PROCESS-BASED APPROACH TO CYBERSECURITY

THE PROCESS-BASED APPROACH TO CYBERSECURITY 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

1. INTRODUCTORY INFORMATION 03

2. THE IMPLEMENTATION OF THE CYBERSECURITY STANDARD 04

3. EXAMPLE OF A SCHEDULE TEMPLATE 05

4. SELECTED PROCESSES OF ORGANIZATION 06
   - **4.1** Procedure for ensuring the human resources security 06
   - **4.2** Procedure regarding the development of security policies 06

5. SELECTED PROCESSES REGARIDNG PHYSICAL SECURITY 07
   - **5.1** Procedures for establishing safe areas 07
   - **5.2** Procedures for ensuring the physical security of equipment. 07

6. SELECTED PROCESSES REGARDING TECHNICAL SAFETY 08
   - **6.1** Procedures for creating backups 08
   - **6.2** Procedure of log file analysis 08
   - **6.3** Incident management procedure 09

03

INTRODUCTORY INFORMATION

- The implementation of the cybersecurity standard as well as, broadly, the holistic approach to cybersecurity management must be treated as a process.

- This means that ensuring certain resources (competences, tools, skills) used to achieve the desired objectives and coordinating activities of the partners will require planned decisions[1].

- A simplified scheme of the process-based approach to implementation of the standard can be found below. It is only a proposal of the approach. Each time, the choice of actions should be adjusted to the characteristics of the entity and resources at its disposal.

- Obviously, the implementation of the standard is only the beginning. It is to create a framework for planning and implementation of organizational, technical and other activities aimed at providing cybersecurity.

- An example of a process-based approach to implementing the standard themselves is presented below. Next, the selected (not all!) examples of both organizational and technical processes which should be implemented in the organization are indicated.

1) cf. Bogdanienko J. (2010) "Organizacja i zarządzanie w zarysie", Wydawnictwo Naukowe Wydziału Zarządzania Uniwersytetu Warszawskiego, Warsaw, p. 16-17.

IMPLEMENTATION OF THE CYBERSECURITY STANDARD

STARTING THE IMPLEMENTATION OF THE STANDARD

PLANNING THE WHOLE PROCESS

STAGE 1 OF THE PPHS STANDARD

STEP 1: Designation of a person responsible for supervising the implementation of the overall process of Information Asset Management (IAM) - IAM process executive.

STEP 2: Defining roles and responsibilities for individual actions:

Task 1: Identification of information assets
(e.g. each department, team, employee - list the assets (groups of assets) with use of which they perform their job - supervision of the IAM process executive)

Task 2: Identification and assignment of each asset for the owner
(IAM process executive in agreement with the above mentioned employees determines the owners of particular asset groups - decisions are accepted by the board of management)

Task 3: Determination of requirements for asset protection
(the owner is responsible for determining the legal and other requirements related to the protection of his or her assets)

Task 4: Determination of the value of assets and their classification.
(process executive IAM prepares classifications of information assets - approval from the management. Then, the owners of the assets are required to mark the assets according to the classification).

Task 5: Identification of the currently used safeguards.
(asset owners identify the safeguards used for their assets)

Task 6: Determination of acceptable risk level
(board of management determines and acknowledges an acceptable risk level)

Task 7: Registration of all collected information.
(asset owners, under the supervision of the IAM process executive complete the register).

STAGE 2 OF THE PPHS STANDARD – Risk management

STEP 1: Designation of a person responsible for supervising the implementation of the overall process of Risk Management (RM) - RM process executive.

STEP 2: Defining roles and responsibilities for individual actions:

Phase 1: Risk identification

Task 1: Identification of the risks, which may have a negative impact on the security of information assets.
(this action can be performed e.g. by the owners of the assets in cooperation with working groups e.g. composed of people from relevant departments with relevant functions - under the supervision of the RM process executive)

Task 2: Identification of vulnerability to risk.
(this action should be performed e.g. by the owners of the assets - under the supervision of the RM process executive - the results of Stage 1, task 5 should be taken into account.)

Phase 2: Risk analysis

Task 1: Potential effect assessment of the identified risks
(this action should be performed e.g. by the owners of the assets - under the supervision of the RM process executive according to the adopted methodology)

Task 2: Probability assessment of threat occurrence.
(this action should be performed e.g. by the owners of the assets - under the supervision of the RM process executive according to the adopted methodology)

Phase 3: Evaluation of the analyzed risk

Task 1: Comparison of risk analysis results with predefined acceptable risk levels.
(task performed by the RM process executive - under the supervision of the management according to the adopted methodology).

Phase 4: Choice of risk management method and its implementation.

Task 1: Choice of risk management method and its announcement.
(this action should be performed by the supervision of the RM process executive - under the supervision of the management)

STAGE 3 OF THE PPHS STANDARD - Security selection and implementation

STEP 1: RM process executive selects the action in the context of the results of the risk assessment. The board of management accepts the choice of actions.

STEP 2: RM process executive together with the asset owners selects specific collaterals and determines the responsibility for their implementations (if it is decided to use collateral).

STAGE 4 OF THE PPHS STANDARD - Security testing, monitoring, audit, continuous improvement

STEP 1: RM process executive together with the owners of the assets monitor regularly the functioning of the tasks and analyze possible improvements.

The board of management supervises the activities and acepts the key directions.

EXAMPLE OF A SCHEDULE TEMPLATE

TIMETABLE FOR THE IMPLEMENTATION OF THE PPHS CYBERSECURITY STANDARD														
			2019											
NO.	TASK	RESPONSIBLE PERSON	I	II	III	IV	V	VI	VII	VIII	IX	X	XI	XII
1	Establishing a schedule, budget for the implementation of the standard	Board Chairman	✓											
2	Designation of IAM process executive	Board Chairman		✓										
3														
4														
5														
6														
7														
8														
9														
10														

06

SELECTED PROCESSES OF ORGANIZATION

PROCEDURE FOR ENSURING THE HUMAN RESOURCES SECURITY[2]

1. Preparation of the examination of candidates.
2. Agreement on terms and conditions of employment, safety and liability rules.
3. Granting access permissions in accordance with the function, responsibilities of an employee.
4. Awareness-raising activities, training and workshops
5. Supervision over the activities undertaken by the employee in connection with the termination of employment.
6. Return of assets.
7. Revocation of access permissions.

PROCEDURE REGARDING THE DEVELOPMENT OF SECURITY POLICIES[3]

1. Creation of a security policy document.
2. Approval of the policy by the management.
3. Establishing the owner of the policy and the rules related to its review and improvement.
4. Announcement of the policymaking to all stakeholders.
5. Implementation of the policy.
6. Policy review and improvement.

2) More ISO 27001
3) Ibid.

07

SELECTED PROCESSES REGARIDNG PHYSICAL SECURITY

PROCEDURES FOR ESTABLISHING SAFE AREAS[4]

1. Establishment of safe areas.
2. Implementation of physical protection in areas, rooms, etc.
3. Implementation of protection mechanisms against external and environmental phenomena.
4. Establishment and announcement of the principles regarding work in safe areas.
5. Ensuring the security of publicly accessible areas, delivery and loading areas.

PROCEDURES FOR ENSURING THE PHYSICAL SECURITY OF EQUIPMENT[5]

1. Establishment of rules for the safe placement of equipment.
2. Providing support systems.
3. Ensuring the safety of cabling.
4. Establishement of rules for safe disposal or reuse of equipment.

4) Ibid.
5) Ibid.

08

SELECTED PROCESSES REGARDING TECHNICAL SAFETY

PROCEDURES FOR CREATING BACKUPS[6]

1. Determining the scope: that is, the assets to be backed up
2. Establishing the schedule, frequency and specific situations in which backups are made
3. Backing up
4. Storage of backups
5. Recovery testing
6. Recovery of data and IT systems from the backups (according to predetermined rules).

PROCEDURE OF LOG FILE ANALYSIS[7]

1. Determining the scope
2. Configuring the log management system, configuration of each client included in the system.
3. Collecting log files
4. Standardisation of collected data
5. Indexing
6. Storage
7. Correlation
8. Creation of a reference level
9. Alarms
10. Reports

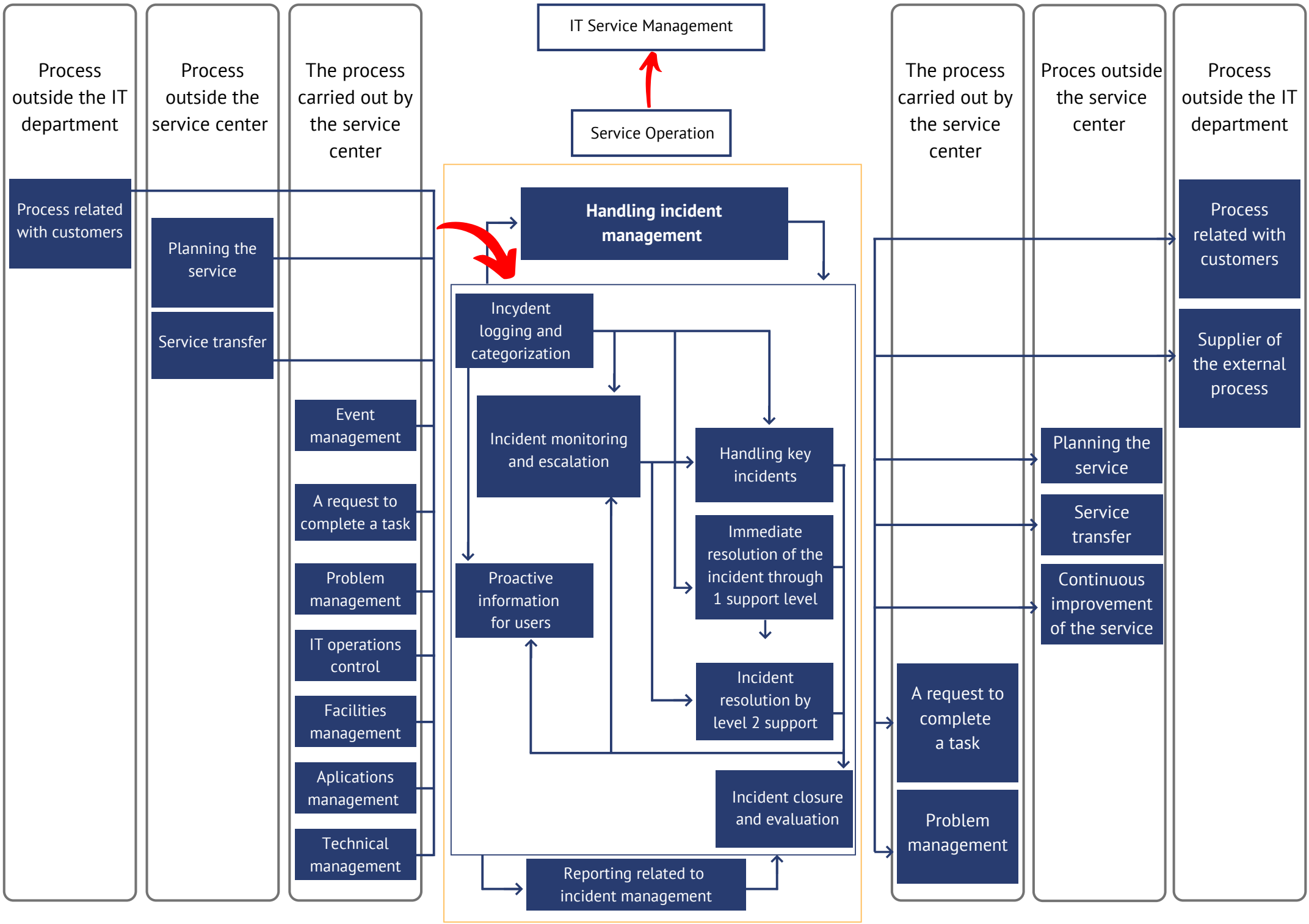
6) Por. Backup procedures. Annex 2, Information Security Policy Świętokrzyskie Voivodship Office.
7) https://www.computerworld.pl/news/Analiza-logow-potencjal-do-wykorzystania,382493,5.html

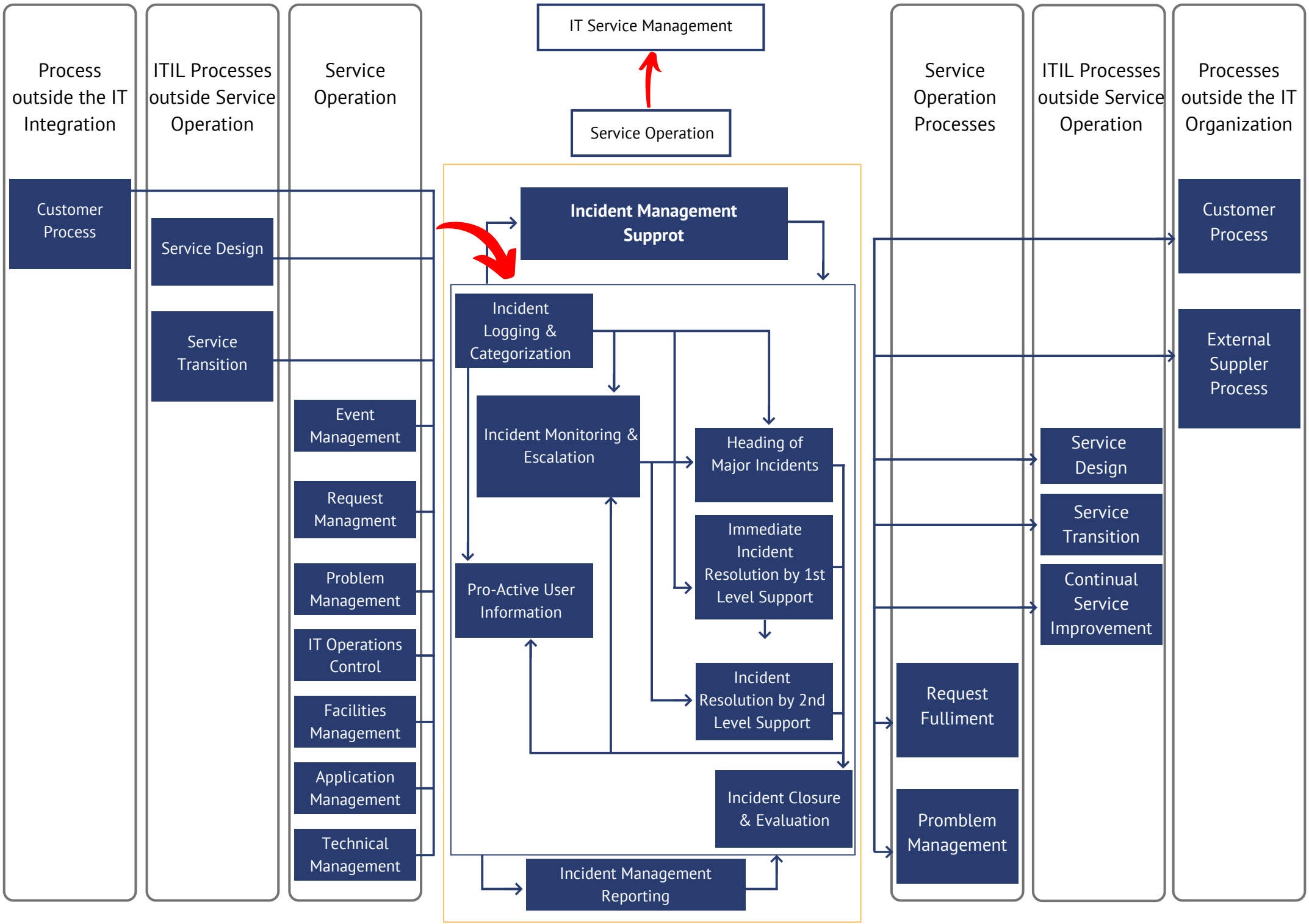
09

SELECTED PROCESSES REGARDING TECHNICAL SAFETY

INCIDENT MANAGEMENT PROCEDURE

The incident management procedure is described in the ITIL methodology. You can find its original version below.


Process outside the IT department
Process outside the service center
The process carried out by the service center
IT Service Management
Service Operation
The process carried out by the service center
Proces outside the service center
Process outside the IT department
Process related with customers
Planning the service
Service transfer
Handling incident management
Incydent logging and categorization
Incident monitoring and escalation
Handling key incidents
Proactive information for users
Immediate resolution of the incident through 1 support level
Incident resolution by level 2 support
Incident closure and evaluation
Reporting related to incident management
Event management
A request to complete a task
Problem management
IT operations control
Facilities management
Aplications management
Technical management
A request to complete a task
Problem management
Planning the service
Service transfer
Continuous improvement of the service
Process related with customers
Supplier of the external process


Process outside the IT Integration
ITIL Processes outside Service Operation
Service Operation
IT Service Management
Service Operation
Service Operation Processes
ITIL Processes outside Service Operation
Processes outside the IT Organization
Customer Process
Service Design
Service Transition
Event Management
Request Managment
Problem Management
IT Operations Control
Facilities Management
Application Management
Technical Management
Incident Management Supprot
Incident Logging & Categorization
Incident Monitoring & Escalation
Heading of Major Incidents
Immediate Incident Resolution by 1st Level Support
Pro-Active User Information
Incident Resolution by 2nd Level Support
Incident Closure & Evaluation
Incident Management Reporting
Request Fulliment
Promblem Management
Service Design
Service Transition
Continual Service Improvement
Customer Process
External Suppler Process

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.