of malware during repair or servicing software leading to removal of information assets/ resources
20. Installation of malware during repair or servicing leading to encryption of information assets/ resources
21. Exploitation of gaps in the systems of mobile devices leading to access to information assets/ resources

ANNEX 1. EXAMPLES[6]:

EXAMPLES OF THREATS

22. Exploitation of gaps in the systems of mobile devices leading to modification to information assets/ resources
23. Exploitation of gaps in the systems of mobile devices leading to removal of information assets/ resources
24. Exploitation of gaps in the systems of mobile devices leading to encryption of information assets/ resources
25. External attack restricting access to information assets/ resources of a DDoS type
26. Takeover of information assets/ resources sent by email
27. Eavesdropping on information assets/ resources transmitted via the radio network
28. Eavesdropping on information assets/ resources transmitted via traditional network
29. Sociotechnical attack to seize information assets/ resources (phishing)
30. Unauthorised physical access to information assets/resources
31. Power cut disabling the use of information assets/ resources
32. Any type of flooding from internal installations disabling the use of information assets/ resources
33. Any type of flooding from internal installations destroying information assets/ resources
34. Fire destroying information assets/ resources
35. Fire disabling the use of information assets/ resources
36. Construction disaster disabling the use of information assets/ resources
37. Construction disaster destroying information assets/ resources

ANNEX 1. EXAMPLES[6]:

EXAMPLES OF THREATS

38. Flood destroying information assets/ resources
39. Flood disabling the use of information assets/ resources
40. Overheating of the equipment disabling the use of information assets/ resources
41. Equipment failure preventing the use of information assets/ resources
42. Inefficient equipment (too slow, not complying with software requirements) preventing the use of information assets/ resources
43. Internet connection instability preventing the use of information assets/ resources
44. Insufficient Internet bandwidth hindering the use of information assets/resources
45. Theft of information assets/liabilities from the premises of the company
46. Losing information assets/ resources
47. Suspicion of information assets/resources at the company's headquarters
48. Peek at information assets/resources at the company's headquarters
49. Authorized users' errors - failure to record information assets/ resources
50. Authorized user's error - deletion of information assets/ resources
51. Authorized user's error – sending information by email to an unauthorized person
52. Deliberate action of authorized users – destruction of information assets/ resources
53. Deliberate action of authorized users – sale of information assets/ resources

ANNEX 1. EXAMPLES[6]:

54. Deliberate action of authorized users – sabotage of information assets/ resources
55. Deliberate action of authorized users – misuse of powers
56. Deliberate action – destruction of information assets/ resources
57. Terrorist attack
58. Use of corruption and blackmail to extract certain information from chosen company employees
59. Infiltration into the environment by finding people who consider themselves disadvantaged by their employer, fired or seeking employment in another organization.
60. Lack of access to information assets/resources due to absence of eligible persons.

EXAMPLES OF VULNERABILITIES

1. Lack of user awareness of risks (threats, vulnerabilities, consequences)
2. Lack of knowledge of safety rules and procedur es
3. Too rarely changed passwords
4. Too weak passwords
5. Too often changed passwords
6. User's non-compliance with safety rules and procedur es
7. Incorrect management of users' permissions - granting of excessive permissions
8. Incorrect management of user permissions - no revocation or very delayed revocation of permissions
9. Eligible user - administrator's mistake - wrong configuration giving excessive permissions
10. Incorrectly configured, including open ports
11. Incorrectly configured operating systems
12. No protection of communication protocols

ANNEX 1. EXAMPLES[6]:

EXAMPLES OF VULNERABILITIES

13. Use of unlicensed software
14. Unreliable control of recorded system events
15. Use of private information resources
16. Lack or incorrect location in the system, or lack of AV software updates
17. Missing, misplaced in network topology or wrong firewall configuration
18. Missing, misplaced in the network topology or incorrect configuration of IPS/IDS software and its sensors
19. Incorrect configuration of security mechanisms in WAN networks
20. No server load monitoring
21. Vulnerability of users to social engineering methods used to obtain information or enter malicious code
22. Incorrect configuration of LAN security mechanisms
23. No network traffic supervision (QoS)
24. Lack of supervision over user's permissions, permissions inadequate to tasks
25. No control over physical access to system components
26. Lack of encryption in WAN connections
27. No system software update

ANNEX 1. EXAMPLES[6]:

MORE INFORMATION ON RISK ASSESSMENT:

- ENISA ad hoc working group on risk assessment and risk management, Risk Assessment and Risk Management Methods: Information Packages for Small and Medium Sized Enterprises (SMEs), 30/03/2006.
- Modified Procedure of Information Security Risk Assessment, Appendix to the Ordinance of the President of the City of Jastrzębie-Zdrój No. Or.IV.0050.635.2015 of 23 November 2015 on the introduction in the City Hall in Jastrzębie-Zdrój of "Procedure of Information Security Risk Assessment".
- TZ-Consultans Tadeusz Zawistowski, Metodyka oceny ryzyka do przygotowania sprawozdania za rok 2013;
- Krzysztof Liderman, Oszacowania jakościowe ryzyka dla potrzeb bezpieczeństwa teleinformatycznego, Biuletyn Instytutu Automatyki i Robotyki NR 19, 2003;
- MC, Metodyka zarządzania ryzykiem cyberprzestrzeni w systemach zarządzania bezpieczeństwem informacji podmiotów rządowych, Warszawa 2015.

POLISH PLATFORM
FOR HOMELAND SECURITY

Polish Platform for Homeland Security

ul. Slowackiego 17/11
60-822 Poznań
www.ppbw.pl/en
tel.: +48 (61) 663 02 21
e-mail: standard-cyber@ppbw.pl

European Funds Smart Growth

Republic of Poland

European Union
European Regional Development Fund

The project "Cybersecurity – PPHS Standard for SME and public institutions" was financed by the European Regional Development Fund.