1. PURPOSE

The purpose of this procedure is to guide the identification and classification of assets by the owner in order to determine the appropriate levels of protection and to pursue the necessary work accordingly.

2. SCOPE

This procedure applies to all assets.

3. DEFINITIONS

3.1. **Asset:** It is defined by the owners of the processes included in the Management System that have value for the organization and its value for the organization is determined.

3.2. **Information:** Any asset that has value to the company and therefore needs to be protected in accordance with business requirements.

3.3. **Confidentiality:** It is the property of information to be accessible only to persons, entities or processes that have been authorized to access it.

3.4. **Integrity:** It is the property of preserving the accuracy and completeness of assets.

3.5. **Availability:** It is the ability of authorized users to access information and related resources when needed.

3.6. **Risk:** Events that may lead to disruption of the confidentiality, integrity or usability of information assets. In order to be able to talk about risk, the confidentiality, integrity, usability of the assets in the asset inventory should be damaged, the presence of a threat (external factor) and a vulnerability (openness) that can be used while damaging the asset.

3.7. **Risk Impact:** It is the damage to the organization by the loss of confidentiality, integrity or usability of the asset. The risk effect is a numerical value between 1 and 4 determined by the Asset and Risk assessment table.

3.8. **Risk Management:** It is the prediction of risk, its measurement and reducing it to an acceptable risk level with the determined control options.

3.9. **Threat:** External factors that can prevent the information entity from working.

3.10. **Vulnerability:** Elements that increase the exposure of the information asset to threats and increase the likelihood of the threat being effective.

3.11. **Risk Appetite:** It is the acceptable risk level determined by the senior management.

3.12. **Risk Map:** It is the display of the risk profile and, accordingly, the processes on the basis of their impact and vulnerabilities.

3.13. **Acceptable Risk:** Risks that fall below the risk appetite.

3.14. **Measure:** Actions taken in relation to operational effectiveness, efficiency, compliance with legislation and management policies.

4. RESPONSIBILITY

It is the responsibility of the Senior Management to ensure that this document is up-to-date, and its implementation is the responsibility of all asset owners. It is the asset owners who are primarily responsible for identifying risks and appropriate control options, and incorporating significant changes in threats into the risk map. It is the responsibility of the Quality unit to keep a record of the risks determined as a result of the risk assessment process. The Senior Management is responsible for choosing the appropriate controls that will reduce the risks to an acceptable risk level, supporting the asset owners in the implementation of these controls, keeping the risks of the assets up-to-date and ensuring that the risks are reduced to an acceptable level by risk management.

5. APPLICATION

5.1. Risk analysis

Business owners determine what potential threats might be by considering the main vulnerabilities on the asset. In order to manage risks effectively, risks should be evaluated with a standard method throughout the organization. For this purpose, the following steps are followed;

- Identifying threats affecting quality
- Identifying vulnerabilities
- Identification of the risk resulting from the vulnerability
- Rating of Risk

5.1.1. Identification of Threats, Vulnerabilities and Risks

A threat is the potential for any source to intentionally or accidentally harm assets by exploiting a vulnerability in an asset or another that affects the asset. A source of threat can be defined as events and situations that are likely to damage assets. Threat sources are listed below;

Natural threats : Threats such as earthquakes, floods, landslides, lightning strikes, storms.
Environmental threats: Prolonged power outages, leaks, etc.
Man-made threats: conscious or unconscious events made or caused by humans. For example, incorrect data entry, network attacks, installation of malware, unauthorized access, etc.

5.1.2. Rating of Risk

5.1.2.1. Determination of Risk Probability

By evaluating the past and current situation by the employer, the probability of realization of the risk is determined by the scales in the table below.

Level	Description	Probability Probability
5	Continually	Once a week
4	Very stylish	Once in a month
3	Rare	Once a year
2nd	unlikely	every 1-5 years
one	Very rare	>every 5 years

5.1.2.2. Identification of Risk Impact

For each asset component, the questions specified in the table for confidentiality, integrity and usability are asked in the calculation table and the relevant field corresponding to the appropriate scale according to the degree of importance is marked. The table will automatically assign the highest value as risk impact for each of the confidentiality, integrity, and availability components. The highest value that appears here is the "Risk Effect" of that asset. If the specified risk materializes, the impact it will have on the confidentiality, integrity and availability of the asset is recorded in the file.

Determination of Risk Level and Prioritization

Revision Nature:	
APPROVED	
General manager	

Risk is expressed as a combination of impact and probability.
Value of Risk = (Highest value out of confidentiality, integrity, availability) X Impact X Probability

Risk Appetite has been determined by the senior management to include those with a risk score below ten points.

Possibility	Business Impact				
		1 Very low	2 Low	3 Middle	4 High school
	5 - Continuous Once a week	5	10	15	20
	4 - Very Often Once in a month	4	8	12	16
	3 - infrequent Once a year	3	6	9	12
	2 - Low Chance Every 1-5 Years	2	4	6	8
	1 - Very Rare > Every 5 Years	1	2	3	4

5.2. Risk management

The parts marked in red in the risk assessment table describe the risk appetite limit determined by the senior management. The risk appetite limit is the level at which the senior management defines the necessity of taking precautions for risk.

After the risk assessment is completed, the resulting table is evaluated by the owner, user and custodian of the relevant asset. Actions (control options) are defined for risks that remain above the risk appetite limit.

Action alternatives that can be taken against all the risks mentioned are listed below.

Risk Avoidance: It is the elimination of risk by abandoning the implementation of the activity/project/work step that may cause the risk.

Reducing the Probability and/or Impact of the Risk: It is the action planning to reduce the impact or probability of occurrence of the risk. Actions such as establishing a new control mechanism, redefining roles and responsibilities, renewing contracts, planning training, and implementing a new system can be planned to reduce the probability/effect of the risk.

Transfer of Risk: Risk can be transferred by insuring the asset or by transferring the risky operation to the contractor.

Accepting the Risk: It is the state of not taking action against the risk, unless it is necessary to take any action against the risk or if there is no additional action. On the other hand, if the cost of action to be taken to eliminate the risk is higher than the loss to be caused by the risk, the 'Risk Acceptance' option should be considered. Risk acceptance is only evaluated for risks below the risk appetite limit.

Residual risk: The risk associated with the event that remains after controls have been applied to reduce the impact and probability of the event.

Revision Nature:	
APPROVED	
General manager	

5.3. Assignment of Control Items

The control items that will reduce the probability of the foreseen risks and their impact on the business are determined by the asset owners. The owner of the asset determines the cost, probability of occurrence of risk and effect by considering the defined control items and conveys it to the Quality unit. The quality unit allows the General Manager and Assistant General Manager to select the controls to be applied in any meeting environment or via e-mail. If the decisions taken are in the meeting environment, the meeting minutes are kept by the Quality unit, if they are in the e-mail environment, the e-mail records are kept. On the third page of the "Asset Inventory Pool" file, the controls are listed under the name of "Control Options", the planned end date of these controls and the action owners. If the actions determined for the control options are more than one, they can be followed with a different file, but the relevant file link must be specified in the control actions field.

The follow-up and coordination of the determined action plan is provided by the quality unit. The quality unit shares the action plan with the managers of the relevant units, monitors the realization of the actions and updates the last level of risk in the follow-up list.
The status of risks is evaluated annually by the Quality unit.