Программа учебной дисциплины «Information Systems Audit»

Утверждена
Академическим советом ООП
Протокол № от «__»_____20__ г.

<table>
<thead>
<tr>
<th>Автор</th>
<th>Грекул В.И., к.т.н.,</th>
</tr>
</thead>
<tbody>
<tr>
<td>Число кредитов</td>
<td>4</td>
</tr>
<tr>
<td>Контактная работа (час.)</td>
<td>72</td>
</tr>
<tr>
<td>Самостоятельная работа (час.)</td>
<td>156</td>
</tr>
<tr>
<td>Курс</td>
<td>2</td>
</tr>
<tr>
<td>Формат изучения дисциплины</td>
<td>Без использования онлайн</td>
</tr>
</tbody>
</table>

I. ЦЕЛЬ, РЕЗУЛЬТАТЫ ОСВОЕНИЯ ДИСЦИПЛИНЫ И ПРЕРЕКВИЗИТЫ

The aim of the course is to teach students to use their generalized knowledge in various fields of IT for estimation of information system (IS) characteristics and IS-related controls.

On completion of this course students should learn:

- IT Audit and Assurance Standards, Guidelines, and Tools and Techniques; Code of Professional Ethics; and other applicable standards.
- Risk assessment concepts, tools and techniques in an audit context.
- Control objectives and controls related to information systems.
- Audit planning and audit project management techniques, including follow-up.
- Fundamental business processes including relevant IT.
- Applicable regulations that affect the scope, evidence collection and preservation, and frequency of audits.
- Evidence collection techniques (e.g., observation, inquiry, inspection, interview data analysis) used to gather protect and preserve audit evidence.
- Reporting and communication techniques (e.g., facilitation, negotiation, conflict resolution, audit report structure).

Students should also gain experience in audit project planning and assessing of main information systems characteristics.

This course is based on the program of CISA (Certified Information Systems Auditor) exam and introduces students to the concepts and practical methods of full cycle of IS auditing. This is the main feature of the course that distinguishes it from other similar disciplines studied in Russian and foreign Universities and aimed usually to separate categories of audit (e.g., audit of Information Security Management, IT strategy audit, Network Infrastructure audit etc.).

This discipline is optional for specialization "Information systems management" within the Master's program "Business Informatics"

The study of this discipline is based on the following disciplines:

- "Design of Information Systems";
- "IT-service management";
• "Improving enterprise architecture".

For the discipline mastering, students should know conceptual foundations of enterprise architecture, basic classes of information systems for business management, fundamental business processes including relevant IT processes, best practices and up-to-date standards in the field of information technology (PMBOK, ISO/IEC 15288, ITIL, CobiT), methodologies of information systems design and implementation, be able to organize and synthesize information to develop specific proposals to improve IT-management processes.

Main provisions of the discipline should be used further to prepare master theses, scientific articles and reports.

II. СОДЕРЖАНИЕ УЧЕБНОЙ ДИСЦИПЛИНЫ

1. The Process of Auditing Information Systems

Main tasks of auditor:
- Develop and implement a risk-based IT audit strategy.
- Plan specific audits to determine whether information systems are protected, controlled and provide value to the organization.
- Conduct audits in accordance with IT audit standards.
- Report audit findings and make recommendations to key stakeholders.
- Conduct follow-ups or prepare status reports to ensure that appropriate actions have been taken by management in a timely manner.

Main areas of auditing expertise: IT Audit and Assurance Standards, Guidelines, and Tools and Techniques; Code of Professional Ethics; and other applicable standards. Risk assessment concepts, tools and techniques in an audit context control objectives and controls related to information systems. Audit planning and audit project management techniques fundamental business processes including relevant IT evidence collection techniques (e.g., observation, inquiry, inspection and interview data analysis) used to gather protect and preserve audit evidence. Compliance and substantive testing. Reporting and communication techniques (e.g., facilitation, negotiation, conflict resolution, audit report structure).

2. Governance and Management of Information Technologies

Main objectives to be evaluated:
- The effectiveness of the IT governance structure.
- IT organizational structure and human resources (personnel) management.
- IT strategy.
- IT policies, standards and procedures.
- Adequacy of the quality management system to determine whether it supports the organization's strategies and objectives in a cost-effective manner.
- IT management and monitoring of controls.
- IT resource investment.
- IT contracting strategies and policies. Risk management practices.
- Monitoring and assurance practices.
Main areas of auditing expertise: IT governance, management, security and control frameworks, and related standards, guidelines and practices. The purpose of IT strategy, policies, standards and procedures for an organization and the essential elements of each. The organizational structure, roles and responsibilities related to IT the processes for the development, implementation and maintenance of IT strategy, policies, standards and procedures. Quality management systems. Maturity models. IT resource investment and allocation practices, including prioritization criteria (e.g., portfolio management, value management, project management). IT supplier selection, conflict management, relationship management and performance monitoring processes including third-party outsourcing relationships enterprise risk management practices for monitoring and reporting of IT performance (e.g., balanced scorecards, key performance indicators [KPIs]). IT human resources (personnel) management practices used to invoke the business continuity plan.

3. Information Systems Acquisition, Development and Implementation

Main objectives to be evaluated:

- Business case for proposed investments in information systems.
- Project management practices and controls.
- Controls for information systems during the requirements, acquisition, development and testing phases.
- Readiness of information systems for implementation and mitigation into production to determine whether project deliverables, controls and the organization’s requirements are met.
- Post-implementation reviews of systems.

Main areas of auditing expertise: Benefits realization practices (e.g., feasibility studies, business cases, total cost of ownership [TCO], ROI). Project governance mechanisms (e.g., steering committee, project oversight board, project management office). Project management control frameworks, practices and tools. Risk management practices applied to projects IT architecture related to data, applications and technology (e.g., distributed applications, web-based applications, web services, n-tier applications) acquisition practices (e.g., evaluation of vendors, vendor management, escrow). Requirements analysis and management practices (e.g., requirements verification, traceability, gap analysis, vulnerability management, security requirements). Project success criteria and risks. Control objectives and techniques that ensure the completeness, accuracy, validity and authorization of transactions and data. system development methodologies and tools, including their strengths and weaknesses (e.g., agile development practices, prototyping, rapid application development [RAD]; object-oriented design techniques). Testing methodologies and practices related to information systems development. Configuration and release management relating to the development of information systems. System migration and infrastructure deployment practices and data conversion tools, techniques and procedures. Post-implementation review objectives and practices.

4. Information Systems Operations, Maintenance and Support

Main objectives to be evaluated:

- Periodic reviews of information systems to determine whether they continue to meet the organization's objectives.
- Service level management practices.
- Third-party management practices.
- Operations and end-user procedures.
- Process of information systems maintenance.
- Data administration practices.
- Capacity and performance monitoring tools and techniques.
- Problem and incident management practices.
- Change, configuration and release management practices.
- Adequacy of backup and restore provisions organization's disaster recovery plan.

**Main areas of auditing expertise:** Service level management practices and the components within a service level agreement. Techniques for monitoring third-party compliance with the organization's internal controls. Operations and end-user procedures for managing scheduled and nonscheduled processes. The technology concepts related to hardware and network components, system software and database management systems. Control techniques that ensure the integrity of system interfaces. Software licensing and inventory practices. System resiliency tools and techniques (e.g., fault tolerant hardware, elimination of single point of failure, clustering). Database administration practices. Capacity planning and related monitoring tools and techniques. Systems performance monitoring processes, tools and techniques (e.g., network analyzers system utilization reports, load balancing). Problem and incident management practices (e.g., help desk, escalation procedures, tracking). Processes for managing scheduled and nonscheduled changes to the production systems and/or infrastructure including change, configuration, release and patch management practices. Data backup, storage, maintenance, retention and restoration practices.

5. **Protection of Information Assets**

**Main objectives to be evaluated:**

- Information security policies, standards and procedures.
- Design, implementation and monitoring of system and logical security controls.
- Design, implementation and monitoring of the data classification processes and procedures for alignment with the organization's policies, standards, procedures and applicable external requirements.
- Design, implementation and monitoring of physical access and environmental controls.
- Processes and procedures used to store, retrieve, transport and dispose of information assets

**Main areas of auditing expertise:** Techniques for the design, implementation and monitoring of security controls, including security awareness programs. Processes related to monitoring and responding to security incidents (e.g., escalation procedures, emergency incident response team). Logical access controls for the identification, authentication and restriction of users to authorized functions and data. Security controls related to hardware, system software (e.g., applications, operating systems), and database management systems. Risks and controls associated with virtualization of systems. Configuration, implementation, operation and maintenance of network security controls. Network and Internet security devices, protocols and techniques. Information system attack methods and techniques. Detection tools and control techniques (e.g., malware, virus detection, spyware). Security testing techniques (e.g., intrusion testing, vulnerability scanning). Risks and controls associated with data leakage. Encryption-related techniques. Public key infrastructure (PKI) components and digital signature techniques. Risks and controls associated with the use of mobile and wireless devices. Voice communications security (e.g., PBX, VoIP). The evidence preservation techniques and processes followed in forensics investigations (e.g., IT, process, chain of custody). Data classification standards and supporting procedures. Physical access controls for the identification, authentication and restriction of users to authorized facilities. Environmental protection devices and supporting practices. Processes and procedures used to store, retrieve, transport and dispose of confidential information assets.

6. **Business Continuity and Disaster Recovery**
Main objectives to be evaluated:

- The adequacy of backup and restore provisions to ensure the availability of information required to resume processing.
- The organization's disaster recovery plan.
- The organization's business continuity plan.

Main areas of auditing expertise: Data backup, storage, maintenance, retention and restoration processes, and practices. Regulatory, legal, contractual and insurance issues related to business continuity and disaster recovery. Business Impact Analysis (BIA). Development and maintenance of the business continuity and disaster recovery plans. Business continuity and disaster recovery testing approaches and methods. Human resources management practices as related to business continuity and disaster recovery (e.g., evacuation planning, response teams). Processes used to invoke the business continuity and disaster recovery plans. Types of alternate processing sites and methods used to monitor the contractual agreements (e.g., hot sites, warm sites, cold sites).

III. ОЦЕНИВАНИЕ

Procedure for the formation of estimates on discipline

Generating estimates of the discipline is made in accordance with the Regulations on the organization of the control of knowledge, approved by the Academic Council of the HSE.

Calculation of the grade

The grade for the course \( Q_{\text{final}} \) is determined as weighted average of follows marks:

\[
Q_{1-6} = \frac{1}{6} \sum Q_i - \text{the mark for progress tests, } Q_i = (1\ldots10) - \text{the mark for the topic } i;
\]

\( Q_e \) – the mark for the essay, \( Q_e = (1\ldots10) \);

\( Q_{cs} \)– the mark for the case study, \( Q_{cs} = (1\ldots10) \);

\( Q_{\text{exam}} \) – the mark for the exam \( Q_{\text{exam}} = (1\ldots10) \);

IV. ПРИМЕРЫ ОЦЕНОЧНЫХ СРЕДСТВ

Evaluation tools for monitoring and certification of the student

Progress Tests (Fragments)

Topic 1

01. Which of the following is the MOST important reason why an audit planning process should be reviewed at periodic intervals?

A. To plan for deployment of available audit resources
B. To consider changes to the risk environment
C. To provide inputs for documentation of the audit charter
D. To identify the applicable IS audit standards

02. When performing a computer forensic investigation [судебное расследование], in regard to the evidence gathered, an IS auditor should be MOST concerned with:
A. Analysis.
B. Evaluation.
C. Preservation.
D. Disclosure.

03. The internal audit department of an organization has developed and maintained ACL scripts for continuous auditing purposes. These scripts were provided to IT management for continuous monitoring purposes. This situation resulted in a potential conflict related to the auditors independence and objectivity. Which of the following actions would BEST resolve this issue?

A. The internal audit team should stop sharing the scripts so that IT management must develop its own scripts.
B. Since continuous monitoring and continuous auditing are similar functions, IT management should assign the continuous monitoring tasks to the internal audit department.
C. IT management should continue to use the scripts for continuous monitoring purposes with the understanding that it is responsible for testing and maintaining the scripts that it uses.
D. The internal audit team should review the areas where these scripts are being used and reduce the audit scope and frequency for those areas.

**Topic 2**

01. In an organization where an IT security baseline has been defined, the IS auditor should FIRST ensure:

A. Implementation
B. Compliance
C. Documentation
D. Sufficiency

02. Which of the following duties would be a concern if performed along with systems administration?

A. Access rule maintenance
B. System audit trail review
C. Data librarian
D. Performance monitoring

03. Which of the following BEST describes an IT department's strategic planning process?

A. The IT department will have either short-range or long-range plans depending on the organization's broader plans and objectives.
B. The IT department's strategic plan must be time- and project-oriented, but not so detailed as to address and help determine priorities to meet business needs.
C. Long-range planning for the IT department should recognize organizational goals, technological advances and regulatory requirements.
D. Short-range planning for the IT department does not need to be integrated into the short-range plans or the organization since technological advances will drive the IT department plans much quicker than organizational plans.

**Topic 3**

01. The most common reason for the failure of information systems to meet the needs of users is that:
A. User needs are constantly changing.
B. The growth of user requirements was forecast inaccurately.
C. The hardware system limits the number of concurrent users.
D. User participation in defining the system’s requirements was inadequate.

02. An IS auditor is assigned audit a software development project which is more than 80 percent complete, but has already overrun time by 10 percent and costs by 25 percent. Which of the following actions should the IS auditor take?

A. Report that the organization does not have effective project management
B. Recommend the project manager be changed
C. Review the IT governance structure
D. Review the conduct of the project and the business case

03. A request for a change to a report format in a module (subsystem) was made. After making the required changes, the programmer should carry out:

A. Unit testing.
B. Unit and module testing.
C. Unit, module and regression testing.
D. Module testing.

**Topic 4**

01. When assessing the portability of a database application, the IS auditor should verify that:

A. A structured query language (SQL) is used.
B. Information import and export procedures exist with other systems.
C. Indexes are used.
D. All entities have a significant name and identified primary and foreign keys.

02. Which of the following would an IS auditor expect to find in a console log?

A. Names of system users
B. Shift supervisor identification
C. System errors
D. Data edit errors

03. In a LAN environment, which of the following minimizes the risk of data corruption during transmission?

A. Using end-to-end encryption for data communication
B. Using separate conduits for electrical and data cables
C. Using check sums for checking the corruption of data
D. Connecting the terminals using a star topology

**Topic 5**

01. Which of the following steps would an IS auditor normally perform FIRST in a data center security review?

A. Evaluate physical access test results.
B. Determine the risks/threats to the data center site.
C. Review business continuity procedures.
D. Test for evidence of physical access at suspect locations.

02. Which of the following concerns associated with the World Wide Web would be addressed by a firewall?

A. Unauthorized access from outside the organization  
B. Unauthorized access from within the organization  
C. A delay in Internet connectivity  
D. A delay in downloading using File Transfer Protocol (FTP)

03. When auditing security for a data center, an IS auditor should look for the presence of a voltage regulator (surge protector) to ensure that the:

A. Hardware is protected against power surges.  
B. Integrity is maintained if the main power is interrupted.  
C. Immediate power will be available if the main power is lost.  
D. Hardware is protected against long-term power fluctuations.

**Topic 6**

01. Which of the following is the best way to ensure that the company’s backup tapes can be used at a warm site?

A. Retrieve the tapes from the off-site facility and verify that the equipment at the original site can read them  
B. Test them on the vendor’s machine, which won’t be used during an emergency  
C. Inventory each tape kept at the vendor’s site twice a month  
D. Test them on the equipment maintained within the hot site

02. Prior to a live disaster test, which of the following is most important?

A. Restore all files in preparation for the test  
B. Document expected findings  
C. Arrange physical security for the test site  
D. Conduct a successful structured walk-through

03. Which is not one of the primary goals of BIA?

A. Criticality prioritization  
B. Downtime estimation  
C. Determining requirements for critical business functions  
D. Deciding on various tests to be performed to validate the business continuity plan

**Final exam topics**

1. IT Audit and Assurance Standards, Guidelines, and Tools and Techniques; Code of Professional Ethics.
2. Risk assessment concepts, tools and techniques in an audit context.
3. Control objectives and controls related to information systems.
4. Audit planning.
5. Evidence collection techniques (e.g., observation, inquiry, inspection, interview data analysis) used to gather protect and preserve audit evidence.
6. Audit sampling methodologies.
7. Organizational structure, roles and responsibilities related to IT
8. Processes for the development, implementation and maintenance of IT strategy, policies, standards and procedures.
9. The use of maturity models.
10. Practices for monitoring and reporting of IT performance (e.g., balanced scorecards, key performance indicators [KPIs]).
11. Project governance mechanisms (e.g., steering committee, project oversight board, project management office).
12. Acquisition practices (e.g., evaluation of vendors, vendor management, escrow).
13. Control objectives and techniques that ensure the completeness, accuracy, validity and authorization of transactions and data.
14. System development methodologies and tools, including their strengths and weaknesses (e.g., agile development practices, prototyping, rapid application development [RAD]; object-oriented design techniques).
15. Testing methodologies and practices related to information systems development.
16. Configuration and release management relating to the development of information systems.
17. Techniques for monitoring third-party compliance with the organization's internal controls.
18. Operations and end-user procedures for managing scheduled and nonscheduled processes.
19. Control techniques that ensure the integrity of system interfaces.
20. Software licensing and inventory practices.
21. System resiliency tools and techniques (e.g., fault tolerant hardware, elimination of single point of failure, clustering).
22. Capacity planning and related monitoring tools and techniques.
23. Data backup, storage, maintenance, retention and restoration practices.
24. Processes related to monitoring and responding to security incidents (e.g., escalation procedures, emergency incident response team).
25. Security controls related to hardware, system software (e.g., applications, operating systems), and database management systems.
26. Risks and controls associated with virtualization of systems.
27. Network and Internet security devices, protocols and techniques.
28. Information system attack methods and techniques.
29. Security testing techniques (e.g., intrusion testing, vulnerability scanning).
30. Risks and controls associated with data leakage.
31. Risks and controls associated with peer-to-peer computing, instant messaging, and web-based technologies (e.g., social networking, message boards, blogs).
32. Controls and risks associated with the use of mobile and wireless devices.
33. The evidence preservation techniques and processes followed in forensics investigations (e.g., IT, process, chain of custody).
34. The processes and procedures used to store, retrieve, transport and dispose of confidential information assets.
35. Data backup, storage, maintenance, retention and restoration processes, and practices.
36. Regulatory, legal, contractual and insurance issues related to business continuity and disaster recovery.
38. The development and maintenance of the business continuity and disaster recovery plans.
39. Business continuity and disaster recovery testing approaches and methods.
40. Processes used to invoke the business continuity and disaster recovery plans.
41. Types of alternate processing sites and methods used to monitor the contractual agreements (e.g., hot sites, warm sites, cold sites).

Essay topics (examples)

1. Information Technology investment methodologies
2. A Real Option strategic decision for IT project selection
3. Customer-related IT investments.
4. Managerial decision-making about IT Investment
5. Efficiency enhancing effects of IT investment
6. A Risk Management approach to IT Services Contract design
7. IT Portfolio Selection methods
8. Economics of Information Technology Outsourcing
9. Information technology process improvement
10. The international economics of information technology

V. РЕСУРСЫ

Textbooks

Core reading

1. Грецул В.И. Аудит информационных технологий. М., Горячая линия-Телеком, 2015

Extended reading


Материально-техническое обеспечение дисциплины

Inventory and logistics support of discipline
Personal computer (laptop) and a projector are used for lectures and seminars. Technical equipment of computer classes may be used too.