**THE FEDERAL STATE AUTONOMOUS EDUCATIONAL INSTITUTION OF HIGHER EDUCATION**
**«SAINT-PETERSBURG NATIONAL RESEARCH UNIVERSITY**
**OF INFORMATION TECHNOLOGIES, MECHANICS AND OPTICS»**

**Faculty of secure information technologies**

# COURSEWORK (PROJECT)

**on course:**
**«Information Security Risk Management»**
**topic of the coursework:**
**«Information Security risk assessment, implementation and control»**

**Written by:**
Author Louise Namugayi _____
(full name) (signature)

**Assessed by:**
Livshitz Ilya, PhD _____
(full name, position) (signature)

Completed with the grade: _____
*(one from above: Excellent, Good, Satisfactory, Unsatisfactory)*

St. Petersburg, 2025

**SAINT-PETERSBURG NATIONAL RESEARCH UNIVERSITY OF INFORMATION TECHNOLOGIES, MECHANICS AND OPTICS**

## OBJECTIVES FOR A COURSEWORK (PROJECT)

**Student** Louise Namugayi
(Full name)

**Faculty of** SIT

**Group** N4156c

**Program/Major** Information Security

**Supervisor** Livshitz Ilya, ITMO University, PhD
(Full name, place of employment, position, academic title, degree)

Course name Information Security Risk Management

Topic of the coursework Information Security risk assessment, implementation and control

Task Controls select of risk identification and assessment methods and their implementation

Guidelines for coursework Lecture material for Information Security Risk Management course

Content of the coursework (list of key issues) Assets identification and assessment, Vulnerabilities identification and assessment, Threats identification and assessment, Risks and residual risks identification and assessment

Source materials and publications ISO 27001, ISO 27005, ISO 13335, ISO 31000, ISO 22301

Supervisor Livshitz Ilya
signature, date

Student Louise Namugayi
signature, date

**SAINT-PETERSBURG NATIONAL RESEARCH UNIVERSITY**
**OF INFORMATION TECHNOLOGIES, MECHANICS AND OPTICS**

## SCHEDULE FOR A COURSEWORK (PROJECT)

**Student** Louise Namugayi
(Full name)
**Faculty of** SIT
**Group** N4156c
**Program/Major** Information Security
**Supervisor** Livshitz Ilya, ITMO University, PhD
(Full name, place of employment, position, academic title, degree)
Course name Information Security Risk Management

Topic of the coursework Information Security risk assessment, implementation and control

**SCHEDULE**

| Stage # | Stage title | Completion date | | Grade and supervisor signature (five-point scale) |
|---|---|---|---|---|
| | | Planned | Actual | |
| 1 | Assets identification and assessment | *19/02/2025* | *20/03/2025* | |
| 2 | Vulnerabilities identification and assessment | *27/02/2025* | *24/03/2025* | |
| 3 | Threats identification and assessment | *6/03/20205* | *27/03/2025* | |
| 4 | Risks and residual risks identification and assessment | *13/03/2025* | *02/04/2025* | |

Supervisor Livshitz Ilya
signature, date
Student Louise Namugayi
signature, date

**SAINT-PETERSBURG NATIONAL RESEARCH UNIVERSITY OF INFORMATION TECHNOLOGIES, MECHANICS AND OPTICS**

## ABSTRACT FOR A COURSEWORK (PROJECT)

**Student** Louise Namugayi
(Full name)

**Faculty of** SIT

**Group** N4156c

**Program/Major** Information Security

**Supervisor** Livshitz Ilya, ITMO University, PhD
(Full name, place of employment, position, academic title, degree)

Course name Information Security Risk Management

Topic of the coursework Information Security risk assessment, implementation and control

## CHARACTERISTICS OF A COURSEWORK (PROJECT)

**1. Purpose and tasks**

☒ Offered by student ☒ Formulated with the participation of the student
☐ Determined by supervisor

**2. Character of work**

☒ Calculation ☐ Design
☐ Simulation ☐ Other, _____

**4. Content of the coursework**

Assets identification and assessment, Vulnerabilities identification and assessment, Threats identification and assessment, Risks and residual risks identification and assessment

**5. Summary of results/conclusions**

The identification and risk assessment was carried out. Recommendations were made for top Management for the protection of IT security.

Supervisor Livshitz Ilya
signature

Student Louise Namugayi
signature

«_2_» __April_____2025 г.

## INTRODUCTION

The goal of coursework: Controls select of risk identification and assessment methods and their implementation.
The tasks of course work:

a) Identify and assess assets;
b) Identify and assess vulnerabilities;
c) Identify and assess assets threats;
d) Identify and assess assets risks and residual risks;
e) Make recommendations for top management for the protection of IT security.

Let's assume Crystal Bank Company.

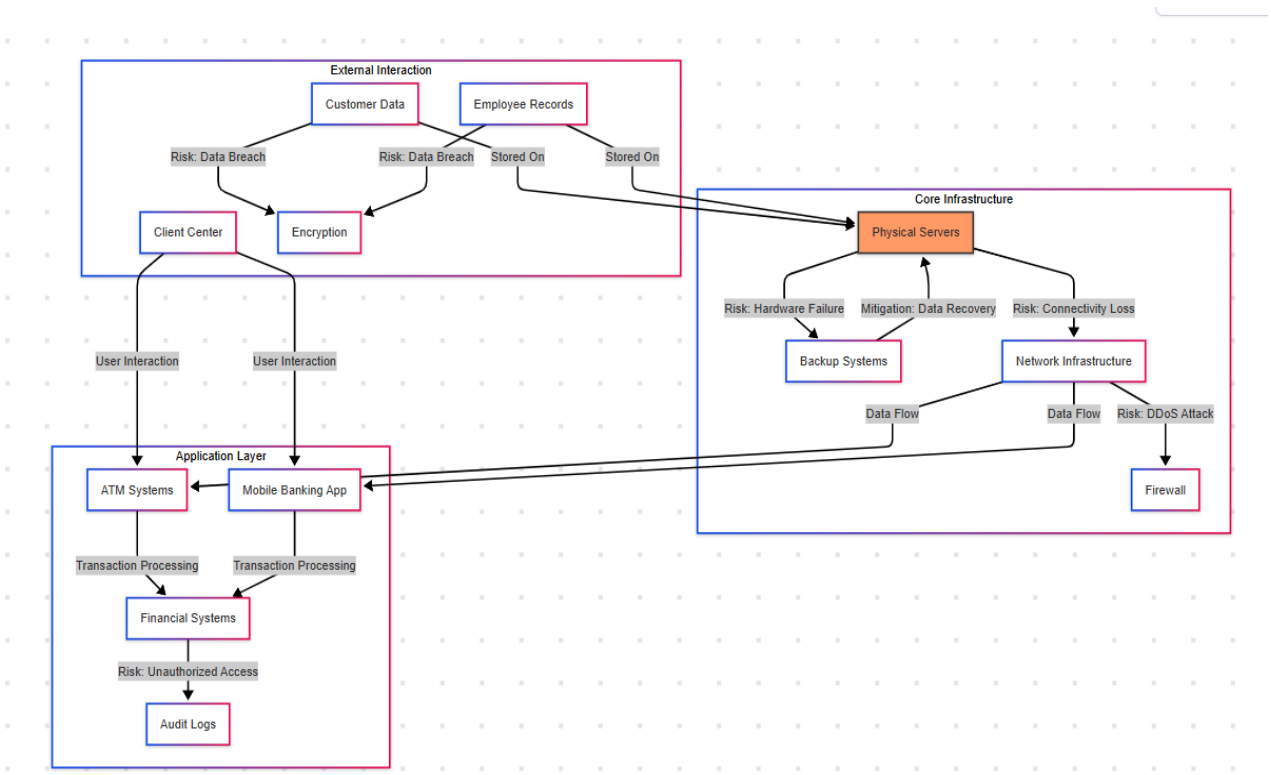


Figure 1. – Company's assets scope

# 1. Assets identification and assessment

## 1.1. Goals

Define list of assets for Crystal Bank and perform both identification and assessment procedures for ones.

## 1.2. Tasks

- Select all applicable types of the assets for Crystal Bank
- Perform identification of assets in accordance with ISO 27001 (ISO 31000)
- Create list of recommendations for top management about IT security protection for assets

## 1.3. Input data

Describe a list of important assets in accordance with scope and boundaries of «Crystal Bank».
The result shown in Table 1.1

**Table 1.1 – Initial assets identification**

| № | Asset name | Asset location | Asset characteristics | Asset technics | Asset scope | Asset boundaries |
|---|---|---|---|---|---|---|
| 1. | *Customer Data* | *Data Center* | *Sensitive customer information* | *Encryption, Access Control* | *Data Privacy* | *Internal and External* |
| 2. | *Employee Records* | *HR Department* | *Personal and Payroll information* | *Access Control, Encryption* | *HR Management* | *Internal* |
| 3. | *Physical Servers* | *Server Room* | *Hardware Infrastructure* | *Environmental Controls* | *IT Infrastructure* | *Physical Security* |
| 4. | *Financial Systems* | *Data Center* | *Core Banking software* | *Firewalls, Intrusion Detection* | *Financial operations* | *Internal Network* |
| 5. | *Network Infrastructure* | *Data Center* | *Router, Switches, Cables* | *Network, Monitoring Redundancy* | *IT Operations* | *Internal and External* |
| 6. | *ATM Systems* | *Branch locations* | *Transaction Processing* | *Encryption, Physical Security* | *Financial operations* | *External* |
| 7. | *Mobile Banking App* | *Cloud* | *Customer transactions* | *Encryption, Access Control* | *Data Privacy* | *External* |
| 8. | *Backup systems* | *Data Center* | *Data replication* | *Encryption, Redundancy* | *IT Operations* | *Internal* |

## 1.4. Outcomes

Define a type and owner for each identified asset.
The result shown in Table 1.2

**Table 1.2 – List of assets identification by type and owner**

| № | Asset name | Asset type | Asset owner |
|---|---|---|---|
| 1. | *Customer data* | *Intangible* | *Chief Data Officer* |
| 2. | *Employee Records* | *Intangible* | *Head of HR Department* |
| 3. | *Physical Servers* | *Tangible* | *IT Infrastructure Manager* |
| 4. | *Financial Systems* | *Digital* | *Chief Information Officer (CIO)* |

| № | Asset name | Asset type | Asset owner |
|---|---|---|---|
| 5. | *Network Infrastructure* | *Physical* | *Head of Networks Department* |
| 6. | *ATM Systems* | *Physical* | *Branch Manager* |
| 7. | *Mobile Banking App* | *Digital* | *Chief Technology Officer* |
| 8. | *Backup Systems* | *Digital* | *IT Operations Manager* |

Define asset' size and asset's cost for each identified assets under asset' owner mark.

There are two methods for asset's part cost evaluation – Qualitative (High, Medium,…) and Quantitate (point, euros,…)

The result shown in Table 1.3

**Table 1.3 – List of assets identification by size, cost after Owner established**

| № | Asset name | Asset size | Asset (tangible part) cost | Asset (intangible part) level | Asset marks |
|---|---|---|---|---|---|
| 1. | *Customer data* | *Big* | *Intangible value* | *Very High* | ***10*** |
| 2. | *Employee Records* | *Medium* | *Intangible value* | *High* | ***8*** |
| 3. | *Physical servers* | *Medium* | *High* | *Medium* | ***7*** |
| 4. | *Financial systems* | *Big* | *High* | *Very High* | ***9*** |
| 5. | *Network Infrastructure* | *Big* | *High* | *High* | ***9*** |
| 6. | *ATM Systems* | *Medium* | *Medium* | *High* | ***7*** |
| 7. | *Mobile Banking App* | *Big* | *High* | *Very High* | ***10*** |
| 8. | *Backup systems* | *Medium* | *Medium* | *Medium* | ***6*** |

## 1.5. Conclusion

The company «Crystal Bank» assets has been defined.

Assets evaluation has been completed against Owner's criteria and installed IT-security controls.

The final list of recommendations for top management about IT-security protection for all identified assets of «Crystal Bank» company has been prepared.

For example, the initial list of assets was cut in half after the analysis in the first stage.

The result shown in Table 1.4

**Table 1.4 – Decision's list after Criteria evaluation**

| № | Asset name | Asset marks | Criteria marks | Decision (Applicable) | List of controls | Responsible |
|---|---|---|---|---|---|---|
| 1. | *Customer Data* | ***10*** | ***7*** | No | *A.8.1.2, A.8.2.1 A.9.4.1* | *Chief Data Officer (CDO)* |
| 2. | *Employee Records* | ***8*** | ***7*** | No | *A.8.2.1 A.9.2.3 A.10.1.1* | *Head of HR Department* |
| 3. | *Financial Systems* | ***9*** | ***7*** | No | *A.12.6.1 A.13.1.1 A.14.1.2* | *Chief Information Officer (CIO)* |
| 4. | *Network Infrastructure* | ***9*** | ***7*** | No | *A.13.1.1 A.17.1.2 A.12.6.1* | *Head of Networks Department* |
| 5. | *Mobile Banking App* | ***10*** | ***7*** | No | *A.14.1.2 A.18.1.4 A.12.4.1* | *Chief Technology Officer (CTO)* |
| 6. | *ATM Systems* | ***7*** | ***7*** | Yes | *A.9.1.1 A.14.1.1* | *Branch Manager* |

| № | Asset name | Asset marks | Criteria marks | Decision (Applicable) | List of controls | Responsible |
|---|---|---|---|---|---|---|
| 7. | *Backup systems* | *6* | *7* | *Yes* | *A.12.3.1*<br>*A.17.1.3* | *IT Operations Manager* |
| 8. | *Physical Servers* | *7* | *7* | *Yes* | *A.11.1.1*<br>*A.11.2.1* | *IT Infrastructure Manager* |

# 2. Vulnerabilities identification and assessment

## 2.1. Goals

Define list of vulnerabilities for «Crystal Bank» assets and perform an assessment procedure for ones.

## 2.2. Tasks

— Select all applicable types of the vulnerabilities for assets of «Crystal Bank»
— Perform assessment of vulnerabilities in accordance with ISO 27005
— Create list of recommendations for top management about IT-security protection for vulnerabilities

## 2.3. Input data

See Table 1.4

## 2.4. Outcomes

Define vulnerabilities and their type for identified assets

**Table 2.1 – List of vulnerabilities and their types**

| № | Asset name | Vulnerability | Vulnerability type |
|---|---|---|---|
| 1. | *Customer Data* | *Lack of encryption* | *Technical* |
| 2. | *Employee Records* | *Unauthorized access* | *Organizational* |
| 3. | *Financial systems* | *Software vulnerabilities* | *Technical* |
| 4. | *Network Infrastructure* | *Network outages* | *Technical* |
| 5. | *Mobile Banking App* | *Weak authentication* | *Technical* |

There are two methods for asset's vulnerabilities evaluation – Qualitative (High, Medium,) and Quantitate (point, …). The assets vulnerabilities assessment are shown below in the scale:

- Very small – 0
- Small – 1 – 2
- Medium – 2 – 3
- High – 3 – 4
- Very High – 4 – 5

**Table 2.2 – List of vulnerabilities assessment**

| № | Asset name | Vulnerability | Assessment method | Vulnerability mark | Auditor |
|---|---|---|---|---|---|
| 1. | *Customer data* | *Lack of encryption* | *Penetration testing* | ***4*** | *Chief Data Officer* |
| 2. | *Employee Records* | *Unauthorized access* | *Audit* | ***3*** | *Head of HR Department* |
| 3. | *Financial Systems* | *Software vulnerabilities* | *Vulnerability scan* | ***4*** | *Chief Information Officer (CIO)* |
| 4. | *Network Infrastructure* | *Network outages* | *Monitoring* | ***4*** | *Head of Networks Department* |
| 5. | *Mobile Banking Application* | *Weak authentication* | *Penetration testing* | ***4*** | *Chief Technology Officer (CTO)* |

## 2.5. Conclusion

Vulnerabilities of the assets of the company «Crystal Bank» were identified.
Vulnerabilities evaluation has been completed against Auditor's criteria for all assets.
The final list of recommendations for top management about IT-security protection for all vulnerabilities of all identified assets of «Crystal Bank» company has been prepared.
For example, the initial list of vulnerabilities of the assets was reduced from 5 to 3 after the analysis in the second stage, focusing on the most critical vulnerabilities.
The result shown in Table 2.3

**Table 2.3 – recommendation list**

| № | Asset name | Vulnerability | Vuln. marks | Criteria marks | Decision (Applicable) | Auditor |
|---|---|---|---|---|---|---|
| 1. | *Customer data* | *Lack of encryption* | *4* | ***3*** | *No* | *Chief Data Officer (CDO)* |
| 2. | *Employee Records* | *Unauthorized access* | *3* | ***3*** | *Yes* | *Head of HR Department* |
| 3. | *Financial Systems* | *Software vulnerabilities* | *4* | *3* | *No* | *Chief Information Officer* |
| 4. | *Mobile Banking Application* | *Weak authentication* | *4* | ***3*** | *No* | *Chief Technology Officer (CTO)* |
| 5. | *Network Infrastructure* | *Network outages* | *4* | ***3*** | *No* | *Head of Networks Department* |

# 3. Threats identification and assessment

## 3.1. Goals

Define list of threats for «Crystal Bank» vulnerabilities of identified assets and perform an assessment procedure for ones.

## 3.2. Tasks

— Select all applicable types of the threats for defined vulnerabilities of «Crystal Bank»
— Perform assessment of threats in accordance with ISO 27005
— Create list of recommendations for top management about IT-security protection for threats

## 3.3. Input data

See Table 2.3

## 3.4. Outcomes

Define threats and their type and origin for vulnerabilities of identified assets.
Use Annexes C and D from ISO/IEC 27005.
The results are shown in Table 3.1

**Table 3.1 – List of threats and threat type**

| № | Asset name | Vulnerability | Threat | Threat type | Threat origin |
|---|---|---|---|---|---|
| 1. | *Customer data* | *Lack of encryption* | *Data Breach* | *Compromise of information* | *External* |
| 2. | *Financial systems* | *Software vulnerabilities* | *Cyber attack* | *Compromise of information* | *External* |
| 3. | *Mobile Banking Application* | *Weak authentication* | *Account takeover* | *Unauthorized action* | *External* |
| 4. | *Network Infrastructure* | *Network Outages* | *Service Disruption* | *Availability Loss* | *Internal* |

There are two methods for asset threat's evaluation – Qualitative (High, Medium,) and Quantitative (point, …). The threat assessment is shown below in the scale:

- Very small – 0
- Small – 1
- Medium – 2
- High – 3
- Very High – 4

The results of threats assessment are shown in Table 3.2

**Table 3.2 – List of threats assessment**

| № | Asset name | Threat | Threat type | Threat origin | Threat mark | Auditor |
|---|---|---|---|---|---|---|
| 1. | *Customer Data* | *Data Breach* | *Compromise of information* | *External* | ***4*** | *Chief Data Officer (CDO)* |
| 2. | *Financial systems* | *Cyber attack* | *Compromise of information* | *External* | ***4*** | *Chief Information Officer (CIO)* |
| 3. | *Mobile Banking Application* | *Account takeover* | *Unauthorized action* | *External* | ***4*** | *Chief Technology Officer (CTO)* |
| 4. | *Network Infrastructure* | *Service Disruption* | *Availability Loss* | *Internal* | ***3*** | *Head of Networks Department* |

## 3.5. Conclusion

All threats of the assets of the company «Crystal Bank» were identified.
Threats evaluation has been completed against Auditor's criteria for all assets.
The final list of recommendations for top management about IT-security protection for all threats of all identified assets of «Crystal Bank» company has been prepared.
For example, the initial list of threats of the assets was cut in half after the analysis in the third stage.
The result shown in Table 3.3

**Table 3.3 – recommendation list**

| № | Asset name | Threat | Threat marks | Criteria marks | Decision (Applicable) | Auditor |
|---|---|---|---|---|---|---|
| 1. | *Customer Data* | *Data breach* | ***4*** | ***3*** | *No* | *Chief Data Officer (CDO)* |
| 2. | *Financial Systems* | *Cyber attack* | ***4*** | ***3*** | *No* | *Chief Information Officer (CIO)* |
| 3. | *Mobile Banking Application* | *Account Takeover* | ***4*** | ***3*** | *No* | *Chief Technology Officer (CTO)* |
| 4. | *Network Infrastructure* | *Service Disruption* | ***3*** | ***3*** | *Yes* | *Head of Networks Department* |

# 4. Risks identification and assessment

## 4.1 Goals

Perform sequential identification and risk assessment for the all defined and pre-assessed assets for «Crystal Bank» company.

## 4.2 Tasks

- Perform identification and assessment of risks in accordance with ISO 27005 for «Crystal Bank» assets.
- Create a list of recommendations for top management about IT-security risks treatment.

## 4.3 Input data

**Table 4.1 – Initial assets identification**

| № | Asset name | Decision (Applicable) Table 1.4 | Vulnerability | Decision (Applicable) Table 2.3 | Threat | Decision (Applicable) Table 3.3 |
|---|---|---|---|---|---|---|
| 1. | *Customer Data* | ***No*** | *Lack of encryption* | ***No*** | *Data Breach* | ***No*** |
| 2. | *Financial Systems* | *No* | *Software vulnerabilities* | *No* | *Cyber attack* | *No* |
| 3. | *Mobile Banking App* | *No* | *Weak Authentication* | *No* | *Account Takeover* | *No* |

## 4.4 Outcomes

There are two methods for risk's evaluation – Qualitative (High, Medium,) and Quantitate (point, …). The risk assessment is shown below in the scale:

- Very small – 0
- Small – 1
- Medium – 2
- High – 3
- Very High – 4

Use Annex E from ISO/IEC 27005.

The results of risk assessment are shown in Table 4.2

Generally, **Risk mark = Likelihood * Business impact (Severity)**

**Table 4.2 – Risk identification and assessment**

| № | Asset name | Threat | Likelihood of incident scenario | Business Impact | Risk level | Risk mark |
|---|---|---|---|---|---|---|
| 1. | *Customer Data* | *Data breach* | *Medium* | *High* | *Medium* | ***2*** |
| 2. | *Financial systems* | *Cyber attack* | *High* | *High* | *High* | ***3*** |
| 3. | *Mobile Banking App* | *Account Takeover* | *High* | *Very High* | *Very High* | ***4*** |

## 4.5 Conclusion

All risks of the assets of the company «Crystal Bank» were identified.

Risks evaluation has been completed against Auditor's criteria for all assets.

The final list of recommendations for top management about IT-security risk for all identified assets of «Crystal Bank» company has been prepared.

The result shown in Table 4.3

**Table 4.3 – Recommendation list**

| № | Asset name | Threat | Risk level | Risk criteria | Decision (Applicable) | Decision (Treatment) | Auditor |
|---|---|---|---|---|---|---|---|
| 1. | *Customer data* | *Data Breach* | *Medium* | *Medium* | *Yes* | *No* | *Chief Data Officer* |
| 2. | *Financial systems* | *Cyber attack* | *High* | ***Medium*** | *No* | ***Yes*** | *Chief Information Officer* |
| 3. | *Mobile Banking App* | *Account Takeover* | *Very High* | ***Medium*** | *No* | ***Yes*** | *Chief Technology Officer* |

# 5. Controls select and implementation

## 5.1. Goals

Select appropriate security measures for risk management

## 5.2. Tasks

— Select the appropriate protection measures for risk treatment in accordance with ISO 27001 and ISO 22301
— Suggest appropriate measures to monitor the selected protection measures in accordance with ISO 31000 (27001) and ISO 22301
— Create a list of recommendations for top management about risks control

## 5.3. Input data

See Table 4.3

## 5.4. Outcomes

Use Annex A from ISO/IEC 27001.
The results of selection of new IT-security control are shown in Table 5.1

**Table 5.1 – Risk treatment and required resources**

| № | Asset name | Threat | Decision (Treatment) | Type of Risk treatment | Required resources | IT-security control (New) |
|---|---|---|---|---|---|---|
| 1. | *Financial systems* | *Cyber attack* | *Yes* | *Changing the likelihood with update software patches and intrusion detection* | *Vulnerability scanning tools. Patch management tools* | *A.12.6.1*<br>*A.13.1.1*<br>*A.14.1.2*<br>*A.5.7*<br>*A.8.16*<br>*A.16.1.1* |
| 2. | *Mobile banking application* | *Account takeover* | *Yes* | *Implement multifactor authentication and session controls* | *Identity Access Management solutions, Authentication protocols* | *A.9.2.3*<br>*A.9.4.1*<br>*A.14.1.2*<br>*A.9.4.2*<br>*A.9.4.4*<br>*A.9.4.5* |

## 5.5. Conclusion

The new IT-security controls for assets of the company «Crystal Bank» were selected.
The types of risk treatment were defined.
The final list of recommendations for top management about treatment the IT-security risk for all identified assets of «Crystal Bank» company has been prepared.
The result shown in Table 5.2

**Table 5.2 – Recommendation list**

| № | Asset name | Threat | Decision (Treatment) | IT-security control (New) | Auditor |
|---|---|---|---|---|---|
| 1. | *Financial Systems* | *Cyber attacks* | *Yes* | *A.12.6.1*<br>*A.13.1.1*<br>*A.14.1.2*<br>*A.5.7*<br>*A.8.16*<br>*A.16.1.1* | *Chief Information Officer* |

| № | Asset name | Threat | Decision (Treatment) | IT-security control (New) | Auditor |
|---|---|---|---|---|---|
| 2. | *Mobile Banking Application* | *Account Takeover* | *Yes* | *A.9.2.3*<br>*A.9.4.1*<br>*A.14.1.2*<br>*A.9.4.2*<br>*A.9.4.4*<br>*A.9.4.5* | *Chief Technology Officer (CTO)* |

# 6. Residual risks identification and re-assessment

## 6.1 Goals

Perform a re-assessment of the risks and residual risks for all identified and pre-assessed assets of the company «Crystal Bank», considering the selected additional protection measures

## 6.2 Tasks

- Perform re-assessment of IT-security risks in accordance with ISO 27005 for «Crystal Bank» assets.
- Perform analyses of IT-security residual risk and evaluate ones against criteria again.
- Create a list of recommendations for top management about IT-security risks treatment.

## 6.3 Input data

See Table 4.3
See Table 5.2

## 6.4 Outcomes

There are two methods for residual risk's evaluation – Qualitative (High, Medium,) and Quantitate (point, …). The risk re-assessment are shown below in the scale:

- Very small – 0
- Small – 1
- Medium – 2
- High – 3
- Very High – 4

Use Annex E from ISO/IEC 27005.
The results of residual risk assessment are shown in Table 6.1
Generally, Residual Risk mark = Likelihood * Business impact (Severity)

**Table 6.1 – Results of residual risk assessment**

| № | Asset name | Threat | IT-security control (New) | Likelihood of incident scenario | Business Impact | Residual risk level | Auditor |
|---|---|---|---|---|---|---|---|
| 1. | *Financial Systems* | *Cyber attack* | *A.12.6.1*<br>*A.13.1.1*<br>*A.14.1.2*<br>*A.5.7*<br>*A.8.16*<br>*A.16.1.1* | *Medium* | *High* | ***Medium*** | *Chief Information Officer* |
| 2. | *Mobile Banking App* | *Account Takeover* | *A.9.2.3*<br>*A.9.4.1*<br>*A.14.1.2*<br>*A.9.4.2*<br>*A.9.4.4* | *Medium* | *Very High* | ***High*** | *Chief Technology Officer* |

| № | Asset name | Threat | IT-security control (New) | Likelihood of incident scenario | Business Impact | Residual risk level | Auditor |
|---|---|---|---|---|---|---|---|
| | | | *A.9.4.5* | | | | |

## 6.5 Conclusion

All residual risks of the assets of the company «Crystal Bank» were identified and re-assessed.
Residual risks evaluation has been completed against Auditor's criteria for all assets.
The final list of recommendations for top management about IT-security residual risk for all identified assets of «Crystal Bank» company has been prepared.
The result shown in Table 6.2

**Table 6.2 – Recommendation list**

| № | Asset name | Threat | Risk level | Risk criteria | Residual risk level | Decision (Final) | Auditor |
|---|---|---|---|---|---|---|---|
| 1. | *Financial Systems* | *Cyber attack* | *High* | ***High*** | ***Medium*** | ***Mitigate further*** | *Chief Information Officer* |
| 2. | *Mobile Banking Application* | *Account Takeover* | *Very High* | ***Very High*** | ***High*** | ***Mitigate immediately*** | *Chief Technology Officer (CTO)* |

## 6.6 Final CONCLUSION

The goal of coursework – Controls select of risk identification and assessment methods and their implementation – was achieved through the following tasks:

- Identify and assess assets;
- Identify and assess vulnerabilities;
- Identify and assess assets threats;
- Identify and assess assets risks and residual risks;
- Make recommendations for top management for the protection of IT-security.

# 7. BIBLIOGRAPHY


- ISO/IEC 13335-1-2004
- ISO/IEC 27005
- ISO/IEC 27001
- ISO/IEC 22301
- ISO/IEC 31000