Information systems security:

Risk assessment

## 

## Process: Internet banking (e-banking)

E-banking is the process that allows bank customers to conduct money transactions, apply for a loan, and use other services that the bank offers.

In addition to the functionality the e-banking service provides today, security is among the most critical components.

The e-banking process under consideration in the framework of this exercise includes the activities of the uses of e-banking. The process starts with logging users into the e-banking system and conducting various activities on the e-banking system until the user is logged off.

What follows are:

diagram of the process as shown in Figure 1: e-banking process diagram,

a description of the activities carried out in the process as shown in Table 1: e-banking description of activities, and

list of resources required to execute a business process as shown in Table 2: an e-banking resource list.

**E-banking process diagram:**



Figure 1: e-banking process diagram

**Activities Description:**

|  |  |
| --- | --- |
| **Activity** | **Description** |
| **Connecting to the web application** | The user connects to the e-banking application via the Internet browser. |
| **User login/authorisation** | User authorisation is done using a smart card or token. |
| **Request to conduct a transaction** | Through the web application, the user enters a request for conducting a transaction (inquiry into the account balance, payment to the account, etc.). |
| **Transaction Authorization** | The user must authorise certain activities (e.g., payment, contracting loans or savings). |
| **Conducting a transaction** | The required transaction is carried out. |
| **Users log off** | After completing work with the web application, the user logs out of the application for e-banking. |

Table 1: e-banking description of activities

**Resources list:**

|  |  |  |
| --- | --- | --- |
| **Category** | **Resource Name** | **Description** |
| **Hardware** | Web server | A server on which a web server and web application for e-banking are running. |
| **Hardware** | Production Application Server | A server on which the application server and banking application are running. |
| **Hardware** | Application Test Server | A test application server on which a test application server and a test banking application are running. |
| **Hardware** | Production DB Server | Database server. |
| **Hardware** | Test DB Server | Test database server. |
| **Hardware** | Authorisation server | A server where services are run that allows users to be authorised to an e-banking application. |
| **Software** | Web application | Web application of e-banking. |
| **Software** | Web server | The web server on which the e-banking application is running. |
| **Software** | Application Server | Application server on which the banking application is running. |
| **Software** | Interface to the banking application | An application that represents an interface to a banking application and forms a layer between e-banking (front-office) and banking application (back-office). |
| **Software** | Banking application | Banking application includes EUR and foreign currency payment transactions, credit operations, deposit operations, general ledger, etc. (application is current as of 1st of January 2023.) |
| **Software** | Database | A database in which all the data used by the banking application is stored. |
| **Software** | Operating system | The operating system is installed on all of the above physical servers. |
| **Information** | Information in the database | All information used by the banking applications is stored in the database. |
| **Information** | Authorisation information | Information that allows user authorisation using smart cards or tokens (e.g. LDAP directory, digital certificates, etc.). |
| **Services** | Internet | Service is necessary for the operation of the web application for e-banking. |
| **Services** | Local area network | It includes all network equipment that allows these servers to interconnect (routers, switches, etc.). |
| **Business partners** | External partner for development and maintenance | External partner responsible for developing and maintaining banking applications, interfaces to banking applications and web applications for e-banking. |
| **Business partners** | Internet Access Provider (ISP) | An ISP that provides internet access service. |
| **Human Resources** | Hardware Maintenance Employees | Employees responsible for maintaining physical servers. |
| **Human Resources** | Software Maintenance Employees | Employees responsible for software maintenance (operating systems, web servers, application servers, databases) |
| **Human Resources** | Network equipment maintenance employees | Employees responsible for providing Internet and intranet services. |

Table 2: an e-banking resource list

**Network schematics:**

Figure 2: e-banking network schematics show the appearance of the part of the network system used as a basis for the risk assessment.



Figure 2: e-banking network schematics

Figure 3: e-banking network schema with the application list shows how applications are distributed across servers, i.e., on which physical servers individual applications are installed.



Figure 3: e-banking network schema with the application list

## Security controls

|  |  |
| --- | --- |
| **Security controls** | **Server room/building/environment** |
| **Alarm/anti-theft system** | No, but there are cameras and NFC card-protected doors. |
| **Antistatic floor covering** | Yes |
| **Recording entries and exits to the system room** | Yes |
| **Flood detector** | No |
| **Diesel generators for electricity generation** | Yes |
| **Electronically monitored access control system** | yes - entry cards |
| **Lightning rod** | Yes |
| **Identifying marks for employees, external partners and visitors** | No, it's just a piece of paper assigned at the reception desk. |
| **Implementation of an adequate air conditioning system for the hall system** | Yes |
| **Use of FTP/STP cables in places of amplified EM radiation** | Yes |
| **Use of cables for rodent protection** | Yes |
| **Use of handheld fire extinguishers** | Yes |
| **Using a system for uninterrupted power supply** | Yes |
| **Supervision of a business facility outside working hours with a specialised security service** | Yes |
| **Surveillance video cameras** | Yes |
| **Mandatory locking when leaving the premises** | Yes |
| **Mandatory locking of rooms in which information equipment is located** | Yes |
| **Obligatory accompanying visitors from/to the entrance/exit** | No |
| **Separating the space for delivery/dispatch of goods from business premises** | No |
| **Disable network sockets that are not in use** | Yes |
| **Site protection against damage caused by floods, fire, earthquake and other natural disasters** | No |
| **Lighting an object at night** | Yes |
| **Periodic conduct of firefighting exercises** | No |
| **Evacuation plan in case of natural disasters** | Yes |
| **Proper grounding of rooms with information equipment** | Yes |
| **Access granted only to authorised persons** | Only those with an NFC card. |
| **Procedures for working in the system room** | Yes |
| **Fire doors in sensitive safety zones** | No |
| **Anti-theft/fire doors** | No |
| **Workrooms and offices aligned with the requirements of the Occupational Safety Act.** | Yes |
| **Regular monitoring and maintenance of electrical, plumbing and gas installations** | Yes |
| **Regular cleaning and maintenance of rooms where information equipment is located** | partially |
| **Regular maintenance and testing of diesel engines** | Yes |
| **Regular maintenance of the system for uninterrupted power supply** | Yes |
| **Manually record entries and exits at the reception** | Yes |
| **Placement of sensitive rooms on the upper floors of the building** | No |
| **Fire detection and extinguishing system** | Yes |
| **Elevated temperature and humidity detection system** | No |
| **Removal and prohibition of the introduction of flammable objects** | Yes - but it's not prescribed |
| **Arranged connecting cables and panels (marking cables and connectors) in communication cabinets** | partially |
| **Arranged connecting cables and sockets by workplace** | Yes |
| **Visual signage at the top of the building/office building** | No |
| **Ban on entering photo/video cameras and mobile devices** | No |
| **Protection of communication and electrical lines from direct physical contact (channels, elevated floors, etc.)** | Yes |
| **Protecting windows on lower floors using bars** | No |
| **The protective fence around the business facility** | No |

Table 3: Security controls

|  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- |
| **Security Controls - Servers** | **Web server** | **Production App Server** | **App Test Server** | **Production DB Server** | **Test DB Server** |
| **Hardware** |  |  |  |  |  |
| **Adequate placement of equipment in communication /server cabinets** | Yes | Yes | Yes | Yes | Yes |
| **Manufacturer/supplier warranty** | Yes | Yes | Yes | Yes | Yes |
| **Mandatory locking of communication/server cabinets** | No | No | No | No | No |
| **Equipment insurance against theft** | No | No | No | No | No |
| **Possession of a replacement/redundant device (offline)** | No | No | No | No | No |
| **Having a configuration with redundant hot-swap components** | No | No | Yes | No | Yes |
| **Replacement/redundant device in failover mode (online)** | No | No | No | No | No |
| **Procedure for regular maintenance of equipment by the specifications and recommendations of the manufacturer** | No | No | No | No | No |
| **System for monitoring the work and monitoring of the state of information resources (Health monitoring)** | No | No | No | No | No |
| **Equipment maintenance contract with manufacturer/supplier** | Yes | Yes | Yes | Yes | Yes |
| **Software** |  |  |  |  |  |
| **802.1x authentication** | Yes | Yes | Yes | Yes | Yes |
| **Certificate authentication** | No | No | No | No | No |
| **Password authentication** | Yes | Yes | Yes | Yes | Yes |
| **Automated installation of security patches** | No | No | No | No | No |
| **Manual installation of security patches** | Yes | Yes | Yes | Yes | Yes |
| **Application level logs** | Yes | Yes | Yes | Yes | Yes |
| **Recording log records of operating systems and network services** | Yes | Yes | Yes | Yes | Yes |
| **Record access records to source libraries** | No | No | No | No | No |
| **Multi-factor authentication** | No | No | No | No | No |
| **Physical separation of development, test and production systems** | No | No | No | No | No |
| **Installed and updated antivirus protection on server computers** | No | No | No | No | No |
| **Installed and updated EDR protection on server computers** | No | No | No | No | No |
| **Unique username for each system user** | Yes | Yes | Yes | Yes | Yes |
| **Control access to source code/source code libraries** |  |  |  |  |  |
| **Use of NTP services** | Yes | Yes | Yes | Yes | Yes |
| **Using a secure channel to distribute initial passwords to users** | Yes | Yes | Yes | Yes | Yes |
| **Use of TLS protection to protect communication protocols** | Yes | Yes | Yes | Yes | Yes |
| **Using a firewall to separate the Internet from the internal network and publicly available services (DMZ)** | Yes | Yes | Yes | Yes | Yes |
| **Logical separation of development, test and production systems (virtual servers)** | No | No | No | No | No |
| **Monitoring administrator activities using specialised software tools** | No | No | No | No | No |
| **Mandatory change of predefined passwords after initial system installation** | Yes | Yes | Yes | Yes | Yes |
| **Disable access to compilers, editors, and other development tools from production servers** | No | No | No | No | No |
| **Periodic audit of user accounts and associated privileges** | No | No | No | No | No |
| **Set date/time and configured time synchronisation** | Yes | Yes | Yes | Yes | Yes |
| **Password usage policy** | No | No | No | No | No |
| **Procedure for granting administrator privileges** | No | No | No | No | No |
| **Procedure for granting access rights to information services and applications** | Yes | Yes | Yes | Yes | Yes |
| **Procedure for switching from development and test to production environment** | Yes | Yes | Yes | Yes | Yes |
| **The process of managing the installation of security patches** | No | No | No | No | No |
| **Change Management Process** | No | No | No | No | No |
| **Process for granting access rights to an information system** | No | No | No | No | No |
| **Forwarding log records to a remote/centralised server** | No | No | No | No | No |
| **Revision of security settings** | No | No | No | No | No |
| **Secure storage of administrator user accounts and passwords** | Yes | Yes | Yes | Yes | Yes |
| **Security strengthening of operating systems/network services/applications (hardening)** | No | No | No | No | No |
| **SSH access (telnet access ban)** | No | No | No | No | No |
| **Single sign-on authentication** | No | No | No | No | No |
| **Unauthorised activity detection/prevention system (IDS/IPS)** | No | No | No | No | No |
| **Additional controls** |  |  |  |  |  |
| **File system integrity check system** | No | No | No | No | No |
| **Identity and Access Management system (IAM)** | Yes | Yes | Yes | Yes | Yes |
| **Security Event and Information Management System (SIEM)** | Yes | Yes | Yes | Yes | Yes |
| **Prohibit the use of administrator privileges to perform day-to-day business activities.** | No | No | No | No | No |
| **Ban on programmers from production systems** | No | No | No | No | No |
| **Ban developers from accessing test systems** | No | No | No | No | No |

Table 4: Security controls per specific server

**Instructions**

Based on the following tables, information from the previous pages and data from the last exercise, identify the required information and make a risk assessment!

**Note:** The tables that follow are something one can adapt to their needs. Categories can be different, there may be more or less of them, and the description of categories, i.e. their meaning, can be adapted to the needs of the person/company using them.

|  |  |  |
| --- | --- | --- |
| **Resource value** | **Numerical value** | **Description** |
| **VL (Very Low)** | 1 | The resource value is up to 100 EUR |
| **L (Low)** | 2 | The resource value is between 100 and 1000 EUR |
| **M (Medium)** | 3 | The resource value is between 1000 and 10 000 EUR |
| **H (High)** | 4 | The resource value is between 10 000 do 100 000 EUR |
| **VH (Very high)** | 5 | The resource value is above 100 000 EUR |

Table 5: Resource values

|  |  |  |
| --- | --- | --- |
| **Impact** | **Numerical value** | **Description** |
| **L (Low)** | 1 | The impact is less than 100 EUR |
| **M (Medium)** | 2 | The impact is between 100 and 1000 EUR |
| **H (High)** | 3 | The impact is above 10 000 EUR |

Table 6: Impact

|  |  |  |
| --- | --- | --- |
| **Probability** | **Value** | **Description** |
| **L (Low)** | 1 | It is expected for the threat/event to happen once a year. |
| **M (Medium)** | 2 | It is expected for the threat/event to happen once a month. |
| **H (High)** | 3 | It is expected for the threat/event to happen once a week. |

Table 7: Probability

## Task

Based on the above information, answer the following questions:

1. Choose three threats you can identify as possible threats based on the information in this document (what is missing, want can be a risk, etc.). For example, you could use the threats identified in the STRIDE model exercise if the controls related to these threats are missing in the above tables.

Threats:\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_

1. Identify resources (from the resources table) on which these threats apply \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_
2. Identify at least three controls (from the controls table) that can mitigate or remove the selected threat impact. \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_
3. Identify the risk source (the “guilty” party) for these threats (e.g. hardware, software, HR, ...)

\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_

1. Can you identify additional control that could mitigate the identified threats, not in the controls table already?

\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_

1. Categorize the resource values and impact if compromised (by using the Resource value and Impact tables). Assign the value between 1-5 for value and 1-3 for impact.

|  |  |  |
| --- | --- | --- |
| **Resource** | **Value** | **Impact** |
|  |  |  |
|  |  |  |
|  |  |  |
|  |  |  |
|  |  |  |

Table 8: Resource value and impact

1. Assign the value to the threats (probability).

Make sure which controls already exist and whether some of these controls already mitigate the risk!

|  |  |
| --- | --- |
| **Threat** | **Probability** |
|  |  |
|  |  |
|  |  |

Table 9: Threat and probability

1. Based on the information collected, assess the risk for the three identified threats using qualitative method based on the table below:

|  |  |  |  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- |
| **Threat** | **Probability** | **1** | | | **2** | | | **3** | | |
|  | **Impact** | **1** | **2** | **3** | **1** | **2** | **3** | **1** | **2** | **3** |
|  | **1** | 1 | 2 | 3 | 2 | 4 | 6 | 3 | 6 | 9 |
| **Resource value** | **2** | 2 | 4 | 6 | 4 | 8 | 12 | 6 | 12 | 18 |
|  | **3** | 3 | 6 | 9 | 6 | 12 | 18 | 9 | 18 | 27 |
|  | **4** | 4 | 8 | 12 | 8 | 16 | **24** | 12 | 24 | 36 |
|  | **5** | 5 | 10 | 15 | 10 | 20 | 30 | 15 | 30 | 45 |

Table 10: qualitative risk assessment table

### Example:

Example for the threat xyz with the following parameters:

**probability 2**

**impact 3**

**resource value 4**

Threat xyz has a value of **24**. One can calculate this by multiplying probability, impact and resource value or by looking at the above table.

\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_

1. Explain how to mitigate the impact of identified threats (mitigation/modification)

\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_

1. Explain how to treat the identified risks:

Acceptance/Retention, Mitigation/Modification, Transfer/Sharing, Avoidance, If you are unsure what to use, start the in-class discussion.

\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_