Vysoká škola ekonomická v Praze

Fakulta informatiky a statistiky

Diplomová práce

2016 Tomáš Mišelnický

Vysoká škola ekonomická v Praze
Fakulta informatiky a statistiky

Data Analysis in the Internal Audit Department

Vypracoval: Bc. Tomáš Mišelnický
Vedoucí práce: doc. Ing. Vlasta Svatá, CSc.
Rok vypracování: 2016

Čestné prohlášení:

Prohlašuji, že jsem tuto bakalářskou práci vypracoval samostatně. Veškeré použité podklady, ze kterých jsem čerpal informace, jsou uvedeny v seznamu použité literatury a citovány v textu podle normy ČSN ISO 690.

V Praze dne 25.4.2016 Podpis: ....

Poděkování:

Rád bych poděkoval vedoucí mé diplomové práce paní doc. Ing. Vlastě Svaté, CSc. za její inspirující rady a značnou flexibilitu v průběhu zpracování práce.

Abstrakt:

Cílem této práce je představit návrh modelu pro lepší plánování interních auditů pobočkové sítě v bance. První část práce se zabývá interním auditem. Je zde představena a diskutována definice interního auditu podle Institute of Internal Auditors (IIA). Poté jsou představeny další relevantní disciplíny – externí audit a assurance. Důležitost těchto disciplín je demonstrována na příkladu společnosti Enron. Práce se dále věnuje frameworku International Professional Practices Framework, zejména pak jeho klíčové části – Standardům. Konec této části je věnován popisu jednotlivých částí projektu interního auditu. Druhá část práce je věnována plánováním projektů interních auditů. Plánování je postavené na rizicích a proto je zde uveden popis bankovních rizik. Závěr této části se věnuje postupu vytváření Annual Audit Plan. V závěrečné části této práce je představen model, vytvořený autorem této práce, který pomůže zlepšit plánování interních auditů pobočkové sítě bank.

Abstract:

The aim of this thesis is to present a draft model for better planning internal audit engagements of branch network of the bank. The first part deals with the internal audit. It presents and discusses the definition of internal auditing by the Institute of Internal Auditors (IIA). Other relevant disciplines are also included - external audit and assurance. The importance of these disciplines is demonstrated in the example of Enron. The thesis presents the International Professional Practices Framework, especially its key components - standards. The end of this section is devoted to a description of the individual parts of an internal audit project. The second part is dedicated to planning internal audit engagements. Planning is based on the risks, therefore, there is a description of banking risks. The conclusion of this section is devoted to the process of creating the Annual Audit Plan. The final part of this work presents a model created by the author which will help to improve the planning of internal audits of the branch network of banks.

Table of content

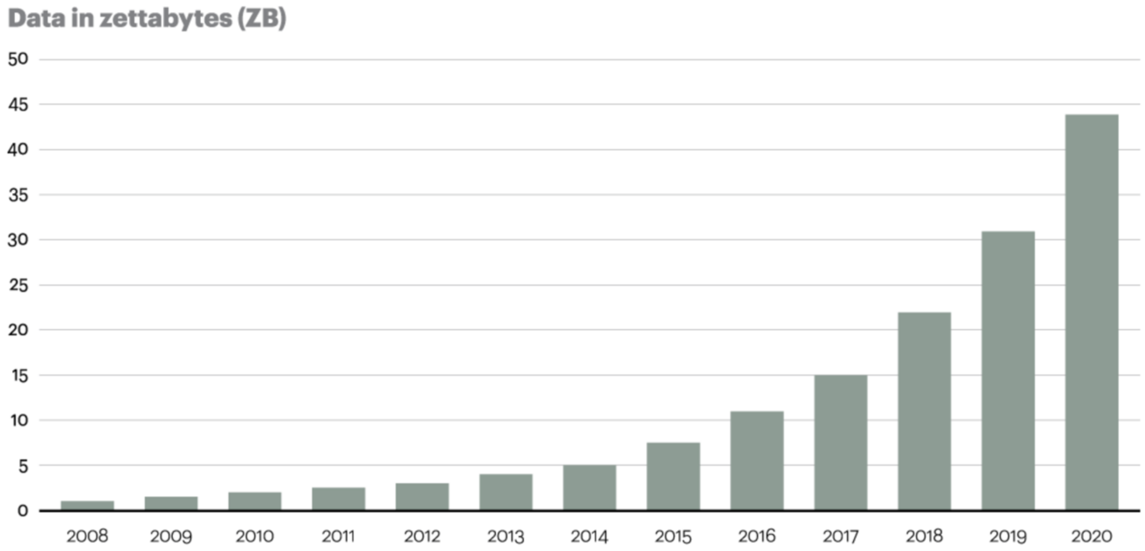
INTRODUCTION **2**
SCOPE 2
STRUCTURE 3
INTERNAL AUDIT **4**
DEFINITION 4
EXTERNAL AUDIT 8
OTHER ASSURANCE SERVICES 10
INSTITUTE OF INTERNAL AUDITORS 12
International Professional Practices Framework *13*
Global certifications *15*
Research and Education *16*
PHASES OF AN INTERNAL AUDIT ENGAGEMENT 16
Planning *17*
Fieldwork *22*
Reporting *25*
RISK-BASED AUDIT PLANNING **29**
PLANNING ENGAGEMENTS ACCORDING THE STANDARDS 29
Internal audit charter *29*
BANKING RISKS 30
ANNUAL AUDIT PLAN 32
MODEL **39**
INTRODUCTION 39
LIMITATIONS OF THE MODEL 40
CREATING A MODEL 40
CONTROLS 41
Sum of loans *42*
Closed accounts *43*
Customer satisfaction *44*
Opening hours *45*
Default on a loan *46*
SUMMARY REPORT 46
NEXT STEPS 47
CONCLUSION **48**
ABBREVIATIONS **49**
TABLE OF FIGURES **50**
RESOURCES **51**
LITERATURE, LAWS, NORMS 51
INTERNET RESOURCES 52
ATTACHMENTS **54**
ATTACHMENT 1 – A LIST OF SERVICES PERFORMED BY INTERNAL AUDIT. 54

Introduction

The title of the thesis is *Data Analysis in the Internal Audit Department*. Neither of the key words mentioned in the title – data, audit – are new. People have been recording, collecting and working with data for thousands of years. The history of auditing also dates back many generations in the past, all the way to some of the ancient civilizations.

When we think again about data, specifically in regards with the incredible capacities of current information technologies, we become overloaded with the unimaginable volume of this commodity. All the devices around us are constantly generating more and more data.

Figure 1 – Volume of data



Source: ATKearney, http://www.atkearney.cz/strategic-it/ideas-insights/article/-/asset_publisher/LCcgOeS4t85g/content/big-data-and-the-creative-destruction-of-today-s-business-models/10192

Figure 1 shows volume of data generated in individual years. We can see that there already is an incredible amount of data. The trend suggests that there will be even more very shortly. That is why this thesis was created. Its purpose is to show how data can be beneficial in the internal audit department.

Scope

It is easy to imagine many different fields and areas where data might be helpful, where it might bring much sought after competitive advantage. It would be impossible to cover all of them. Therefore, the scope of this thesis is to discuss how data can be beneficial for planning the internal audit engagements in the banking sector. It specifies on planning audit engagement with the branch network.

Structure

The thesis is divided into three parts – internal audit, risk-based audit planning and the model. The first part (internal audit) presents and discusses the definition of internal auditing by the Institute of Internal Auditors (IIA). All the key aspects of the definition are analyzed and different views of other authors and institutions are presented. Other related disciplines – external audit and assurance – and their differences are also discussed. The Institute of Internal Auditors is presented and special focus is given to the International Professional Practices Framework and especially the Standards. The last part of the chapter describes three phases of an internal audit engagement – planning, fieldwork and reporting. The second part is devoted to planning internal audit engagements. Planning is based on the risks, therefore, there is a description of banking risks. The conclusion of this section is dedicated to the process of creating the Annual Audit Plan. The last part of this thesis describes a model, created by the author, which will help to improve the planning of internal audits of the branch network of banks. It explains the process of how the model was created, lists limitations of the model and describes the individual aspects of the model.

Internal audit

Definition

The goal of this thesis is to discuss how data can be beneficial for planning internal audit projects. Internal audit is defined by the Institute of Internal Auditors (IAA) [1] as *"an independent, objective assurance and consulting activity designed to add value and improve an organization's operations."* The definition further states that the activity can help an organization to *"accomplish its objectives by bringing a systematic, disciplined approach to evaluate and improve the effectiveness of risk management, control, and governance processes."* [2]

Pickett[3] analyzed the definition and identified ten key concepts:

1. Independence
2. Assurance and consulting
3. Activity
4. Add value
5. Organization's operations
6. Organization's objectives
7. Systematic and disciplined approach
8. Evaluate and improve
9. Effectiveness
10. Risk management, control, and governance process

Independence

The International Federation of Accountants (IFAC)[4] distinguishes between two forms of independence.

- Independence of mind
- Independence in appearance

Independence of mind is defined as "the state of mind that permits the provision of an opinion without being affected by influences that compromise professional judgment, allowing an individual to act with integrity, and exercise objectivity and professional skepticism." [5]

Independence in appearance is defined as "the avoidance of facts and circumstances that are so significant a reasonable and informed third party, having knowledge of all relevant

[1] https://na.theiia.org/Pages/IIAHome.aspx

[2] IIA, https://na.theiia.org/standards-guidance/mandatory-guidance/Pages/Definition-of-Internal-Auditing.aspx

[3] Pickett, 2005, p. 109 - 111

[4] http://www.ifac.org

[5] Handbook of international quality control, auditing review, other assurance, and related services pronouncements, 2015, p. 16

information, including any safeguards applied, would reasonably conclude a firm's, or a member of the assurance team's, integrity, objectivity or professional skepticism had been compromised." [6]

Another view on the independence is presented by Pickett[7]. He specified seven conditions that must be fulfilled to be able to consider internal auditing independent.

1. Objectivity – appropriate procedures must be adopted to promote fair considerations
2. Impartiality – approach from the internal audit should be the same for everybody, regardless their status and influence
3. Unbiased views – auditors should not be affected by libels or their own preferences
4. Valid opinion – the outcome of the work must my made based on the evidence, not somebody's likings
5. No spying for management – auditors must behave in a professional manner and not be used just as a tool by management
6. No 'no-go' areas – auditors must be granted an access to all areas and employees that the need
7. Sensitive areas – auditor must be able to audit sensitive areas
8. Auditing senior management – auditors should not only focus on the operational aspects but audit the whole management
9. No backing-off – auditors should never quit their work when somebody, regardless of the position, shows displeasure

The key concepts are consistent in both views. The importance is given to professional opinion that is based on integrity and objectivity. An interesting notion presented by the IFAC is the *independence in appearance.* Following their suggestion, auditors should proactively avoid all influences, regardless of their form, that could compromise their judgment.

Some of the points from the Pickett's definition can be put together and characterized with one word *fearless*. Auditors should not choose projects based on difficulty, sensitivity or what their friends might like. They should be free from the influence of any third party. Once the work has begun, if there is any potentially important discovery, it should be examined regardless of what it might hurt.

We have established that the independence is a basic prerequisite for a meaningful function of the internal audit department. It should be specified in the company's bylaws and it must be enforced. It is important to stress out the second part of the sentence – to be enforced. It is a common situation that companies put a great effort to formulate their values but the employees, including the management, are only vaguely informed and nobody is making any effort to follow it. An example is a former company called Enron which will be described later and one of their key values – integrity. [8]

[6] Handbook of international quality control, auditing review, other assurance, and related services pronouncements, 2015, p. 16

[7] Pickett, 2005, p. 117 - 119

[8] McLean, Bethany, Elkind, 2013, p. 44

Assurance and consulting

The scope of internal audit activities is wider than what could be expected at first glance. Griffiths[9] distinguishes between three roles internal auditors have

- Policeman
- Risk assessor
- Consultant

The first role in the list *policeman* is a traditional view on the profession of internal auditing. The auditors are, as policeman do, keeping order in the company by evaluating the current state of processes and controls. It is a very common perception of the auditors. It is necessary but it definitely is not the only role they should play.

The second role *risk assessor* is becoming more common in the modern audit era. And it is good. Especially for banks, managing risks is a core activity and the auditors should be present in the process. Risk-based audit will be described in the second part of the thesis.

There is a broad list of activities which was compiled by Pickett[10]. It is presented as an Attachment 1.

Activity

Internal audit must be considered as an activity. In the context of modern companies, we can think of this activity as a defined service. The service can be ordered by another subject (department), for a specific price, with certain conditions and guarantees. There is also a possibility to outsource the service, however, local law and regulations must be abided.

Add value

Moeller[11] discusses the importance of adding value and improving effectiveness. He states that "Internal audit's role is not just to find *what is wrong* in an enterprise but to bring in some value through their recommendations." This is consistent with Griffiths' view, which was discussed above, where he characterized the three roles for internal audit – policeman, risk assessor and consultant.

Adding a value is the ultimate goal of internal audit. It should be derived from organization's objectives and reflected to organization's operations. As we discussed *independence* above, there should be no negative influence on planning internal audit projects.

Organization's operations and objectives

[9] Griffiths, 2005, p. 14

[10] Pickett, 2005, p. 115 - 117

[11] Moeller, 2008, p. 317

The purpose of an organization is to fulfill its objectives. After the objectives are defined and communicated, the internal audit department can help to fulfill them.

As we have described, the scope of internal audit is incredibly wide. Attachment 1 presents a list with some of the possible activities. Let us just highlight the three areas that are included in the definition of internal audit by the IIA - risk management, control, and governance processes.

Systematic and disciplined

Internal audit is not a random activity that is performed whenever there is time for it. To fully accomplish its objectives, it demands a systematic and disciplined approach. We will discuss later how to make an audit plan and how to perform an individual assignment.

Evaluate and improve

An auditor's work might be characterized as evaluating evidence and drawing conclusions. In addition to it, an auditor might also suggest how to make some improvements, if it is appropriate. Some details of the process will be discussed later.

Effectiveness

Cambridge online dictionary defines effectiveness as "the ability to be successful and produce the intended results" [12] The definition is well suited in the context of internal auditing as the purpose is to "evaluate and improve the effectiveness of risk management, control, and governance" [13]

Gray, Manson, Crawford[14] distinguish between efficiency auditing and effectiveness auditing. Efficiency auditing "determines whether resources are used optimally and within the bounds of what is feasible" while effectiveness auditing "determines whether resources are being used to proper effect."

The two terms are sometimes used interchangeably which is not correct as we have seen from the previous definitions.

Risk management, control and governance

Risk management, control and governance are the most important subjects of interest in internal auditing. They will be discussed later.

[12] Cambridge Online Dictionary, http://dictionary.cambridge.org/dictionary/english/effectiveness

[13] IIA, https://na.theiia.org/standards-guidance/mandatory-guidance/Pages/Definition-of-Internal-Auditing.aspx

[14] Gray, Manson, Crawford, 2015, p. 625 - 626

External audit

There are several related disciplines to internal audit. The closest one is external audit.

External audit is defined as a *"systematic process of objectively obtaining and evaluating evidence regarding assertions about economic actions and events to ascertain the degree of correspondence between those assertions and established criteria and communicating the results to interested users."* [15]

Rittenberg, Schwieger, Johnstone [16] analyze the definition and point out three essential parts.

- Auditors obtain and evaluate evidence
- Assertions and established criteria
- Communicating results to users

A different definition of external audit is provided by Gray, Manson, Crawford[17]. "An audit is an investigation or a search for evidence to enable reasonable assurance to be given on the truth and fairness of financial and other information by a person or persons independent of the preparer and persons likely to gain directly from the use of the information, and the issue of a report on the information with the intention of increasing its credibility and therefore its usefulness."

The essence of both definitions is very similar. Audit is defined as an *investigation* or *systematic process of gathering evidence* and it needs to be *objective* and *independent*. The Auditing Concepts Committee further enhanced the definition by *assertions* and *established criteria* while Gray, Manson, Crawford described in more detail the independence of the auditor from the person or persons that might benefit from the audit report.

External auditors play an important role in the modern society. The capital markets and their users – investors, companies, regulators – depend on accurate, reliable and objective information. When the demand is not met, it can have terrible consequences on the entire financial system. An example is the failure of Enron.

Enron

Enron was an American energy company that became a symbol of corporate fraud, misusing accounting standards and one of the biggest audit failures in history. The company used various unethical practices to hide losses on their balance sheet and overestimate earnings. Two of the them were mark-to-market accounting and special purpose entities (SPE).

Mark-to-market accounting was used to account for the long-term contracts. Income was estimated as the present value of future cash flows. It was difficult to objectively estimate the

[15] Auditing Concepts Committee, "Report of the Committee on Basic Auditing Concepts," The Accounting Review, 47, Supp. (1972), 18.
[16] Rittenberg, Schwieger, Johnstone, 2008, p. 5 - 7
[17] Gray, Manson, Crawford, 2015, p. 25

real values so the investors were typically given overestimated income and underestimated losses. The management was aware of that when they overestimated revenue in one year they had to come up with an even larger amount in the next one. It forced them to keep increasing the estimates until the situation was revealed. [18]

Special purpose entities (SPEs) were used by Enron to hide risks associated with their projects. A SPE was created to transfer the risks from Enron to the particular SPE. These SPEs appeared separately from Enron which created an illusion that risks were hedged by a third party while Enron is only realizing the income. Enron used thousands of SPEs to manipulate investors and stock price. [19]

These activities could not continue forever. Once the public became aware of Enron's practices, the stock price began to fall. From it's high of over $90 it was trading for less than a dollar several months after. The company declared bankruptcy shortly after.

To ensure the overall stability of the entire financial system and eliminate any future failures, such as Enron's, the audit must:

- Perform test on the financial statements to determine if they are accurate
- Make judgments about the fairness of complex accounting process
- Evaluate and test the organization's system of internal controls
- Do all the above in an objective, unbiased and professionally skeptical manner [20]

Differences between internal and external audit

The Chartered Institute of Internal Auditors[21] characterized the difference between internal and external audit in four key areas[22].

- Users of reports
- Objectives
- Coverage
- Responsibility for improvement

Users of external audit reports are typically shareholders, if the organization is listed on the stock market, or other parties outside of the organization's governance. Internal audit reports are aimed for the management of the company or the Board.

Previously shown definition of external audit by Gray, Manson, Crawford specified that the objective of external audit is *to enable reasonable assurance on the truth and fairness of*

[18] Bethany, McLean, Elkind, 2013, p. 167 - 175
[19] Bethany, McLean, Elkind, 2013, p. 495 - 497
[20] Rittenberg, Schwieger, Johnstone, 2008, p. 3
[21] https://www.iia.org.uk
[22] The Chartered Institute of Internal Auditors, https://www.iia.org.uk/about-us/what-is-internal-audit/

financial information. Objective of internal audit, according to the IIA, is *to evaluate and improve the effectiveness of risk management, control, and governance.*

External audit covers primarily financial reports and related financial risks. Internal audit may cover various kinds of risks, such as operational, market etc.

External auditors are not responsible for any improvement, however, they are obligated to report all appropriate findings. Improvement is a fundamental concept for internal auditors as their primary objective is to *add value*. Internal auditors make suggestions and recommendations but the ultimate responsibility for any changes is on the management.

Other assurance services

Audit, both internal and external, is a part of much broader concept – assurance. The American Institute of Certified Public Accountants (AICPA)[23] defines the purpose of assurance as *"to provide a service that increases confidence in the information, the independent professional providing it has to engender trust, not only as a provider of the service but also in the process the professional uses to deliver it."* [24]

ISACA[25] defines assurance as "Pursuant to an accountable relationship between two or more parties, an IT audit and assurance professional is engaged to issue a written communication expressing a conclusion about the subject matters for which the accountable party is responsible. Assurance refers to a number of related activities designed to provide the reader or user of the report with a level of assurance or comfort over the subject matter." [26]

The definition from ISACA can be explained using an illustration of an assurance initiative provided as Figure 2. The illustration shows that assurance consists of five key components.

- Three-party relationship
- Subject matter
- Suitable criteria
- Execution
- Conclusion

The three-party relationship is a relationship between an assurance professional, an accountable party and a user. The assurance professional performs the assurance process and is responsible for it. The Accountable party governs and manages the process and is ultimately responsible for the subject matter. The user benefits from the process by being provided with a conclusion about the subject matter.

[23] http://www.aicpa.org/Pages/default.aspx
[24] AICPA Assurance Services: A White Paper for Providers and Users of Business Information, http://www.aicpa.org/InterestAreas/FRC/AssuranceAdvisoryServices/DownloadableDocuments/ASEC_WP_Providers_Users_BI.PDF
[25] https://www.isaca.org/Pages/default.aspx
[26] ISACA, http://www.isaca.org/Pages/Glossary.aspx?tid=1087&char=A

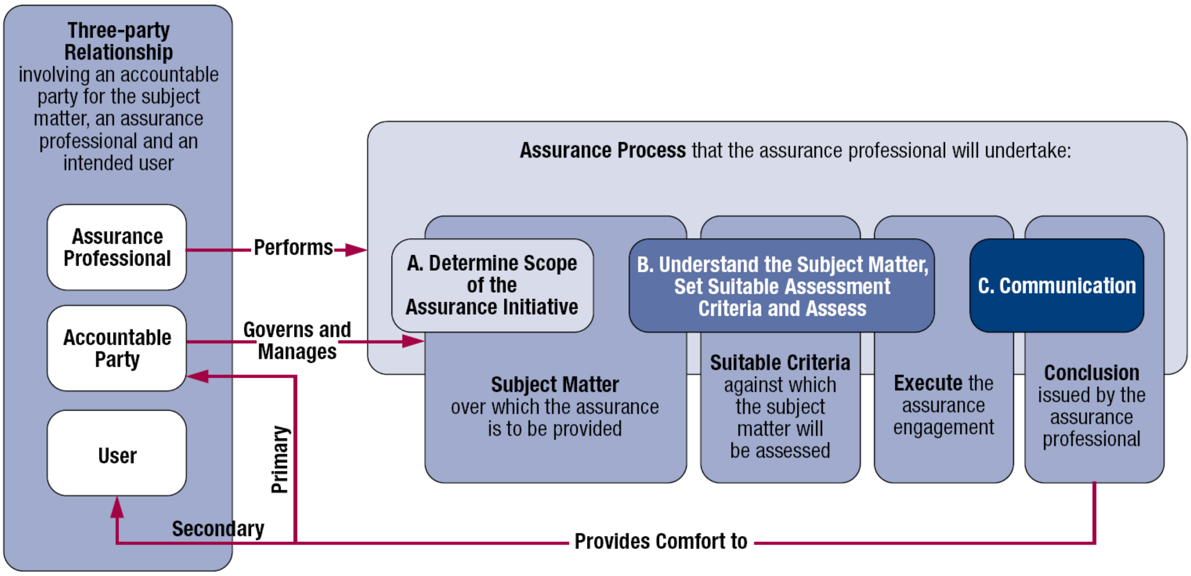
The subject matter is a subject on which the assurance process performed and the assurance is provided. The scope of assurance engagements could be wide. Some examples are provided by ISACA "support for audited financial statements; assessment of value provided by IT to the enterprise; reviews of controls; compliance with required standards and practices; and compliance with agreements, licenses, legislation and regulations." [27]

Suitable criteria are standards and benchmarks against which the subject matter is evaluated. There could be a different set of criteria for the same subject matter. The criteria could be some of the international standards (such as COBIT or ITIL) or they could be internally developed within an organization.

After the scope of the assurance initiative has been defined and suitable criteria have been set, the assessment process may begin. In its essence it is about gathering and evaluating evidence against identified suitable criteria.

The output of the process is a conclusion. The conclusion in the form of the report is delivered to the user and the accountable party.

Figure 2: An assurance initiative (ISACA)


Three-party Relationship involving an accountable party for the subject matter, an assurance professional and an intended user
Assurance Professional
Accountable Party
User
Performs
Governs and Manages
Primary
Secondary
Provides Comfort to
Assurance Process that the assurance professional will undertake:
A. Determine Scope of the Assurance Initiative
B. Understand the Subject Matter, Set Suitable Assessment Criteria and Assess
C. Communication
Subject Matter over which the assurance is to be provided
Suitable Criteria against which the subject matter will be assessed
Execute the assurance engagement
Conclusion issued by the assurance professional

Source: ISACA, http://www.isaca.org/Knowledge-Center/cobit/cobit-focus/Pages/COBIT-Focus-Volume-3-July-2013.aspx

Rittenberg, Schwieger and Johnstone[28] define assurance services as a relationship between three components:

- Information or processes intended to be assessed
- A user or a group of users interested in the output of the assessment
- An assurance service provider

[27] ISACA, http://www.isaca.org/Knowledge-Center/cobit/cobit-focus/Pages/COBIT-Focus-Volume-3-July-2013.aspx

[28] Rittenberg, Schwieger, Johnstone, 2008, p. 14

The definition from Rittenberg, Schwieger and Johnstone is a simplified version of the ISACA's version. It only contains two of its components the *subject matter* and the *three-party relationship*.

ISACA distinguishes between three types of assurance services.

- Audit
- Review
- Agreed-upon procedures

An analysis of these terms, especially the differences, is provided in ITAF[29] [30]

An audit provides the highest level of assurance about the effectiveness of control procedures. A review provides a moderate level of assurance. It is due to limitations in quantity of work and available time. An agreed-upon procedure does not provide the expression with any level of assurance. It is a procedure to gather specific information that was requested by the parties that have agreed on it.

Institute of Internal Auditors

The Institute of Internal Auditors is a professional organization that connect experts from all over the world. The members of the organization are not only internal auditors but they are professionals from various backgrounds, typically internal audit, governance, risk management and other related fields. The organization was established in 1941 in the USA. Nowadays, it has more the 180,000 members. [31]

The purpose of the organization is characterized in its mission statement: "The mission of The Institute of Internal Auditors is to provide dynamic leadership for the global profession of internal auditing." [32]

The organization has identified five key activities to support the mission statement:

- Advocating and promotion the value that internal auditors bring to their organization
- Providing guidance, standards, education, recommendations, and certification for internal auditors
- Doing research and further promoting knowledge in the field of internal auditing
- Education all interested subjects on best practices in internal auditing
- Connecting internal auditors from all over the word to share knowledge and experiences

[29] ITAF: A Professional Practices Framework for IS Audit/Assurance, 2nd edition, p. 86 - 87

[30] The framework has been revised in 2014 and ISACA published the 3rd edition. However, the definitions are not provided and are referenced back to the 2nd edition.

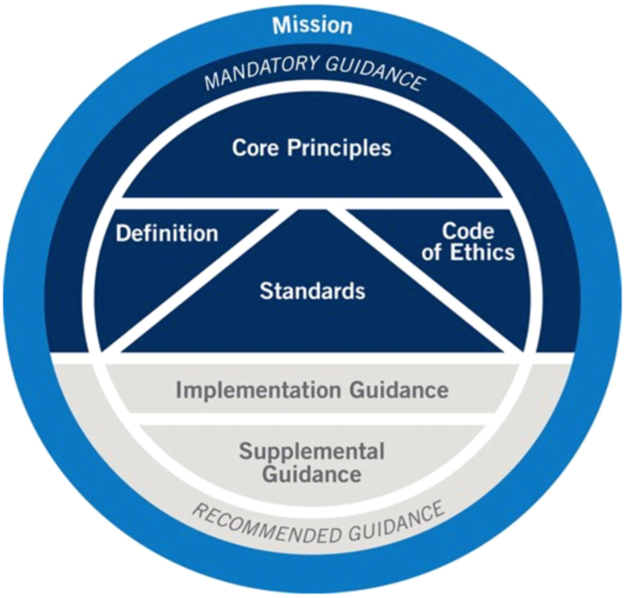
[31] IIA, https://na.theiia.org/about-us/Pages/About-The-Institute-of-Internal-Auditors.aspx

[32] IIA, https://na.theiia.org/about-us/Pages/About-The-Institute-of-Internal-Auditors.aspx

International Professional Practices Framework

In 2015, the IIA Board of Directors has approved and published the International Professional Practices Framework (IPPF). The Framework provides guidance for internal audit professionals all over the world. The key concepts of the IPPF are presented as Figure 3.

Figure 3 - IPPF



Source: IIA, https://na.theiia.org/standards-guidance/Pages/Standards-and-Guidance-IPPF.aspx

The Framework is divided into two parts – mandatory guidance (dark blue color) and recommended guidance (grey color). Both parts are connected with one overarching element – the mission (light blue color).

The IIA defines the mission of internal audit as "enhance and protect organizational value by providing risk-based and objective assurance, advice, and insight." [33]

The mandatory elements (guidance) are: [34]

- Core Principles for the Professional Practice of Internal Auditing
- Definition of Internal Auditing
- Code of Ethics
- International Standards for the Professional Practice of Internal Auditing

The recommended elements (guidance) are:

- Implementation Guidance
- Supplemental Guidance

[33] IIA, https://na.theiia.org/standards-guidance/Pages/Mission-of-Internal-Audit.aspx

[34] IIA, https://na.theiia.org/standards-guidance/Pages/Standards-and-Guidance-IPPF.aspx#mandatory

Core principles

The IAA has defined the following ten core principles that should ensure the effectiveness of internal auditing. It is worth mentioning that just following all of the principles does not automatically mean that the internal audit is operating at its full potential. Each country and each organization might have its own specifics that should be reflected.

1. Demonstrates integrity.
2. Demonstrates competence and due professional care.
3. Is objective and independent
4. Aligns with the strategies, objectives, and risks of the organization.
5. Is appropriately positioned and adequately resourced.
6. Demonstrates quality and continuous improvement.
7. Communicates effectively.
8. Provides risk-based assurance.
9. Is insightful, proactive, and future-focused.
10. Promotes organizational improvement. [35]

Code of Ethics

The Code of Ethics prescribes the behavior that is expected from individuals and organizations while performing internal audit. It further enhances the definitions of internal audit. All the recipients of the IIA certifications are required to follow the Code of Ethics and others are encouraged. The Code of Ethics might not include all necessary elements appropriate for a particular country or a company. Therefore, it should always be evaluated and modified if required. It includes four principles and the rules of conduct specifying how to apply those principles.

1. Integrity
2. Objectivity
3. Confidentiality
4. Competency[36]

Standards

The International Standards for the Professional Practice of Internal Auditing (Standards) were published in 2008 by IIA (revised in 2012).

The purpose of the Standards is to:

1. Define basic principles of internal auditing.

[35] IIA, https://na.theiia.org/standards-guidance/mandatory-guidance/Pages/Core-Principles-for-the-Professional-Practice-of-Internal-Auditing.aspx

[36] IIA, https://na.theiia.org/standards-guidance/mandatory-guidance/Pages/Code-of-Ethics.aspx

2. Provide a framework value-added services of internal auditing.
3. Enable the evaluation of internal audit performance.
4. Nurture processes and operations within the organization.

The Standards are divided into two parts. The first part – Attributes – contains characteristics applicable to subjects who perform internal auditing. The second part – Performance Standards – explains the nature of internal auditing and provides criteria for evaluation of internal audit performance. Information about recommended implementation steps are provided in both parts.

Attribute standards are:

- 1000 – Purpose, Authority, and Responsibility
- 1100 – Independence and Objectivity
- 1130 – impairment to Independence and Objectivity
- 1200 – Proficiency and Due Professional Care
- 1300 – Quality Assurance and Improvement Program

Performance standards are:

- 2000 – Managing the Internal Audit Activity
- 2100 – Nature of Work
- 2200 – Engagement Planning
- 2300 – Performing the Engagement
- 2400 – Communicating Results
- 2500 – Monitoring Progress
- 2600 – Communicating the Acceptance of Risks

The Standards identify five main elements that can be characterized as the scope of internal auditing:

1. Achievement of the organization's strategic objectives
2. Reliability and integrity of financial and operational information
3. Effectiveness and efficiency of operations and programs
4. Safeguarding of assets
5. Compliance with laws, regulations, policies, procedures, and contracts

Implementation and Supplemental Guidance

There are various publications available for the IIA members regarding implementation and conducting internal audit activities.

Global certifications

Another activity of the IIA is providing internationally acceptable certifications. There are various benefits that come with a certification. The person who has been awarded an IIA certification gains credibility in a respective field. That could translate to an increase in salary or new job offers. The certificate guarantees that the candidate possesses a certain level of knowledge and skills which assures an employer of his/her abilities.

The IIA is currently offering seven certifications:

- Certified Internal Auditor (CIA)
- Certified Government Auditing Professional (CGAP)
- Certified Financial Services Auditor (CFSA)
- Certification in Control Self-assessment (CCSA)
- Certification in Risk Management Assurances (CRMA)
- Qualification in Internal Audit Leadership (QIAL)
- Certification for Environmental, Health and Safety Auditors (BEAC) [37]

Research and Education

The IIA has established the IIA Research Foundation (IIARF) that is a nonprofit organization responsible for research activities on behalf of the IIA. The IIARF facilitate research in areas of internal auditing, governance, controls, fraud detection, security and many others. It has published over 200 research reports. [38]

The IIA provides professional education in various forms – public seminars, online courses, workshops and many others. The IIA also partners with universities providing solid foundation for the students. [39]

Phases of an internal audit engagement

According to Russell[40], there are seven phases of internal audit.

1. Audit assignment
2. Prepare
3. Evaluate documents
4. Begin the internal audit
5. Perform
6. Analyze and finish
7. Follow-up and closure

There are many other views on how the phases of internal audit should be named and in which level of detail they should be presented. For example, Moeller[41] provides a more expanded list with twelve steps of the process.

1. Perform risk analysis to identify potential control risks

[37] IIA, https://na.theiia.org/certification/Pages/Certification.aspx
[38] IIA, https://na.theiia.org/about-us/Public%20Documents/IIA%20Brochure.pdf
[39] IIA, https://na.theiia.org/about-us/Public%20Documents/IIA%20Brochure.pdf
[40] Russell, 2007, p. 14
[41] Moeller, 2009, p. 181

2. Develop audit plan
3. Schedule internal audit and allocate resources
4. Review any past audit reports and workpapers
5. Visit site and perform field survey
6. Prepare audit programs
7. Prepare and deliver engagement letter
8. Begin internal audit fieldwork
9. Document processes and perform planned procedures
10. Develop audit point sheets covering preliminary findings
11. Complete audit documentation
12. Complete fieldwork and review proposed findings with auditee

Another example is presented by the Office of Internal Audit from Wayne State University[42]. The Office only names three phases of the process and provides a list of activities for each phase.

1. Planning
2. Fieldwork
3. Reporting

In the following text we will discuss the content of the individual phases of internal audit using the Office of Internal Audit from Wayne State University's proposed convention.

Planning

Purpose of planning

The overall objective of internal audit is to support risk management, controls and assurance processes in an organization. While the general purpose is still the same, the individual audits will differ greatly in all possible details. For that reason, each internal audit must be carefully planned to ensure that the project fulfills its objectives and runs smoothly and effectively.

Pitt[43] suggests that spending time on planning will help internal auditors in the following ways.

- Obtain a comprehensive understanding of the operations and activities
- Ensure alignment between internal audit engagements, the annual audit plan, and the annual audit charter
- Confirm alignment between the internal audit function and other assurance activities
- Confirm that engagement fieldwork is compliant with the internal audit function's policies and procedures
- Maximize the potential to address the engagement objectives

There are several terms that have not yet been specified.

[42] Office of Internal Audit, Wayne State University, http://internalaudit.wayne.edu/process.php
[43] Pitt, 2014, p. 225

Annual audit plan is a plan of all scheduled internal audits in a specific year.

Audit charter is "a formal written document that defines the purpose, authority, and responsibility of the Internal Auditing Office. The Charter establishes the Internal Audit Office's position within the organization; authorizes access to records, personnel, and physical properties relevant to the performance of engagements; and defines the scope of work." [44]

Internal audit function, in this context, represents the internal audit department.

Audit triggers

Moeller[45] describes three triggers which could cause the start of an internal audit engagement.

- Scheduled engagement based on internal audit annual plan
- Special request from the management
- Response to an unplanned event

Internal audit engagements may start according to the schedule specified in the internal audit annual plan. This is the most typical trigger. We will discuss the plan and the process of how to create the plan later.

Special request from the management could be made if there is a situation that needs to be dealt with. Typically, it would be a suspicion of a fraud or other negative activity.

Audit engagement may also start as a response to an unplanned event. An example could be negative business results.

Planning according to the Standards

The need for a plan is specified in the Standard 2200 – Engagement planning[46]. "Internal auditors must develop and document a plan for each engagement, including the engagement's objectives, scope, timing, and resource allocations."

Following Standards provide further guidance on the planning process.

Standard 2201 – Planning Considerations provides a list of items that should be considered by internal auditors in the planning process.

- Objectives of the activity being review
- Significant risks

[44] Austin Community College, http://www.austincc.edu/audit/documents/AuditCharter091103.pdf
[45] Moeller, 2009, p. 154 - 155
[46] International Standards for the Professional Practice of Internal Auditing, 2012, IIA

- Adequacy and effectiveness of the activity’s governance, risk management, and control processes
- Opportunities for making significant improvements to the governance, risk management, and control processes

Standard 2210 – Engagement Objectives requires that objectives must be established for each assessment. Engagement objectives must be based on a preliminary assessment of relevant risks. Auditors must always consider the possibility of error, fraud, noncompliance and other exposures.

Standard 2220 – Engagement Scope mandates that the established scope must be sufficient to the objectives of the engagement. The scope must also include consideration of relevant systems, records, personnel and physical properties.

Standard 2230 – Engagement Resource Allocation requires that sufficient resources must be allocated based on the complexity of each engagement.

Standard 2240 – Engagement Work Program states that internal auditors must develop and document work programs that achieve the engagement objectives. Work programs must contain procedures for identifying, analyzing, evaluating, and documenting information during the engagement.

In other words, work program is a manual on how to conduct the particular engagement. It includes a detailed plan of work and all the necessary steps that must be taken to achieve the engagements’ objectives.

Rife[47] discusses the work program and highlights what a successful work program should do.

- Provide an outline of the work
- Assist in controlling work
- Keep a record of completed work
- Encourage a thorough understanding of the audited unit
- Prove that an adequate plan has been made
- Assure that all relevant risk areas have been considered and addressed
- Give coherence to the audit

He suggests that the work program should be written in a way that even an inexperienced auditor is able to perform the steps. However, it should encourage critical thinking so that the auditors will use appropriate judgement rather than blindly following the prescribed steps.

The work program should be prepared before the fieldwork starts. It should be approved by the CAE or other appropriate party. If necessary, the plan can be modified during the fieldwork, however, the changes have to be approved.

[47] Randal Rife, Planning for Success, 2006, https://iaonline.theiia.org/planning-for-success

Moeller's views on planning

Moeller[48] discusses three topics that should be covered during internal audit preparatory stage.

1. Determining the audit objectives
2. Scheduling an audit engagement
3. Preliminary surveys

Each internal audit must be characterized with a high-level statement about its objectives. The purpose of the statement is to clearly articulate the ultimate goal of the engagement. It does not have to be too detailed but it should have sufficient information so the auditee and other relevant parties understand the purpose of the project. The statement should convince them about the importance of it.

Each individual audit should be scheduled based on the objectives, scope and availability of auditors. The number of auditors and their allocation is based on the nature and complexity of audit projects. The engagement should be broken down into individual tasks which should be assigned to the auditors. Auditor's skills and knowledge are to be reflected in the assignment.

Moeller[49] also distinguishes between four kinds of preliminary surveys. They are particularly valuable if the area to be audited (the subject matter) has previously been reviewed.

- Prior work papers
- Prior audit reports
- Organization chart
- Other related materials

Audit objectives, scope, workpapers, programs and other relevant documents should be reviewed prior to the start of a new engagement. It will enable auditors to quickly familiarize themselves with approaches used in the past. An analysis might reveal their strengths, weaknesses and possibly even some opportunities for future improvement. Prior workpapers will also help with time estimates for the particular audit engagement.

If the area has previously been reviewed, the auditors should also look into the report of the project. Significant findings and their consequences should be carefully reviewed and considered prior to the start of the new project. The findings might shape the structure of the project as some particular areas may need special attention. If the last project resulted with recommendations for the management or their commitments, the results should also be evaluated.

It is recommended to obtain the organization chart of the audited entity and became familiarized with its structure. In addition to this, the auditor should understand its function

[48] Moeller, 2009, p. 157 - 159
[49] Moeller, 2009, p. 159 - 160

and purpose. It is also helpful to have some general understanding of the activities of the entity.

Along with all the sources mentioned above, there could be some other relevant materials. The sources of such information could be wide, for example the literature, news articles, surveys etc.

Audit program[50] is the guide that should walk the auditors through the assignment. It specifies how the particular procedures should be made and which techniques should be used.

Picket's view on planning

Picket[51] identified nine key factors that should be considered during the planning phase.

- The terms of reference
- The scope of work
- Target dates
- A full definition of the system under review
- High risk areas
- Reporting and review arrangements
- Audit program
- Travel arrangements
- Staff

The terms of reference are the initial document that is delivered to the client. The document describes key characteristics of the project – scope, objectives, time frame, requirements etc. The document should explain the project and promote it to the client.

The scope of work should cover all areas that will be audited but it should also specify those that will not be audited at this time.

A timeline of the project is to be included in the initial documentation. All projects should be characterized with at least a start date and completion date. Larger projects may be divided into separate stages. Each individual stage has its own start date and completion date.

A full definition of the system (the subject matter) is recommended to be made. Having the description enables better understanding of the subject matter, specifically, where it starts, ends, and how it interacts with other elements in the organizations.

Understanding high risk areas and other critical elements of the system could be and very often it is the deciding factor of the engagement. A need for this activity is also specified in the Standard 2201.

[50] A different terminology is used in the Standard 2240. The Standards prefer 'Audit work program'.
[51] Pickett, 2005, p. 215 - 217

Reporting and review arrangements together with travelling and hotel arrangements is to be done to cover the necessary logistics.

Individual auditors should be assigned to the project (or its part) with a specific role. The assignment should reflect their skills and knowledge.

Russell's views on planning

Russell[52] says that the first phase of an internal audit engagement is delivering and agreeing on the audit assignment. The assignment should specify five key elements: who, what, when, where, and why (sometimes called 5 Ws).

Firstly, the audit assignment should specify who is responsible for the audit. The person is called the lead auditor. In addition to the lead auditor, there could also be some other senior and junior auditors participating on the project. The person who has ordered the particular internal audit project is the client. The client needs to possess the authority to make such a call. The last party specified in the assignment is somebody that is being audited – the auditee.

The next elements specify what, when and where is going to be audited. The subject matter of the audit must be provided. It is also beneficial to provide a more detailed description of the system to be audited as it clarifies the assignment and prevents from potential misunderstanding. An expected timeline and location of the project and should be provided as it helps the client to make suitable arrangements.

The last element to be specified in the audit engagement is the *why*. We have already discussed its importance in regards to the overall audit objective *to add value*.

Fieldwork

After the thorough preparation has been made and the engagement letter has been received by the auditee, it is time to start the fieldwork. There could be various approaches on how to perform the conduct, and some of them will be discussed later, but in its essence the fieldwork is about following the agreed engagement plan while utilizing the audit work program.

Fieldwork in the Standards

Fieldwork is captured in the *Standard 2300 – Performing the Engagement*[53]. It says that "Internal auditors must identify, analyze, evaluate, and document sufficient information to achieve the engagement's objectives."

Standard 2310 – Identifying Information requires auditors to identify sufficient, reliable, relevant and useful information to achieve the objectives.

[52] Russell, 2007, p. 13

[53] International Standards for the Professional Practice of Internal Auditing, 2012, IIA

- *Sufficient* is defined as "factual, adequate, and convincing so that a prudent, informed person would reach the same conclusions as the auditor."
- *Reliable* as "the best attainable information through the use of appropriate engagement techniques."
- *Relevant* as "information that supports engagement observations and recommendations and is consistent with the objectives for the engagement."
- *Useful* as "information that helps the organization meet its goals."

Standard 2320 – Analysis and Evaluation simply states that conclusions must be based on appropriate analysis and evaluation.

Standard 2330 – Documenting Information requires auditors to document relevant information which was used to make conclusions. CAE is responsible for such records and must develop and control policies governing the access and storage.

Standard 2340 – Engagement Supervision states that all engagements must be properly supervised.

Opening meeting

Russell[54] recommends to start the fieldwork phase with an opening meeting. The purpose of the meeting is to formally start the project, introduce the lead auditor and his/her colleagues, describe the project, and make connections with the auditee' staff. The agenda of the meeting is typically prepared and delivered by the lead auditor. A typical opening meeting agenda might look like this:

1. Introduce everybody on the audit team
2. Thank the person who made arrangements for the audit
3. Briefly review the plan – especially the objectives, scope, methods and timeline
4. Explain the outputs of the project
5. Confirm the availability of required staff members
6. Confirm logistics – meeting rooms, offices
7. Set up and explain the exit meeting

Characteristics for Evidence

The fieldwork phase is fundamentally about gathering and evaluating evidence. The Standard 2310 specifies some basic requirements for information (evidence) - sufficient, reliable, relevant and useful. Pitt[55] expands the basic requirements and defines other characteristics for audit evidence.

- Credible, authoritative, and accurate and fairly represents a particular condition
- The source is independent from the client
- In its original form

[54] Russell, 2007, p. 67 - 70

[55] Pitt, 2004, p. 249 - 250

- Documentation is available to support testimonial evidence
- Obtained through direct observation

An interesting concept regarding evidence is presented by Vona[56] as Trier of Fact. He defines the trier of fact as "the person or group of people who will read the fraud audit report, both the opinions and fact and circumstances, and then make a determination as to the next course of action." In regards to trier of fact, there are five evidence questions.

- Sufficiency: Measure of quantity
- Competency: Measure of quality
- Authenticity: The genuineness of the evidence
- Admissibility: The quality or state of being allowed to be entered into evidence in the legal arena
- Weight of Evidence: The evaluative significance assigned by the trier of fact

Pitt's characteristics for audit evidence are definitely helpful in regards with quality of obtained information. The problem is that they are too strict and so a lot of potentially interesting pieces of evidence would not be considered. Vona's characteristics could be helpful in this case because they are not too limiting but in the same time capture the essence.

Sources of Evidence

There could be various sources available for auditors to gather evidence. Russell[57] describes four basic categories:

- Documents and records
- Physical examination
- Observing
- Interviewing

The major sources of factual evidence are documents and record. They could be both in physical or electronic format. Documents typically describe how the subject matter should function, its connection to other elements and who is responsible. Therefore, it is important to check whether the reality corresponds to the documented state. Another good source of factual evidence are records. The advantage of using records is that they are usually correct. It is rather difficult to falsify them as the control mechanisms should be in place to prevent such behavior. Falsifying records can be a criminal act which might bring severe penalties. Although falsifying records might be difficult, it is important to evaluate the control mechanisms and look for potential weaknesses in the system.

Physical examination is an excellent source of evidence as the information gathered from it are typically objective. It will require more work from the audit team because the examination should be performed by them. There is a possibility for the auditors to ask the auditee staff

[56] Vona, 2011, p. 104
[57] Russell, 2007, p. 78

for their cooperation, especially if there are circumstances that prevents auditors from doing so.

A different way to collect the factual evidence is to observe the system. It requires sufficient skills and knowledge as without deep understanding of the system it might be difficult to recognize potential weaknesses that should be addressed.

Interviewing is the last method of getting evidence and it is also the most challenging one. It requires substantial skills from the auditor. To get expected results, an interview must be conducted in a professional manner. There are different methods how to conduct an interview and most auditors have their own preference.

The European Court of Auditors[58] published a document[59] providing guidelines on how to conduct a successful interview. It is divided into three parts. The first part specifies three purposes an interview might have – confirmation, examination and orientation – and characterizes two types of interview – structured and unstructured. The second part describes usage of an interview in the planning phase and also in the execution phase. The last part advises on how to conduct a successful interview.

The Guideline emphasizes the importance of preparation. The auditor must have a clear understanding of the purpose of the interview. It is also helpful to develop an interview guide. The interview should be scheduled ahead and so giving the auditor sufficient time to prepare. The interview should be opened by thanking the interviewee for participating and explaining the purpose. It must be conducted in a professional matter.

Analyzing evidence

After the evidence has been collected, it is time to analyze it. The methods of analysis differ greatly based on the type, quantity and quality of evidence. Some examples are data-mining, root cause analysis or statistical sampling. Fundamentally, it is about comparing the current state with expected. The expected result can be obtained from regulations, norms, standards, manuals etc. Any activity performed with a piece of evidence must be carried out in a way that is traceable and could be repeated by a different auditor. All the evidence and related material examined during the fieldwork or taken for later examination should be logged.

Reporting

The first phase of an audit project has dealt with how to prepare for the engagement. After the preparation, the second phases showed how to perform the fieldwork. Now, all there is left is to communicate the results.

Reporting in the Standards

[58] http://www.eca.europa.eu/en/Pages/ecadefault.aspx

[59] Guidelines on Audit Interview, 2013, European Court of Auditors

Reporting results is the topic of the *Standard 2400 – Communicating Results*[60]*.* It demands that "Internal auditors must communicate the results of engagements."

Standard 2410 – Criteria for Communicating prescribes that the engagement's objectives, scope, conclusions, recommendations, and actions plans must be communicated. If it is appropriate, the communication should also include auditor's opinion and conclusions. Satisfactory performance is encouraged to be acknowledged. Any communication outside the organization should include limitations on distribution.

Standard 2420 – Quality of Communications requires communication to be accurate, objective, clear, concise, constructive, complete, and timely.

- *Accurate* is defined as "free from errors and distortions and are faithful to the underlying facts."
- *Objective* as "fair, impartial, and unbiased and are the result of a fair-minded and balanced assessment of all relevant facts and circumstances."
- *Clear* as "easily understood and logical, avoiding unnecessary technical language and providing all significant and relevant information."
- *Concise* as "to the point and avoid unnecessary elaboration, superfluous detail, redundancy, and wordiness."
- *Constructive* as "helpful to the engagement client and the organization and lead to improvements where needed."
- *Complete* as "lack nothing that is essential to the target audience and include all significant and relevant information and observations to support recommendations and conclusions."
- *Timely* as "opportune and expedient, depending on the significance of the issue, allowing management to take appropriate corrective action."

Standard 2430 – Use of "Conducted in Conformance with the International Standards for the Professional Practice of Internal Auditing" specifies that the statement in the parenthesis may only be included in the report if the results of the quality assurance and improvement program support the statement.

Standard 2431 – Engagement Disclosure of Nonconformance specifies that if there are nonconformance with the Definition of Internal Auditing, the Code of Ethics or the Standards, the communication must disclose the respective document, reason for nonconformance and its impact.

Standard 2440 – Disseminating Results requires from the the chief audit executive to communicate results to the appropriate parties.

Standard 2450 – Overall Opinions specifies that if an overall opinion is issued, it must take into account the expectations of senior management, the board, and other stakeholders. The opinion must be supported by sufficient, reliable, relevant, and useful information.

[60] International Standards for the Professional Practice of Internal Auditing, 2012, IIA

Audit report

The audit report summarizes the results of the fieldwork. It is essential for the report to be created in a professional manner as it might be the only artifact that is received by the management. Therefore, it must present the conclusions in such way that the management understands the issues and takes appropriate actions. It should be created and delivered as soon as possible because some of the issues might require an immediate action.

Kagermann[61] describes three elements that are essential for most audit reports.

- Implementation report
- Management summary
- Board summary

The implementation report describes observations and findings that were made during the fieldwork. It is primary targeted for the operational management and so it should be presented from an operational perspective. The report should also include recommendations. It is helpful to provide both views. The first one describes how the situation looks like now (as-is) and the second one, how could the situation look like if the recommendations were implemented (to-be).

The management summary provides an aggregated version of the implementation report. The purpose of the summary is to present, in a compact form, the findings and their consequences to the management. The auditors should point out the relationships between individual findings.

The Board summary presents all relevant finding as well as the overall assessment of the audit to a respective Board member. The findings should be ordered by importance.

Pitt[62] provides a more detailed list of the elements that should be included in the report.

- Data of report
- Timeframe of the engagement
- Executive summary
- Engagement objectives and scope
- Findings and observations
- Recommended or agreed management actions
- Conclusion(s) and opinion(s)
- Appendices

There are many other views on what the format and the content of the report should be. For example, Russell[63] presents a generic template of the report which includes the following elements.

[61] Kagermann, 2008, p. 251 - 253

[62] Pitt, 2014, p. 277 - 280

[63] Russell, 2007, p. 130 - 131

- Audit report identification – date, title, number
- Confidential classification – classification of confidentiality based on the entity’s guidelines
- Introduction – purpose, scope, timeline, standards, audited areas, client and the audit team members
- Limitations – limitations of audit
- Conclusion – overall assessment of the audit
- Noteworthy achievement – good things found
- Detailed audit results – details of the findings
- Improvement points
- Identification of the lead auditor and his/her signature

The audit report is usually created using the company template. The template should include the elements discussed above. We would recommend to use the Russell’s template and add an executive summary and possible appendices.

Closure

If there were no nonconformities found during the engagement, the auditor creates the audit report. He/she should not forget to include any good practices discovered during the fieldwork. The report is presented at the exit meeting where the auditor, typically, summarizes the engagement and gives thanks to staff for their participation.

If there were some nonconformities found during the engagement, they should be addressed at the exit meeting. Based on their importance, they could require an immediate action or they could be dealt with later. In any case, there should be a commitment from the auditee to make appropriate changes.

If the auditor decides that the proposed changes do not properly address the issues, he/she should follow the *Standard 2600 – Communicating the Acceptance of Risks.* It states that if the CAE concludes that a level of risks accepted by the management is too high for the organization, he/she must discuss the matter with senior management. If the matter has not been resolved by the senior management, he/she must discuss the matter with the Board.

Risk-based audit planning

Planning engagements according the Standards

The *Standard 2000 – Managing the Internal Audit Activity* requires that the CAE must manage the internal audit activity[64] in such way to ensure it adds value to the organization. It implicates that the results of the activity's work achieve the goals defined in the internal audit charter.

Internal audit charter

The internal audit charter is a document that is specified in the *Standard 1000 – Purpose, Authority, and Responsibility*. It defines the internal audit charter as a "formal document that defines the internal audit activity's purpose, authority, and responsibility. It establishes the internal audit activity's position within the organization, including the nature of the chief audit executive's functional reporting relationship with the board; authorizes access to records, personnel, and physical properties relevant to the performance of engagements; and defines the scope of internal audit activities."

Pickett[65] adds that the purpose of the internal audit charter is also to explain the activity to other employees in the company and so it can be view as a marketing prospect. It is an excellent point because the activity is commonly viewed as a sort of policeman who is observing other people's behavior and giving fines. It is a pity because the potential of internal audit is much greater. As we discussed in numerous occasions the purpose of internal audit is to add value to a company by improving risk management, control, and governance processes. Pickett further specifies that the internal audit charter should cover these six areas.

1. The nature of internal auditing
2. Objectives
3. Scope
4. Authority
5. Responsibilities
6. Independence

Swanson[66] discusses the process of creating the internal audit charter. He acknowledges that it is not always easy to create the charter, therefore, it might be helpful to look for inspiration in similar companies and their charters. The function (most likely the internal audit department) should be able to answer two basic questions.

1. What services should it provide?
2. What its priorities should be?

[64] Internal audit activity is an entity in the organization which is responsible for internal audit services. Typically, it would be the Internal Audit Department or other similar unit.
[65] Pickett, 2005, p. 113
[66] Swanson, 2010, p. 109 - 111

When a draft of the charter has been developed, there should be a discussion with the key executives about its content. There could be several iterations of the process. After the agreement has been reached, the final version of the charter is to be published. Swanson also recommends an annual meeting of the audit committee and the internal audit department to better align the direction and activities of both entities.

Other relevant standards

The *Standard 2010 – Planning* says that the CAE must establish a risk-based plan which is consistent with the organization's goals. The plan must reflect the organization's risk appetite and be updated if any chances occur. The plan must be based on a documented risk assessment and inputs from the senior management and the Board should be also reflected.

The *Standard 2020 – Communication and Approval* states that the plan and resource requirements must be communicated with the senior management and the Board.

The *Standard 2030 – Resource Management* states that the adequate and sufficient resources to fulfil the plan must be secured by the CAE. Resources, in this context, mainly mean the number of staff and their skills and knowledge.

The *Standard 2040 – Policies and Procedures* states the the CAE must establish policies and procedures to guide the internal audit activity.

Banking risks

The Standard 2010 required that the CAE must create a plan of engagements which is based on risks. The following text provides a basic overview of risks in banking.

Let us begin with a few definitions of risk. Cade[67] states that risk is an "exposure to uncertainty of outcome." There are three key words contained in the definition. *Outcome* is a result of a particular action. It is typically represented in a financial form, however, it could be virtually anything relevant – number of customers, gain/loss in reputation etc. *Exposure* represents a situation where the bank has a stake in the outcome. And lastly *uncertainty* reflects the volatility of potential outcomes.

AS/NZS ISO 31000:2009 defines risk as "the effect of uncertainty on objectives". The key difference between both definitions is the word *objectives*. It better suits the organization's needs as the purpose of any organization is to fulfill its objectives. In this context, risk is a chance that that ability to fulfil the objectives could be affected.

Griffiths[68] presents three common and wrong assumptions about risk.

1. "Risk is only something for finance and insurance to worry about"
2. "Risk comes up on the agenda once a year"

[67] Cade, 1997, p. 2

[68] Griffiths, 2005, p. 18

3. “Business risk management is just another layer of unnecessary bureaucracy. It is just another initiative”

Cade [69] specifies five categories of risk that a bank faces:

- Solvency risk
- Liquidity risk
- Credit risk
- Interest rate risk
- Operating risk

Solvency risk represents a risk that a bank is not able to repay its obligations which is effectively its end. It is a very serious situation as declaring bankruptcy has a very negative influence on the overall stability of the financial system. The solvency of any bank is closely monitored and must be managed carefully in compliance with all applicable laws and regulations.

Liquidity risk is a risk that a bank does not have enough liquidity to cover all withdrawals and other orders on time. It is always presented because bank’s clients, usually, deposit money for a short time (current account, saving account) but borrow money with much longer maturity (30 years for the mortgage). Therefore, the banks must carefully manage the discrepancy in maturity dates.

Credit risk is presented any time a bank lends money to its client. It is a risk that the client is not able to pay off the borrowed amount and so the bank realizes a loss. Because of the nature of bank’s business operation, an ability to repay the debt is always calculated for a client before any money is offered. It is commonly called the credit score.

Interest rate risk is a risk that bank’s assets or liabilities will increase or decrease. The risk is associated with movements of exchange rates because some of bank’s financial instrument are associated with these rates. Examples of such rates are London InterBank Offered Rate (LIBOR) or Prague InterBank Offered Rate (PRIBOR).

Operating risk is the last category of risks that is present in any company in the world. It arises from its operations. It can be found in various forms – fraud, insufficient control, wrong design of a business process etc.

Banks and Dunn[70] discuss the topic in great detail. They characterize seven main categories of risk – market, credit, liquidity, model, suitability, process and legal. Each category contains further subcategories. Market, credit, liquidity and process risks were already covered in the previous paragraphs. We will now focus on the remaining three.

Model risk represents a risk of loss that was caused by the use of inappropriate models and other analytics. It is an important aspect that must be always taken into consideration as banks

[69] Cade, 1997, p. 16

[70] Banks and Dunn, 2003, p. 15 - 23

used many models and related tools in various areas of their business. Especially futures, illiquid assets and other complex contracts require sophisticated calculations. Model risk is particularly important for those financial companies that perform high-frequency trading[71] because even a small mistake in the model might have catastrophic consequences.

Suitability risk is a loss that occurred due to transaction suitability issues. The counterparty claims that it was not properly informed about the potential downsides of the transaction and might want to cancel the transaction or sue for damages. Even if the legal department believes that the transaction was properly made, the bank might still want to settle with the counterparty to avoid bad press.

Suitability risk could be considered a part of a bigger category – legal risks. Legal risk is a loss that was caused by a failure in the legal process. Banks sign thousands of contract each day. Some of these contracts are quite complicated and so there is always a chance that a mistake in the contract might have negative consequences.

Annual audit plan

In the ideal world, the internal audit department would carefully examine all aspects of the company. The management, employees, processes, controls, external partners… Everybody and everything would be inspected. Certainly, it could be helpful. The owners would be assured that all control, risk and assurance processes are properly designed and well managed. Unfortunately, the ideal world does not exist. Each department in the company, including the internal audit, is operating with a specific budget. It is not possible to somehow obtain unlimited resources and so to ensure the full theoretical scope of its operations.

As the number and scope of individual engagements the internal department can perform in a single year is limited, the CAE together with his/her colleagues must carefully plan the scope of work. The result of this planning is the annual audit plan.

Kagermann's approach

Kagermann's[72] approach to creating the annual audit plan is based on three phases.

- Creation of risk profiles for audit topics
- Compilation of the audit inventory
- Creation of the annual audit plan

A list of all audit topics[73] is a prerequisite for the process. It should include all the possible audit topics in a particular organization. The list should be made realistically. It means that the content should be feasible and at the same time must be relevant to the organization, particularly to its objectives. It is recommended to use a variety of sources for the preparation of the list. The sources could be both inside the organization (such as the compliance

[71] http://www.investopedia.com/terms/h/high-frequency-trading.asp
[72] Kagermann, 2008, p. 461
[73] Sometimes called the Audit Universe

department, legal, or IT) and outside (for example auditors from other companies, professional organization).

A risk profile for each suitable audit topic is created based on its exposure to individual risk categories[74] and their impact on the entire organization. The process of how to calculate the risk profile should be described in detail. It should provide guidelines for objective risk estimations. The next step would be to create the audit inventory based on risk profiles and priorities identified by the risk management. The annual audit plan should then be created according to the current personnel capacity of the internal audit department.

Pitt's objective-based approach

Pitt[75] argues that internal auditing should not just use the risk-based approach but also the objectives-based approach. It means that internal auditing would focus both on strategic risks as well as strategic objectives. The risk-based approach can be viewed as finding the negatives. In its essence, it is about looking for what could go wrong in the organization. However, the purpose of internal audit is to add value, therefore, in addition to looking for what could go wrong it should also look for what is necessary to do it right.

The objective-based approach is based on truly understanding the organization's business. It might appear self-evident and so it is commonly skipped because auditors believe that they somehow know what is going on but it is essential to spend time with senior management and fully understand the organization's objectives, strategies used to fulfill the objectives and risks that arise from those strategies.

The first step in the process is identifying risks. Pitt[76] discusses two different approaches to identify risk.

- Identifying at the activity, organizational and external levels
- Identifying at the environmental, people and organizational level

While the terminology and the methods are slightly different, the essence of both approaches is to identify risks that are internal (strategic, staffing and operational) and external (interaction with external entities).

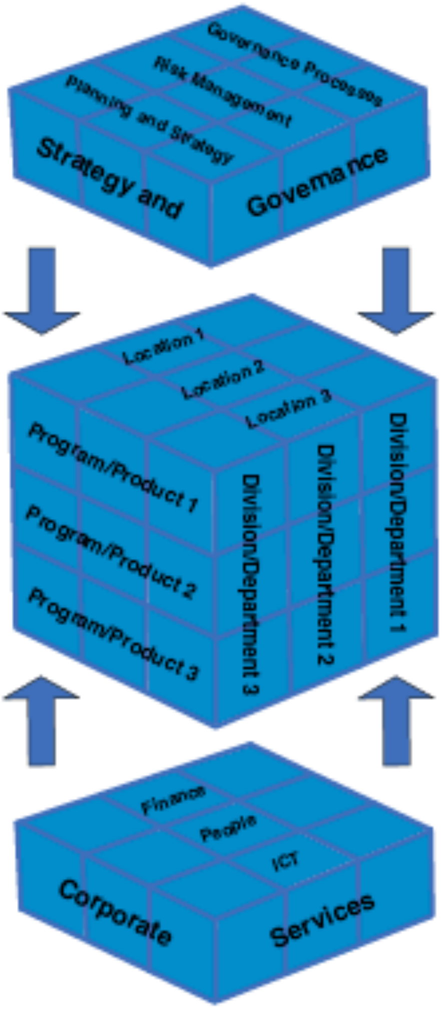
After the risks have been identified, internal auditors need to rate them. It is recommended to use the organizational risk framework. If the framework is not available, the internal audit function needs to create its own guidelines on how to rate risks. A suggested framework based on the Czech legislation is presented later in the chapter.

The next step is to map all auditable areas and create the audit universe. We have previously discussed Kagermann's approach on how to create a list. Pitt[77] recommends a different

[74] The categories were described in the previous chapter.
[75] Pitt, 2014, p. 203 - 204
[76] Pitt, 2014, p. 206 - 208
[77] Pitt, 2014, p. 212 - 213

method – the Matrix approach. It can be particularly helpful for larger organizations where corporate services, strategies and governance processes might be shared across across different divisions. Therefore, a better way of looking at these element is a three-dimensional view that their interplay. Figure 4 shows an example of the model.

Figure 4 – Model of the three-dimensional audit universe



Source: Pitt, 2014, p. 212

The last step of the process is to select individual audit areas from the audit universe based on their risk assessment with respect to available resources.

Griffiths' approach

Griffiths[78] analyzes seven stages in which an annual plan is developed.

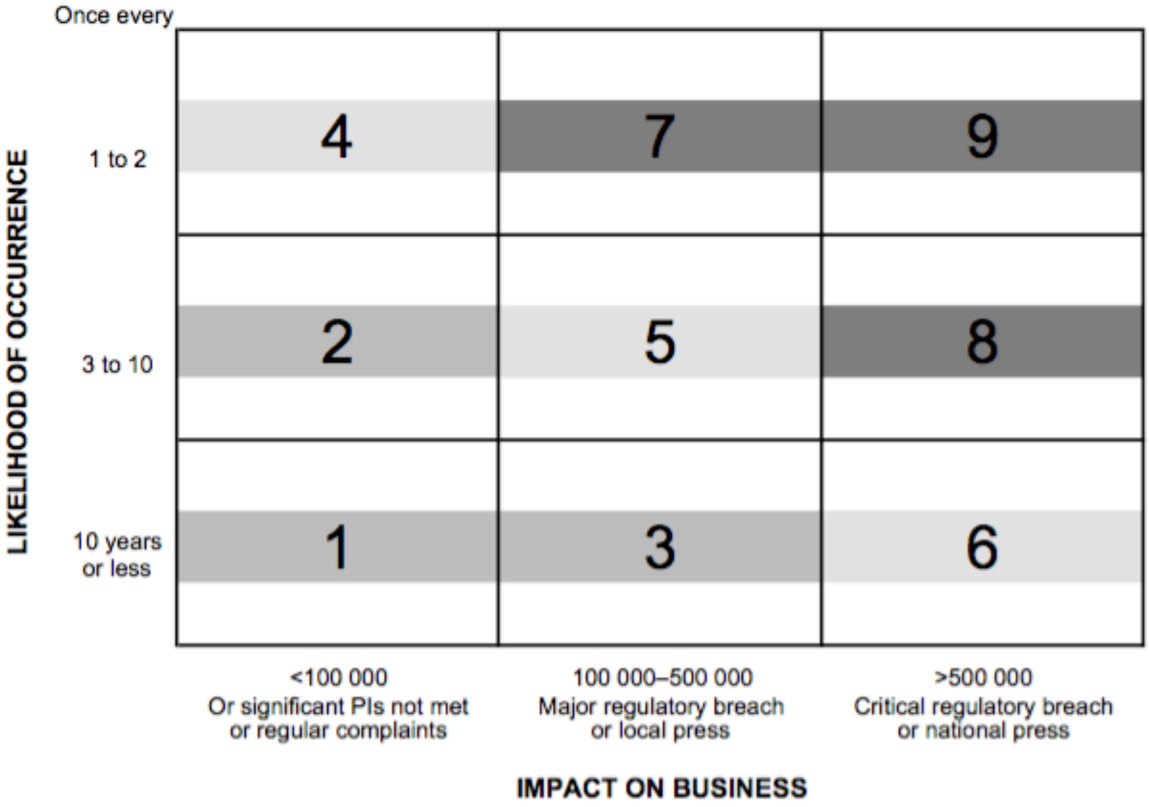
- Develop audit universe
- Decide on level of assurance
- Prioritize audits (based on risks)

[78] Griffiths, 2005, p. 180

- Prepare audit schedule (three-year plan)
- Separate into individual years
- Develop quarterly plan
- Publish quarterly plan

The first step of the process is the creation of the audit universe. This phase was included in both Pitt's and Kagermann's approach. Griffiths has created his own assessment matrix. It is presented as Figure 5.

Figure 5 – Risk assessment matrix



LIKELIHOOD OF OCCURRENCE Once every			
1 to 2	4	7	9
3 to 10	2	5	8
10 years or less	1	3	6
IMPACT ON BUSINESS	<100 000 Or significant PIs not met or regular complaints	100 000–500 000 Major regulatory breach or local press	>500 000 Critical regulatory breach or national press

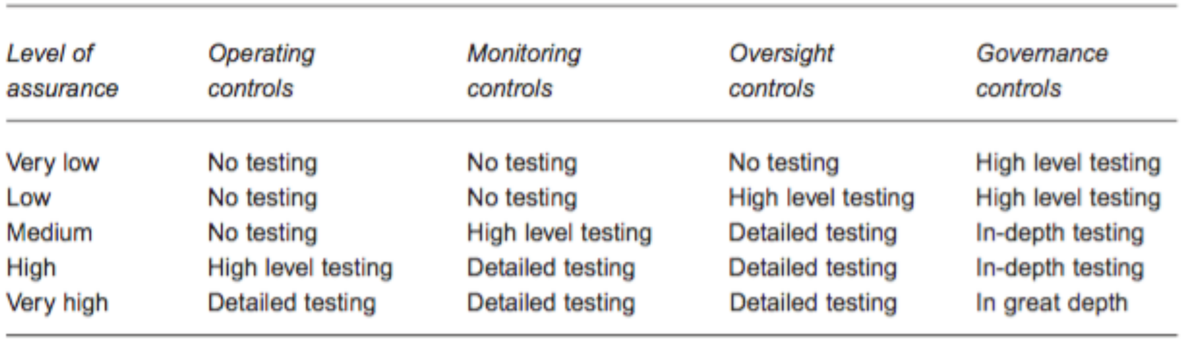
Source: Griffiths, 2005, p. 75

Each audit topic is put into one of these nine categories. 1 being the lowest overall risk and 9 the greatest. It is based on its impact on business and likelihood of occurrence. Impact on business can be either low (first column), medium (second column) or high (third column). The same scale applies to the likelihood. Low impact means small financial losses or minor related losses. Medium impact represents substantial effect on business (for example significant financial loss or business disrupt). High impact represents catastrophic effect on business (such as major financial loss or bad publicity in the press). Likelihood is measured in how often the it occurs.

The next step is to determine the level of assurance required for a particular audit topic. The level influences the depth of the audit, therefore, it is necessary not to overvalue it (due to limited resources) but also not to undervalue it (might not accomplish its objectives).

Griffiths[79] recommends to assign the appropriate level based on different controls and how much testing is necessary to be performed for each type. The table for evaluation of assurance level is presented as Figure 6. The level of assurance is assigned based on how much testing is required and which control it is.

Figure 6 – Evaluation of assurance level



Level of assurance	*Operating controls*	*Monitoring controls*	*Oversight controls*	*Governance controls*
Very low	No testing	No testing	No testing	High level testing
Low	No testing	No testing	High level testing	High level testing
Medium	No testing	High level testing	Detailed testing	In-depth testing
High	High level testing	Detailed testing	Detailed testing	In-depth testing
Very high	Detailed testing	Detailed testing	Detailed testing	In great depth

Source: Griffiths, 2005, p. 77

There are four types of controls. Operating controls are the day-to-day controls that are performed immediately and for each transaction. An example is checking the receipt before the goods are given away. Monitoring controls are performed by supervisors not too long after the transaction has occurred. An example is checking a batch of receipts and comparing it with sold goods. Oversight controls are performed by managers based on information from supervisors. An example is checking a bank account statements whether it corresponds with the receipts. These controls are typically performed some time after the transaction has occurred. The last controls are governance controls which are assurance assessments.

The next step is to prioritize audits based on the level of risks and available resources. Inputs for the phase are a sorted list of audit topics based on nine risk categories and evaluation of assurance level. Risk categories 9, 8, 7 should be dealt with first as they represent areas with high likelihood of occurrence and potentially catastrophic impact. Categories 6, 5, 4 are also important but only after the first group has already been dealt with. The last three categories 3, 2, 1 are only to be scheduled if there are still some resources available. Estimating resources is done based on level of assurance and type of control. Figure 5 specifies how much testing is required for each combination.

Pickett[80] discusses two approaches for creating timelines of audit projects. The first approach is to individually plan every single engagement. Timeline of a particular engagement is created based on its objectives and scope. It helps to ensure that the goals of the project could be realistically reached. The disadvantage of the approach is that the planning could be rather difficult as without doing research and knowing specific details it is hard to estimate necessary time.

Due to the difficulty in planning, most internal audit functions use an alternative approach. The CAE creates categories for a typical audit assignment. An example might look like this:

[79] Griffiths, 2005, p. 76 - 77

[80] Pickett, 2005, p. 217

- Large audit – 20 MD
- Medium-sized audit – 10 MD
- Small audit – 5 MD

Individual assignments are firstly assigned to appropriate categories and the extent of work is based on the category quota.

Risk assessment based on the Czech legislation

The Czech legislation provides a framework for risk assessment that can be used to create guidelines for rating risks in the internal audit function. The main components of the framework are included in the Regulation No. 316/2014 Coll. on Security Measures, Cyber Security Incidents and Reactive Measures that implements. the Law No. 181/2014 on Cyber Security

The regulation defines a formula for rating risks as

risk = threat x impact x vulnerability

The scales for rating threat, impact and vulnerability are as follows

Scale for threats assessment	
Level	Description
Low	The threat does not exist or is unlikely. Expected realization of the threat is less often than once every 5 years.
Middle	The threat is unlikely to probable. Expected realization of the threat is in the range from 1 year to 5 years.
High	The threat is likely or very likely. Expected realization of the threat is in the range from 1 month to 1 year.
Critical	The threat is very likely to more or less certain. Expected realization of the threat is more frequent than once a month.

Source: Regulation No. 316/2014 Coll. on Security Measures, Cyber Security Incidents and Reactive Measures

Scale for impact assessment	
Level	Description
Low	Impact is a limited period of time and a small scale and not be catastrophic. The scope of potential damages exceeding financial or material losses to CZK 5,000,000
Middle	The impact is limited in scope and limited period of time. The scope of potential damages ranges financial or material losses from CZK 5,000,000 to CZK 50,000,000
High	The impact is small scale but permanent or catastrophic. The scope of potential damages ranges: financial or material losses from CZK 5,000,000 to CZK 500,000,000
Critical	The impact of the areal extent, permanent and catastrophic.

	The scope of potential damages ranges: financial or material losses in excess of CZK 500,000,000

Source: Regulation No. 316/2014 Coll. on Security Measures, Cyber Security Incidents and Reactive Measures

Scale for vulnerability assessment	
Level	Description
Low	There is no vulnerability or abuse of vulnerability is unlikely. There are good security measures, which are able to timely detect possible weaknesses or possible attempts to overcome the action.
Middle	Vulnerability is unlikely to probable. There are good security measures whose effectiveness is checked regularly. Ability to timely security measures to detect possible weaknesses or possible attempts to overcome the action is limited. There are no known successful attempts to overcome security measures.
High	Vulnerability is likely or very likely. Security measures exist, but their effectiveness does not cover all necessary aspects and is checked regularly. There are known partial successful attempts to overcome the security measures.
Critical	Vulnerability is very likely to more or less certain abuses. Safety measures are not implemented or their effectiveness is greatly reduced. Controls for effectiveness of security measures. There are known successful attempts to overcome the security measures.

Source: Regulation No. 316/2014 Coll. on Security Measures, Cyber Security Incidents and Reactive Measures

The overall level of risk is then estimated based on threat, impact and vulnerability. For practical purposes, it is helpful to assign a numeric value to each category which will then allow a more precise calculation.

Model

Introduction

The following part of the thesis discusses a model which was created by the author to help internal audit departments in banks better plan audit engagements of their branch network. The model uses rather generic elements and so it can be adopted by any bank regardless of its size and location. It was not our goal to construct the model according to any specific national or international legislation. The model should be viewed rather as an inspiration on how data can be beneficial for planning audit engagements. Some elements of the model can be also used by other organizations.

As we have already discussed on numerous occasions, the scope of activities that can be performed by internal audit department is very wide. Therefore, the first steps in the planning process should always be creating the audit universe, assigning a level of risk for each individual topic and selecting topics based on risk and available resources. In a typical bank, one of the selected topic would always be auditing branch network. The problem is hidden in the extreme complexity of the task. Some of the larger banks in the world could have hundreds or even thousands of branches. In each single branch, there is a wide range of processes that could be of an interest for auditors. The question is – WHO to send WHERE to audit WHAT.

There are various ways on how to approach the task. The first option would be to simply hire as many auditors as is necessary to audit everything and everywhere. We can easily imagine that the approach would require an enormous amount of staff and so in the real world it is not usable.

The second approach would be to randomly create a list of all the branches and then send auditors to the individual branches based on the order of the list. The objectives of the engagements would be based on most significant risks and so would be almost the same in all the projects. The scope would be determined by the size of the branch. Nowadays, this approach is commonly used in most banks.

There are several major disadvantages of the list. First of all, the list could be quite extensive. There might be several hundreds or thousands of branches and so it could take years before the auditors would get to the very last one. The problem is not only the significant amount of time before an issue could be discovered but also the fact that the employees are aware of the situation and so after the audit passes they know that is going to be a few more years until the auditors come again. We can all imagine how badly the situation can result.

The previously discussed disadvantage relates to the WHERE part of the question. There are also disadvantages that relate to the other key words – WHO and WHAT. Continuing with our list example, when the auditors get to a new branch, how do they decide what should be the subject matter of the engagement. The International Standards for the Professional Practice of Internal Auditing requires that planning internal audit engagements must be risk-based. Therefore, all auditable areas are assigned an overall risk rating and the ones with the highest ratings are chosen. The problem is that if the evaluation is made on the global level then the objectives of individual engagements would always be the same. They would not reflect a situation in each particular branch. It could also be an issues because the audit program would become known and so the branches would have an incentive to particularly focus on the audited areas, however, other processes could become neglected. Other possibility would be to make an individual audit plan for every single branch. The previously discussed issued would then become not relevant but it would significantly increase the timeline and so either limit the scope of each audit or further increased the elapsed time between the first and the last item on the list.

Limitations of the model

The common practice (the list method) clearly has some significant downsides that should be addressed. Due to the discussed disadvantages, the author suggests a different approach – create a model using already available data to predict most probable problematic branch and most probable area. We have to stress out that the goal of the model is not to say "Y area is wrong at branch X" but rather "out of all branches, the most probable problematic one is X and most likely in Y area." The difference between the statements is that the first one is a result of a model that perfectly captures all aspects of the reality. Sadly, it is only theoretically possible to create such a complex model. Therefore, we are going to focus on a model that is not perfect, however, it should significantly improve the probability of the prediction.

The non-perfect model has of course some other limitations. The model is using data for the predictions. Based on the data, it estimates where there could a problem and in what. The model assumes that there are sufficient government mechanisms set in place and so the data is correct and has not been fraudulently modified. While there are a few limited ways how it could predict that the data might be wrong, it is beyond the scope of the thesis to consider this option. The prerequisite for data integrity should not be interpreted as that the model is not able to uncover a fraudulent activity. On the contrary, we will discuss various way how some predictions could be made.

The purpose of the model is not to substitute internal auditors. It is also not to substitute the whole risk-based audit planning process discussed in the previous chapter. It should be used as a tool that helps internal auditors with one specific task – planning internal audits in the branch network.

Initial parameters of the model were estimated as the best guess values. We have not performed any testing on banking data or other simulated values. Therefore, they should be adjusted according to the organization and its insider knowledge (data sources).

Creating a model

The following text will describe the process how the model was developed. The phases of the process are generic and so can be used not just for this specific task but also for a wide range of other topics.

1. Map sources
2. Find out available data
3. Understand data

4. Select appropriate data
5. Create a model
6. Evaluate model
7. Optimization
    a. Tuning parameters
    b. Repeat 4 – 5 – 6
8. Presentation

The first step of the process is to map all available sources of data. The range of the sources could be wide. It depends on size of the organization, type of business and level of IT (especially it the organization uses a sophisticated BI solution with centralized DWH). Useful data can be usually found in various databases (centralized, local), reports, spreadsheets, IT systems etc.

After the sources have been specified, all data categories (columns) should be mapped. It is helpful to import them into either excel spreadsheet or a database. There could be hundreds or even thousands of entities so for easier understanding it might be helpful to categorize them into meaningful groups.

Categorizing data is also a part of the next step – understanding data. It happens very often, and especially if data comes from different sources (different departments in the organization) that differ greatly, even in those values that should be the same (for example customer's name). Auditors need to understand what exactly each particular item means.

It is not going to be possible to include all the items in the model. Especially in the earlier stages, it is recommended to start with a few of them and possibly add others later. The initial items used for the model should be those which we expect that are most relevant.

There are various tools and techniques, some of them very complex, that could be used to create the model. The purpose of the thesis is not to provide the most sophisticated solution but rather to be seen as an inspiration on how to approach the process and how the initial model could look like.

The next step would be to evaluate the model. The best method is to use some historical data and calculate how many time were the predictions correct (against the known output).

Based on the evaluation of the model, there might be a need to tune its parameters. The process typically works in cycles – tune – evaluate – tune – evaluate etc. If tuning parameters is not making sufficient improvements, we have to repeat phases 4, 5 and 6 again.

The last phase of the process is to present the model and the results to relevant parties (CAE, senior management or others).

Controls

We have identified five key components of the model.

1. Measure the ability to get new business – performance (sold products)
2. Measure the ability to keep business – level of service (canceled products)
3. Measure customer satisfaction
4. Optimize the environment (opening hours)
5. Measure level of compliance (defaults)

The following text describes five controls which are the core of the model. The first control 'sum of loans' is used to measure performance of a particular branch against the others. We have chosen loans as an example of a common product. Similar controls should be created for other important products (checking account, saving account, debit cards, credit cards, mortgages, investments etc.).

The second control 'closed accounts' is used to measure how well a particular branch is able to keep the business. Generally, it shows a level of service. Similar controls should also be created for other important products (checking account, saving account, debit cards, credit cards, mortgages, investments etc.).

The third control 'customer satisfaction' measures level of customer satisfaction. It is an important indicator for a bank as it creates its image in public.

The fourth control 'opening hours' analyzes customers' behavior in a sense when do they visit a particular branch. It helps to optimize opening hours – identifies branches with too short or too long opening hours.

The last control 'default on a loan' measure rate of defaults. It indicates possible problems in compliance with internal guidelines or insufficient oversight. The problem could also be in the credit process. Similar control should also be created for other products (credit cards, mortgages etc.).

Sum of loans

The first element of the model is 'Sum of loans'. The purpose of the control is to identify those branches that have weaker performance (measured in the total sum of loans sold over a specific period) in comparison with the others.

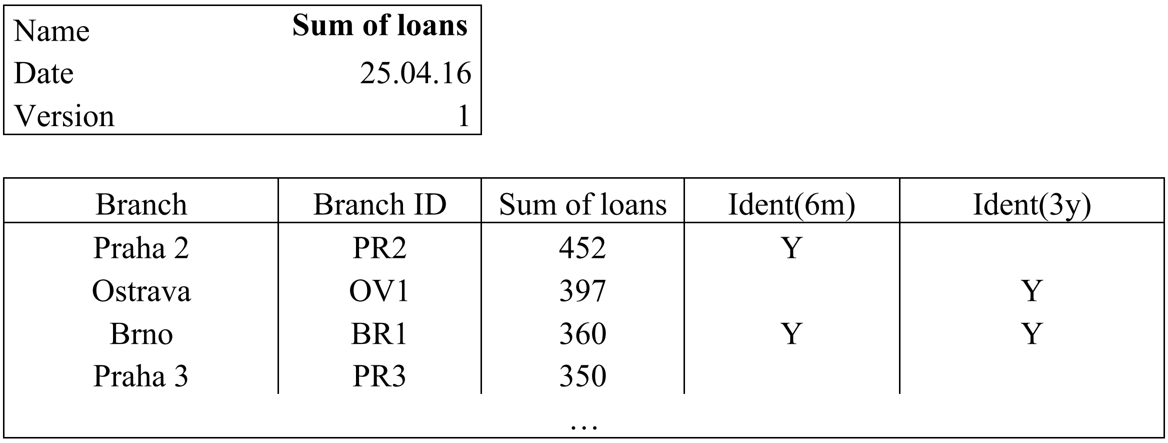
We have chosen loans as an example of how to set the control for a specific product. The auditors should also consider creating similar controls for other products – accounts, cards, mortgages, investments etc.

Name	Sum of loans
Action	1. Identify 5% of branches that sold the least total sum of loans. 2. Highlight those branches that have already been identified by the control in past 6 months. 3. Highlight those branches that have already been identified by the control more than 4 times in past 3 years.
Data sources	Branch, loan amount
Risks	Business risk

Bank area	Retail, corporate
Type	Performance
Significance	10%
Description	The control identifies individual branches that have sold the least loans (measured in the total sum of all loans sold over a specific period) and highlight those that have already been identified in past 6 months and also those that have been identified more than 4 times in past 3 years. If a branch has been identified, the auditors should perform an audit to discover why the sales are lower in comparison with other branches and recommend a solution. The problematic aspects could be inefficient management, training, lack of sales skills or others. If the branch has already been identified in past 6 months, the auditors should check how well the suggested solution has been implemented and consider other recommendations. If the branch has been identified multiple times in past 3 years, a more thorough audit should be performed to discover the fundament of the problem and recommend appropriate actions.

Figure 7 presents a draft of the output of the control.

Figure 7 – Report of sum of loans



Name	**Sum of loans**
Date	25.04.16
Version	1

Branch	Branch ID	Sum of loans	Ident(6m)	Ident(3y)
Praha 2	PR2	452	Y	
Ostrava	OV1	397		Y
Brno	BR1	360	Y	Y
Praha 3	PR3	350		
		…		

Note: All the data in the report are fictional.
Source: Author

Closed accounts

The second element in the model is 'Closed accounts'. It identifies branches where clients close more accounts than they open. It also identifies branches with the highest number of closed accounts. Identified branches should be examined to find out the problem and recommend solutions.

Same as for the previous control, the auditors should consider creating similar controls for other products – accounts, cards, mortgages, investments etc.

Name	Closed accounts
Action	1. Identify branches with negative balance between opened and closed accounts. 2. Identify 5% of branches with highest number of closed accounts.
Data sources	Branch, customer rating
Risks	Business risk
Bank area	Retail, corporate
Type	Performance
Significance	5%
Description	The control identifies individual branches that have negative balance between opened account and closed account. Having negative balance suggests that customers are not satisfied either with the product or the service from the employees is not sufficient – product is not properly explained, parameters of the product are not optimally set, general poor service etc. Auditors should examine the situation and recommend actions. The control also identifies 5% of branches with highest number of closed accounts. The auditors should perform an audit to discover why the performance is worse in comparison with other branches and recommend a solution.

Customer satisfaction

The next element of the model is ‘Customer satisfaction’. Customers are asked to rate how happy they were with the service. The same scale as in school is used for the rating 1 – 2 – 3 – 4 – 5 (1 being the best and 5 the worst).

The purpose of the control is to identify branches with very negative rating (marks 4 and 5). Those branches should be examined and advised on how to make improvements. The control also identifies branches with neutral rating (3) for whom some recommendations may also be given. The last group of identified branches are those where the rating has decreased by more than 1,5 since the last evaluation. It might be useful to make small corrections while the situation is still not critical rather than wait until it blows out of proportion.

Name	Customer satisfaction
Action	1. Identify branches with rating 4 and 5 in customer satisfaction 2. Identify branches with rating 3 3. Identify all branches where rating has decreased by more than 1,5
Data sources	Branch, customer rating

Risks	Business risk
Bank area	Retail, corporate
Type	Performance
Significance	15%
Description	The control identifies individual branches that have very negative rating in customer satisfaction (marks 4 and 5). Such negative valuation suggests that there is a significant problem that needs to be immediately addressed. Auditors should examine the situation and make recommendation. It is suggested to further monitor the situation to make sure that the recommendations were implemented and are successful. The control also identifies branches with rating 3 in customer satisfaction. Auditors might want to reach out to the branches to get more information about the current situation but it is not necessary to perform a comprehensive audit at this moment. If the situation does not get better in a foreseeable future, auditors might want to start the engagement. The control identifies those branches where customer satisfaction has decreased by more than 1,5 points. It warns auditors against a negative trend in the rating. Auditors should further investigate and discover what has caused the problem. It is generally useful to make small corrections while the situation is still not critical rather than wait and let the problem expand.

Opening hours

The next control is 'Opening hours'. The purpose of the control is to make sure that opening hours of each branch are set properly according to demand. The control creates an hourly graph of opening hours and a number of customers that visit in the respective hour (x-axis: hours, y-axis: customers). It identifies those branches where there are a few customers visiting in any hourly segment (typically the first in morning, lunch time and the last in the afternoon). It also identifies branches where there are a lot customer visiting in the first or the last segment. Auditors should consult with the identified branches and suggest appropriate adjustments.

Name	Opening hours
Action	1. Based on the hourly graph (x-axis: hours, y-axis: customers), identify those branches and respective time segments where less than 1% of customers visit in any hourly segment. 2. Based on the hourly graph, identify those branches where more than 5% of customers visit in the first or the last time segment.
Data sources	Branch, opening hours, customers
Risks	Business risk
Bank area	Retail, corporate

Type	Performance
Significance	5%
Description	The control creates an hourly graph of opening hours and a number of customers that visit in the respective hour. It identifies those branches and time segments where less than 1% of customers visit in any hourly segment. It might suggest that the opening hours could be too long (very little customers comes either in the morning or in the evening). Auditors should consult the situation with the management and possibly recommend to adjust the opening hours. The control also identifies branches where more than 5% of customers visit in the first or the last time segment. It might suggest that a large number of customers want to visit the branch either before it opens or after it closes and so auditors should consult the situation with the management and possibly recommend to adjust the opening hours.

Default on a loan

The last control is 'Default on a loan'. It identifies those branches where the default on loans rate is very high and high. The purpose of the control is to notify auditors of a possible credit risk problem and point out to suspicious branches.

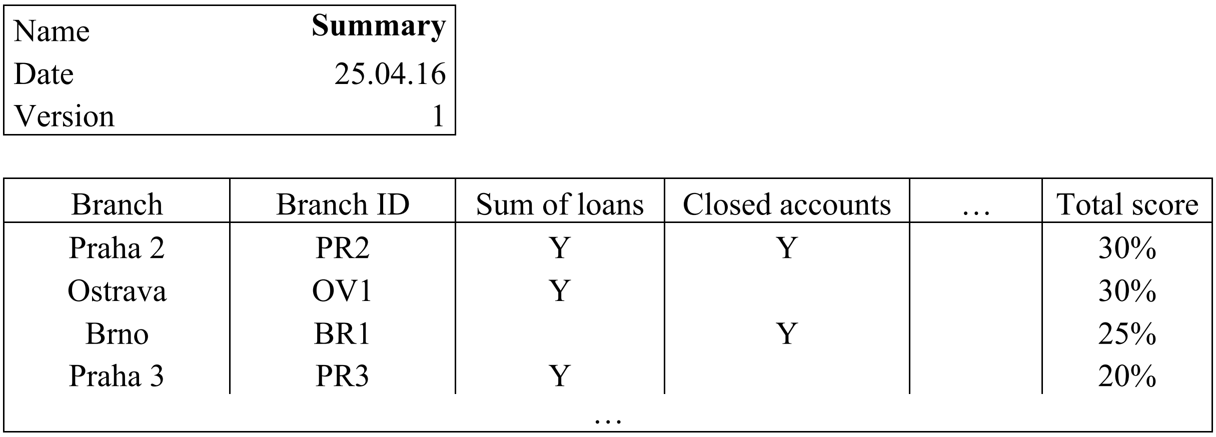
Name	Default on a loan
Action	1. Identify branches where default on loans rate is greater than 3% 2. Identify branches where default on loans rate is greater than 2%
Data sources	Branch, loans, defaults
Risks	Credit risk
Bank area	Retail, corporate
Type	Performance
Significance	10%
Description	The control identifies branches where default on a loan rate is higher than 3%. Auditors should analyze the identified subjects. If the analysis does not reveal the problem, an internal audit engagement should be performed. Special focus should be given on the credit process, in particular an analysis of creditworthiness. The control also identifies branches where default on a loan rate is higher than 2% but lower than 3%. Auditors should perform a quick analysis to decide whether the situation is normal or a more thorough examination is required.

Summary report

Each control shall have its own output. An example of how it might look like was provided as Figure 7. This is beneficial if auditors are interested in any specific area.

The output of the model should be presented in one consolidated report. An example of such report is provided as Figure 8. All the controls are evaluated together based on the significance of each element. For example, if 'sum of loans' has significance 10% then any branch that was identified by the control will add 10% to the total score. After all all controls have been evaluated, a list of branches is prepared ordered by total score.

Figure 8 – Summary report



Name	**Summary**
Date	25.04.16
Version	1

Branch	Branch ID	Sum of loans	Closed accounts	…	Total score
Praha 2	PR2	Y	Y		30%
Ostrava	OV1	Y			30%
Brno	BR1		Y		25%
Praha 3	PR3	Y			20%
…					

Note: All the data in the report are fictional.
Source: Author

Next steps

As we have declared in the limitations, the presented model is not aimed to be a complete solution which could be just taken and used as it is. The purpose of the model was rather to provide an inspiration for such a solution.

We recommend to start with a simple version, such as the proposed one, and later add more data and use more methods of how to manipulate with those data. In the begging, it is possible to only use simple SELECT queries (SQL) and import data into an Excel file where the manual calculation could be performed. Later, it would be beneficial to move from the manual calculation and create an automated solution, for example using macros (VBA) in Excel.

There are also a lot of sophisticated tools available that can be used. To name a few examples – BI solutions, data-mining tools, advanced statistical software etc.

Conclusion

The purpose of the thesis was to present a model for better planning internal audit engagements of branch network of the bank. The first part dealt with the internal audit. We presented and discussed the definition of internal auditing by the Institute of Internal Auditors (IIA). Other relevant disciplines – external audit and assurance – and their differences were also specified. The importance of these disciplines was demonstrated in the example of Enron. Later, we presented the International Professional Practices Framework, especially its key component - Standards. The end of this section was devoted to a description of the individual parts of an internal audit project. The second part of the thesis focused on planning internal audit engagements. We explained the risk-based planning approach and the Internal Audit Charter according to the Standards and other authors. Later, we listed and explained banking risks. The conclusion of this section was devoted to the process of creating the Annual Audit Plan.

The last part of the thesis describes a model, created by the author, which will help to improve planning of internal audits of the branch network of banks. It discusses the current situation in the internal audit departments and the needs for a better way of planning the individual engagements. It provides a description of limitations that the model has together with necessary phases of the process. The model is based on five key components.

1. Measure the ability to get new business – performance (sold products)
2. Measure the ability to keep business – level of service (canceled products)
3. Measure customer satisfaction
4. Optimize the environment (opening hours)
5. Measure level of compliance (defaults)

These components are transformed as controls.

1. Sum of loans
2. Closed accounts
3. Customer satisfaction
4. Opening hours
5. Default on a loan

Each component is to be individually evaluated and presented as a report. An example of such report was provided. The output of the entire model should be presented in one consolidated report. The components of the model are evaluated based on the significance of each element. An example of such report was also provided.

Abbreviations

IIA – Institute of Internal Auditors
IIARF – IIA Research Foundation
IPPF – International Professional Practices Framework
IFRS – International Financial Reporting Standards
GAAP – generally accepted accounting principles
CAE – chief audit executives
MD – man-day
SPE – special purpose entities
IFAC – International Federation of Accountants
AICPA – American Institute of Public Accountants
ECA – European Court of Auditors
BI – business intelligence
DWH – data warehouse
VBA – Visual Basic for Applications

Table of figures

Figure 1 – Volume of data
Figure 2 – An assurance initiative (ISACA)
Figure 3 – IPPF
Figure 4 – Model of the three-dimensional audit universe
Figure 5 – Risk assessment matrix
Figure 6 – Evaluation of assurance level
Figure 7 – Report of sum of loans
Figure 8 – Summary report

Resources

Literature, laws, norms

Moeller, Robert R., and Victor Z. Brink. *Brink's modern internal auditing a common body of knowledge.* Hoboken, N.J: Wiley, 2009. Print. ISBN 978-0-470-29303-4

Pickett. *The essential handbook of internal auditing.* Chichester, West Sussex, England Hoboken, NJ: John Wiley, 2005. Print. ISBN 978-0-470-01316-8

Rittenberg, Larry E., Bradley J. Schwieger, and Karla M. Johnstone. *Auditing: a business risk approach.* Mason, OH: Thomson/South-Western, 2008. Print. ISBN 978-0-324-37558-9

Russell, J. P. *The internal auditing pocket guide: preparing, performing, reporting, and follow-up*. Milwaukee, Wisconsin: ASQ Quality Press, 2007. Print. ISBN 978-0-87389-710-5

McLean, Bethany, and Peter Elkind. *The smartest guys in the room: the amazing rise and scandalous fall of Enron.* New York, New York: Portfolio/Penguin, 2013. Print. ISBN 978-1-59184-660-4

Cade, Eddie. *Managing banking risks.* Cambridge, England: Gresham Books, in association with the Chartered Institute of Bankers, 1997. Print. ISBN 1-85573-206-8

Vona, Leonard W. *The fraud audit responding to the risk of fraud in core business systems.* Hoboken, N.J: Wiley, 2011. Print. ISBN 978-1-118-09371-9

Handbook of international quality control, auditing review, other assurance, and related services pronouncements. New York: International Federation of Accountants, 2015. Print. ISBN 978-1-60815-250-6

Griffiths, Phil. *Risk based auditing*. Aldershot, Hants, England Burlington, VT: Gower, 2005. Print. ISBN 0-566-08652-2

Moeller, Robert R. *Sarbanes-Oxley internal controls: effective auditing with AS5, CobiT and ITIL.* Hoboken, NJ: John Wiley & Sons, 2008. Print. ISBN 978-0-470-17092-2

Gray, Iain, Stuart Manson, and Louise Crawford. *The audit process: principles, practice and cases.* Andover, Hampshire, U.K: Cengage Learning, 2015. Print. ISBN 978-1-4080-8170-9

ITAF: A Professional Practices Framework for IS Audit/Assurance, 2nd Edition, 2013, ISACA

ITAF: A Professional Practices Framework for IS Audit/Assurance, 3rd Edition, 2014, ISACA

Auditing Concepts Committee, “Report of the Committee on Basic Auditing Concepts,” The Accounting Review, 47, Supp. (1972), 18.

Assurance Services: A White Paper for Providers and Users of Business Information, 2013, AICPA Assurance Services Executive Committee

Pitt. *Internal audit quality: developing a quality assurance and improvement program.* Hoboken, New Jersey: John Wiley & Sons, Inc, 2014. Print. ISBN 978-1-118-71551-2

International Standards for the Professional Practice of Internal Auditing, 2012, The Institute of Internal Auditors

Guidelines on Audit Interview, 2013, European Court of Auditors

Kagermann, Henning. *Internal audit handbook management with the SAP-Audit Roadmap.* Berlin: Springer, 2008. Print. ISBN 978-3-540-70886-5

Swanson, Dan. *Swanson on Internal Auditing Raising the Bar*. Ely: IT Governance Pub, 2010. Print. ISBN 978-1-84928-068-6

AS/NZS ISO 31000:2009, 2010

Banks, Erik, and Richard Dunn. *Practical risk management: an executive guide to avoiding surprises and losses*. West Sussex, England New Jersey: J. Wiley, 2003. Print. ISBN 0-470-84967-3

Law No. 181/2014 Coll. on Cyber Security

Regulation No. 316/2014 Coll. on Security Measures, Cyber Security Incidents and Reactive Measures

Internet resources

IIA, https://na.theiia.org/Pages/IIAHome.aspx

IIA, https://na.theiia.org/standards-guidance/mandatory-guidance/Pages/Definition-of-Internal-Auditing.aspx

IFAC, http://www.ifac.org

Cambridge Online Dictionary, http://dictionary.cambridge.org/dictionary/english/effectiveness

The Chartered Institute of Internal Auditors, https://www.iia.org.uk

The Chartered Institute of Internal Auditors, https://www.iia.org.uk/about-us/what-is-internal-audit/

AICPA, http://www.aicpa.org/Pages/default.aspx

AICPA Assurance Services, A White Paper for Providers and Users of Business Information, http://www.aicpa.org/InterestAreas/FRC/AssuranceAdvisoryServices/DownloadableDocuments/ASEC_WP_Providers_Users_BI.PDF

ISACA, https://www.isaca.org/Pages/default.aspx

ISACA, http://www.isaca.org/Pages/Glossary.aspx?tid=1087&char=A

ISACA, http://www.isaca.org/Knowledge-Center/cobit/cobit-focus/Pages/COBIT-Focus-Volume-3-July-2013.aspx

IIA, https://na.theiia.org/about-us/Pages/About-The-Institute-of-Internal-Auditors.aspx

IIA, https://na.theiia.org/standards-guidance/Pages/Mission-of-Internal-Audit.aspx

IIA, https://na.theiia.org/standards-guidance/Pages/Standards-and-Guidance-IPPF.aspx#mandatory

IIA, https://na.theiia.org/standards-guidance/mandatory-guidance/Pages/Core-Principles-for-the-Professional-Practice-of-Internal-Auditing.aspx

IIA, https://na.theiia.org/standards-guidance/mandatory-guidance/Pages/Code-of-Ethics.aspx

IIA, https://na.theiia.org/certification/Pages/Certification.aspx

IIA, https://na.theiia.org/about-us/Public%20Documents/IIA%20Brochure.pdf

Office of Internal Audit, Wayne State University,
http://internalaudit.wayne.edu/process.php

Austin Community College,
http://www.austincc.edu/audit/documents/AuditCharter091103.pdf

Randal Rife, Planning for Success, 2006, https://iaonline.theiia.org/planning-for-success

The European Court of Auditors, http://www.eca.europa.eu/en/Pages/ecadefault.aspx

Investopedia, http://www.investopedia.com/terms/h/high-frequency-trading.asp

All internet resources were accessed on 25th of April 2016

Attachments

Attachment 1 – A list of services performed by internal audit.

- Cyclical audit (stock petty cash payroll).
- Investigations into specific problems.
- Responding to requests by management.
- Operational efficiency and effectiveness reviews.
- Internal control reviews.
- Fraud investigations.
- Compliance reviews.
- Reviewing controls over revenue, contracts administration and operational expenses.
- Acting as a contact point for allegations of fraud, waste and abuse.
- Information system reviews.
- Financial and compliance audits.
- Performance audits.
- Internal control reviews and testing poor areas.
- Investigative audits into reported irregularities.
- Verify assets and review safeguards.
- Evaluation of reporting systems and procedures.
- Cost saving reviews.
- Review of administration and accounting controls.
- Financial and performance audits.
- Revenue audits.
- Management studies into cost savings, problems in technical support and performance.
- Special reviews of projects.
- Control self-assessment facilitation.
- Environmental audits.
- Auditing the change management process.
- Operational audits.
- Computer audits.
- Control self-assessment questionnaire design and analysis.
- Issuing guidance to staff on internal control.
- Value driven internal consultancy, acting as change agents.
- Business process analysis.
- Business risk assessments.
- Quality advocates and reviews.
- Providing measures to strengthen mechanisms to achieving objectives.
- Evaluation of corporate governance processes.
- Working with management on their risk management practices.
- Advising clients on risk exposures and measures to remedy.
- Review risk management arrangements.
- Provide practical solutions and supporting management in implementing them.
- Participating in major information systems projects.
- Reviews to improve quality of management processes.

- Communicate risk information to clients.
- Operational auditing (or management audits).
- Financial systems audits, accounting and financial reporting.
- Compliance auditing on adherence to laws, regulations, policies and procedures
- Computer auditing during development stage.
- Audit approach determined by discussion with management but final result remains an internal audit prerogative.
- Advice to managers when making changes to procedure.
- Training in risk and control awareness.
- Provision of independent assurance on internal controls.
- General advice and guidance on control related issues.
- Operate follow-up system for outstanding audit recommendations.
- Evaluate action plans made in response to audit recommendations.
- Liaison and joint projects with external audit.
- Special projects as requested by management.
- Management reviews of new or existing programs, systems, procedures.
- Control consciousness seminars.
- Recommendations for enhancing cost-effective control systems.
- Monitoring financial information and reporting results.
- Reviews of fixed assets, cash receipts, budgets, purchasing and accounting routines.
- Surprise audits over cash funds, accounting records, employee records, observation of operations, and inventory records.
- Accountability and fraud awareness training.
- Projects to improve quality of information or its context for decision making.
- Reviews of e-commerce arrangements and security.
- Audits of internal control structures, efficiency and effectiveness and best practice.
- Safeguarding assets (and information) using verification of asset registers, inventories and the adopted security policy.

Adapted from Pickett [81]

[81] Pickett, 2005, p. 115 - 117