Ministry of Finance
of the Republic of North Macedonia

The experience of MF's Internal Audit Department in Auditing IT General Controls

Natasha Radeska Krstevska, CIA

Skopje, 2021

Why Auditing of IT General Controls?

Definition of Internal Auditing

Internal auditing is an independent, objective **assurance and consulting activity designed to add value and improve an organization's operations.** It helps an organization accomplish its objectives by brining a systematic, disciplined approach to evaluate and improve **the effectiveness of risk management, control and governance processes**.

Two of the Core Principles

- Promote organizational improvement, and
- Be insightful, proactive and future-focused.

In time when:

- automation of processes and use of IT are our present and future, and
- that is reinforced by the COVID-19 reality.

Internal Audit Engagement Objectives, IT Business Assurance Objectives and Goals of Information Security

The primary objective of the Audits of IT General Controls is to assess the design, establishment and operation of the system of internal IT General controls and to contribute to its continuous improvement.

The five categories of IT Business Assurance Objectives are:

1) **Availability**
2) **Capability**
3) **Functionality**
4) **Accountability**
5) **Protectability**

Three Goals of Information Security are:

1) **Availability**
2) **Confidentiality**
3) **Integrity** (includes **accuracy, completeness and security**)

Risks to the IT Business Assurance Objectives and the Goals of Information Security

Risk is the probability of an event occurring with a negative impact on the achievement of the entity's objectives.

In identifying and assessing risks internal auditors consider:

- management's current risk assessment (e.g. Risk Register);
- the risk assessment made for the Annual Plan;
- prior engagement-level risk assessment;
- prior audit reports,
- and sometime they use brainstorming sessions to identify key risks and controls, during which they use following questions:
  - What would prevent the IT activity from achieving its business and security objectives?
  - How would the activity be affected if no control existed?

Risks to the IT Business Assurance Objectives and the Goals of Information Security

Register of IT resources by groups of related resource categories:	Threat	Vulnerability	Risk
Software (Operating system, Application software, Utility software)	unauthorized use of the software	accessibility of the software	compromised data integrity and security
	improper use of software	software complexity	reduced quality of data and reports
	software changes	software complexity	poor operation, violation of the integrity of data, unavailability
	malware (viruses, spam, ...)	software susceptibility to viruses	reduced services due to in part or complete loss of programs and data
	destruction of the software file	feature of software and electronic information	inability to effectively resume work in the event of loss of data and programs
	natural disasters	susceptibility to destruction	termination of functions due to partial or complete destruction of software and databases
	use of unlicensed software	software product copyrights	non-compliance with legal obligations and lack of professional support and maintenance
	poor quality and out of date documentation	software complexity	poor quality operation
	software errors	property of the software	reduced quality of data and reports
Hardware (computer equipment such as personal computer, servers, laptops, peripheral computer equipment etc.)	loss or destruction of magnetic media	portability and susceptibility to destruction	data loss
	poor system administration	complexity of the system	reduced IT functionality and security
	equipment malfunction (computers and network)	equipment feature	reduced quality and efficiency
	poor maintenance	susceptibility to damage	interrupted business processes
	reduced safety of use	confidentiality of system and information	reduced IT functionality and security
	improper equipment configuration	complexity of the equipment	inadequate performance of computer system and the network
	lack of technical information about the equipment	complexity of the equipment	unreliable operation of IT equipment
Infrastructures (building, offices, air conditioning, heating ...)	unauthorized access	availability	reducing the reliability of information resources
	flood	unsuitable and unprotected storage location of documentation	partial or complete destruction of documentation and the equipment
	earthquake	non-seismic construction of the building	partial or complete destruction of documentation and the equipment

Administrative Security Controls

Administrative security controls include:

- **Policies** (govern how to resolve issues and the use of IT infrastructure to resolve issues);
- **Standards** (assist the implementation of policies by detailing what actions must occur to comply with policy);
- **Procedures** and **Guidelines** (illustrate how to comply with policies by providing detailed instructions).

➢ **They are very important for the auditor:**

- **As a criteria for assessing the design, establishment and operation of the internal control system**.

Controls over information and related technologies

Controls over information and related technologies can be broadly classified into two categories:

1) IT General controls are comprehensive controls at the organizational level, that pertain to all systems components, processes and data present in the IT environment of the organization.

2) Application controls are specific controls that relate to individual business processes or applications.

Most common IT General controls are:

- **Physical security controls over the data center;**
- **Logical access controls over infrastructure, applications and data;**
- **Systems development life cycle controls;**
- **Program change management controls;**
- **System and data backup and recovery controls.**

Physical Security - Physical Access Controls and Environmental Controls

Physical access controls that limit who can physically access systems (separates unauthorized individuals from computer resources) are:

- Keypad devices;
- Card reader controls;
- Biometric technologies.

The most important **environmental controls** are:

- Temperature and humidity control;
- Fire-suppression system (gaseous, not water);
- Data center not located on an outside wall;
- Building of the data center not located in a flood plain.

Logical Security Controls

Logical security controls, that prevent improper use or manipulation of data files and programs and ensure that only those persons with authorization and a bona fide purpose have access to computer systems, are:

- **Access control software** (e.g. firewall);
- **Passwords;**
- **File attributes** (e.g. read only, read/write, archive, hidden);
- **Access control matrices** (tables or lists of authorized users or devices);
- **Automatic log-off (disconnection)** of inactive data terminal;
- **A system access log;**
- **Encryption;**
- **Controlled disposal of documents;**
- **Security specialist** (e.g. Information Security Officer).

Systems development life cycle controls

The Systems Development Life-Cycle (SDLC) approach is the traditional methodology applied for the development of large, highly structured application systems**,** whose main advantage is **the increased management and control of the development process,** and it consists of the following five steps:

- Initiation, Feasibility, and Planning;
- Requirements Analysis and Definition;
- System Design;
- Acceptance, Installation and Implementation;
- Operations and Maintenance.

End-user developed applications, that are not created with the above approach, may not be subject to an independent outside review by systems analysts and may lack appropriate standards, controls, quality assurance procedures and documentation, and may be difficult to integrate with other information systems (that makes them more risky).

Program change management controls

Change management are processes that manage the changes to production systems (e.g. enhancements, updates, incremental fixes, and patches), with primary goal to sustain and improve the organization's operations with minimal impact on, and risk to, production systems, and for that purpose the changes must be managed in a defined, repeatable and predictable manner.

- Top risk indicators of **ineffective change management** are:
  1) unauthorized changes;
  2) unplanned outages;
  3) low change success rate;
  4) high number of emergency changes;
  5) delayed project implementation.

Controls:

Preventive controls:
- segregation of duties;
- change authorization;
- limiting persons who may update access to production data and programs.

Detective controls:
- monitoring;
- reconciling actual to approved changes;
- assurance services.

Corrective controls
- post-implementation reviews.

Contingency planning (Disaster recovery and Business continuity)

Contingency planning is the name commonly given to:

1) Disaster recovery is the process of resuming normal information processing operations after the occurrence of a major interruption caused by disasters (such as floods, fires or earthquakes), which requires an facility for alternative processing, and

2) Business continuity is the continuation of business by other means during the period in which computer processing is unavailable or reduced (for example due to accidental intrusions such as viruses or intentional intrusions such as hacking incidents).

It is crucial to have:

- comprehensive and current (tested at least annually) **Disaster Recovery plan**, which addresses the actual steps, people, and resources required to recover a critical business process and contains
  - **Backup and Offsite Rotation**

Practical tips about Auditing IT General Controls

Check the policies and the procedures for IT General Controls

If they do not exist	• Determine the appropriate criteria for audit and • Recommend their implementation in accordance with the acceptable Framework (e.g. ISO 27001/27002)
If they exist but have weaknesses	• Recommend their appropriate improvement
If they exist and are appropriate	• Use them as a criterion when evaluating controls

Check the Risk Management System (RMS)

If RMS is not designed or established	• Recommend introduction of Strategy and Methodology for Risk Management • Recommend establishment of Risk Register
If RMS exists but have weaknesses in design or functioning	• Recommend appropriate improvement (e.g. Risk Register to be regularly updated, at least once a year)
If RMS is appropriately designed, established and functioning	• Use it for your risk assessment during the auditing

Practical tips about Auditing IT General Controls

Check the situation with the employees (job description, qualifications, number)

Rulebook for systema-tization

- *May recommend its improvement for the IT Department regarding adequacy of the: job description, required qualifications and competencies, proper division of duties etc.*

Staffing of workplaces and Training of IT staff

- *May recommend, improvement of policies and practices of employment, retention and training of employees in the IT Department*

Information Security Officer and Personal Data Protection Officer

- *May recommend appointment of Information Security Officer and Personal Data Protection Officer*
- *Appropriate authorizations of IT staff for processing personal data*

Check the segregation of duties

If it is not existing or have weaknesses

- *May recommend certain responsibilities (such as of systems analysts, programmers, operators, file librarians, and others) to be assign to different individuals*

If it exists but has weaknesses in design or functioning

- *May recommend e.g. that Systems analysts and Programmers don't have access to data center operations, production programs or data files / Operators don't to have duties for systems design or opportunity to make changes in programs*

Check the existence of compensating controls

- *May recommend introduction or improvement of effective supervision, computer logs or library controls*

Practical tips about Auditing IT General Controls

Check the Physical Access and Environmental controls

Physical access controls

- *May recommend e.g. introduction and/or updating of the: Access Control system e.g.Card reader controls; Register of IT Resources; Matrix of rights of physical access and the Scheme of protective measures for control of physical access or appropriate documentation and control of the movement (issuance and return) of equipment and media.*

Environmental controls

- *May recommend e.g. implementation or proper use and maintenance of temperature and humidity control or fire-suppression system (gaseous, not water) etc.*

Check the Contingency planning

Disaster Recovery Plan

- *May recommend e.g. Plan to be developed and be comprehensive and current (regularly updated)*

Business Impact Analysis

- *May recommend e.g. to be performed and be comprehensive*

Periodic backup and Offsite rotation

- *May recommend e.g. Periodic backup of crucial data and programs to be performed, and*
- *to be kept in an appropriate Offsite location.*

Practical tips about Auditing IT General Controls

Check the Logical Access Controls

Check whether a detailed User Access Management Procedure is applied;

Make an inspection of the User Account Management System that manages and monitors user access permissions and access rights to files, systems and services - whether new accounts are added correctly and assigned only to authorized users, old and unused accounts are removed promptly;

Make an inspection of the Access control matrices – whether tables of authorized users or devices restrict access to user or physical devices that should logically need access;

Examine the System logs of actions that require scrutiny, such as repeated failed login attempts and the use of powerful utility programs;

Inspect whether regular checks by Information Security Officer and Personal Data Protection Officer are made on system access logs of access attempts, especially unsuccessful ones and of the use of powerful utility programs;

Especially focus on the persons with administrator rights and privileges and check whether the administrator approach and the administrator group are regularly monitored;

Check whether Automatic log-off (disconnection) of inactive data terminal is used, to prevent viewing of sensitive data on an unattended data terminal;

Check whether Wi-Fi network that is open for use by unauthorized persons (e.g. external visitors) is separated from the internal network;

Ensure that the administrative panel for content management and system setup is not directly accessible via Internet (remote maintenance is performed via VPN);

Make sure that a VPN connection is established in case of remote access, with mandatory authenti-cation of the authorized person;

Practical tips about Auditing IT General Controls

Check the Logical Access Controls

Check whether protection of the internal network is provided by restricting access to the Internet by blocking non-essential services through a **Firewall,** and make an insight into it's reports on organization-wide Internet use, unusual usage patterns and system penetration attempts.

Check security measures for safeguarding **Passwords** from theft, such as:

- changing passwords frequently (establishing a relatively short maximum retention period);
- mandating a minimum retention period so users cannot promptly change passwords back to their old and convenient values;
- and retaining old passwords to prevent their use;
- not displaying or printing passwords;
- setting minimum lengths, and use of optimal passwords that are randomly generated, eight-character or longer combinations of numbers, uppercase and lowercase letters and special symbols (not containing words or phrases).

Check the use of **Encryption,** especially:

- encryption measures for protection of mobile workstations and media for mobile storage of personal data (laptop, USB, external hard drives, CD-ROM, DVD, etc.);
- use of the latest version of the cryptographic protocol (TLS replacing SSL) on web pages;
- encrypting backups with personal data;
- transfer of sensitive data via VPN, by using encryption;
- encryption methods in Wi-Fi network management (e.g. WPA2 or WPA2-PSK).

Check the existence of **Controlled disposal of documents** that enforce access restrictions by destroying data when they are no longer in use (by shredding of paper documents and erasing magnetic media).

Practical tips about Auditing IT General Controls

Check the Controls against Malware (Malicious Software)

Check whether:

Procedures are established and **Responsibility** are assigned for coping with malware and **Education and Awareness raising** of users exist;

Authorized software is used and adherence to **licensing agreements** exists (only clean and certified copies of software are used, shareware software is not used, new software is checked with antivirus software);

Prompt installation of the **most recent patches, fixes, and updates** is done and updates are **tested before installation**;

Network servers have software to detect and erase or store malware;

Email attachments and downloads (and files on unauthorized media or from networks that are not secure) are checked, **email gateways** have software to scan attachments;

Antivirus software continuously monitor the system for viruses (or worms) and eradicate them and is immediately upgraded as soon as information about new threats becomes available;

Software and data for critical systems are regularly reviewed.

Practical tips about Auditing IT General Controls

Check Systems Development

Check:

Existence and use of the Systems Development Life-Cycle (SDLC) approach:

Formal proposal - based on the need assessment,

Feasibility studies,

System approval by the IT Steering Committee,

Design by Systems analysts and Development by Programmers,

Especially check whether:

- **Testing have been performed (and well documented) during system development;**
- **There have been some problems during the conversion;**
- **Training has been performed and documentation exists;**
- **Is there monitoring to ensure ongoing performance and continuous improvement and check it's results.**

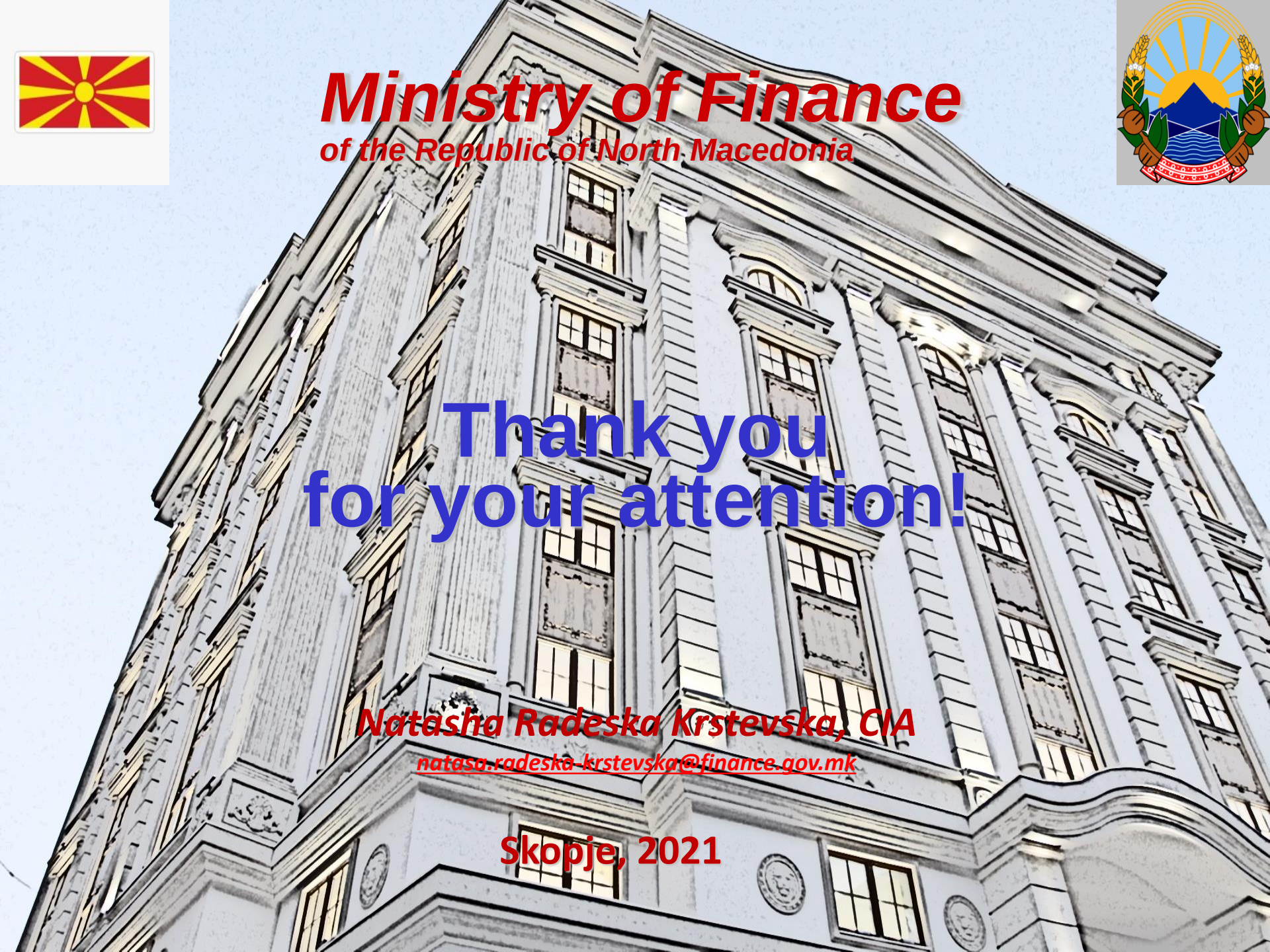
Check the Change Management Process

Whether it has been managed in a defined, repeatable, and predictable manner . Especially check whether

- **Changes are tested in a pre production (separate) environment;**
- **Change authorization, segregation of duties and limitation who may update access to production data and production programs, exist;**
- **Monitoring and Reconciling actual changes to approved changes exist.**

Existence of Reports on lessons learned, based on assessing whether

- **Change was successful;**
- **Change process was followed;**
- **Variances existed between the planned and implemented change;**
- **Compliance requirements were maintained.**



Ministry of Finance

of the Republic of North Macedonia

Thank you for your attention!

Natasha Radeska Krstevska, CIA

natasa.radeska-krstevska@finance.gov.mk

Skopje, 2021