**Establishing Modern Master-level Studies in Information Systems   
561592-EPP-1-2015-1- FR-EPPKA2-CBHE-JP**

**ІT – infrastructure**

**Guidelines to perform laboratory works**

Laboratory work # 4

Topic: Risk analysis of IT infrastructure of the company

**draft version**



**Theoretical information**

With the growing dependence on the implementation of IT solutions, the company's dependence on the risks associated with the use of IT increases. IT risk management becomes an integral part of global business risk management processes, and IT risk assessment and management require an analysis of IT-specific factors, including those related to information security (IT) of implemented solutions.

• External and internal fraud.

• unauthorized use of company resources.

• Violation of the confidentiality, integrity and authenticity of information.

• Loss of resource availability.

• Human factor and staff mistakes.

• Failure of information systems, unplanned simple systems.

• Non-compliance with regulatory and regulatory requirements, etc.

Identifying and reducing the risks of IT solutions is an integral part of the company's information security service, which is increasingly complicated by the growing number of IT infrastructure components and systems interactions.

**Classification of IT Risks**

|  |  |  |
| --- | --- | --- |
| **Category** | **Value** | **Example** |
| Technology | Inactive, unreliable, or non-compliant with business, hardware or software needs | Router refusal  Denial of database server |
| Security | Loss, damage or theft of equipment or data, unauthorized access or use of data | Unauthorized access to the network through a web server  Data leak on CDs, flash cards, etc.  Hacking passwords |
| Politics and law | Lack of procedures and policies that result in misuse, inability to rehabilitate, non-compliance with legislation | Emergency recovery procedure is not documented and not tested  Damage to health due to non-compliance with safety  Use of non-licensed software  Installing unnecessary or inappropriate software  Failure to receive important letters |
| Staff | Human mistakes, dismissal of key employees | Errors updating SQL Server database  Lack of necessary skills and abilities |
| Infrastructure | Disconnection of external services (electricity, telephone, internet); failure of key vendors | Inability to use e-mail  The inability to solve business challenges with key applications |

**Risk assessment**

To assess risks, one can use qualitative analysis when the level of risk is determined by the ratio of the probability of an incident and its impact on the business.

**Probability of occurrence**

|  |  |
| --- | --- |
| High | The incident occurs once a month or more often |
| Average | An incident occurs 1 to 11 times a year |
| Low | The incident occurs once a year or less frequently |

**Risk level**

|  |  |  |
| --- | --- | --- |
| Extraordinary | Major business processes stop for more than a day or irrevocably | Immediate risk management is required.  The management should be informed about the risk and measures to reduce it. |
| High | The main business processes stop for an hour to a day | Risk management should be started within a month from the moment of confirmation.  The management should be informed about the risk and measures to reduce it. |
| Average | Major business processes stop at less than an hour | It is necessary to start the risk management within six months from the moment of confirmation. |
| Low | Short stop, which has no negative consequences for business | Permissible risks that do not require management.  As needed, a reassessment can be made. |

You need to keep an IT Risk Log, which tracks the current level of risk management and measures taken to reduce risks.

**Template of Log**

|  |  |
| --- | --- |
| Risk |  |
| Consequences |  |
| Management level |  |
| Probability of occurrence |  |
| Influence on business |  |
| Rank |  |
| Date of the rank assignment |  |
| Responsible person |  |
| Need for additional measures |  |
| Terms of ficsing |  |
| Action |  |
| Rank after taking action |  |
| Date of implementation |  |
| The date of the next check |  |

The first part of the Journal describes the categories of risks (with short estimates) and typical actions to reduce the risks. This will allow assessing the status of executed, deferred and current risk management tasks, as well as highlighting tasks that are subject to re-examination. The frequency of repeat checks is arbitrary: not too rare, so as not to be exposed to new risks caused by system or structural changes, but also not very frequent, otherwise you can spend all the time on risk assessment with the mark "unchanged".

The second part of the Magazine provides detailed risk assessments and additional risk mitigation measures where possible. Additional measures may include system changes, new procedures, policy changes, or re-training or hiring specialists. example:

• Saving images of system drives, in addition to backing up files;

• purchase of spare equipment;

• View password security policy;

• Monitoring of data leakage;

• introduction of the rules of permissible use;

• improved documentation of systems;

• Caution when choosing vendors.

The IT risk logging log is required to be reviewed annually to ensure that the risks are objectively evaluated, to assess the effectiveness of risk mitigation and to include new risk categories.

**Task**

Object of development - IT infrastructure of the enterprise (company) for which IT infrastructure audit in the laboratory work No. 1 was performed.

Analyze the technological, financial, technical and integration risks of the IT infrastructure for two options: virtual and non-virtual infrastructure.

Assess the level of infrastructure risk. Based on the analysis, formulate recommendations.

Prepare report.

**Testing questions:**

1. Technological risks.

2. Financial risks.

3. Technical risks.

4. Integration risks.

5. Methods of assessing information risks

6. Criminal risks

7. The concept and objectives of information security.

8. Structures providing information security.

9. Stages of information security development.

10. Unified communications. Data access and synchronization.

11. Unified communications. Closed Protocols.

12. Unified communications. Smart networks

**LIST OF RECOMMENDED LITERATURE**

1. Олейник А. И., Сизов А. В. (2012) ИТ-инфраструктура [Текст]: учеб.-метод. пособие / А. И. Олейник, А. В. Сизов; Нац .исслед. ун-т «Высшая школа экономики». — М.: Изд. дом Высшей школы экономики. — 134 с.
2. ITIL - IT Infrastructure Library - Available at <https://www.axelos.com/store>
3. Bernard S. A. (2005) Introduction to Enterprise Architecture; Publisher: authorHOUSE™
4. Alter S., "Work System Theory: Overview of Core Concepts, Extensions, and Challenges for the Future" (2013). Business Analytics and Information Systems. Paper 35.
5. Adner R., Kapoor, R. (2016). Right Tech, Wrong Time. Harvard business review, 94(11), 60-67.