National Academy for Finance and Economics
Ministry of Finance

Introduction Seminar: Information and Technology Audit

The Hague, May 2015

Ferdinand Uittenbogaard

Content

Focus on theoretical backbone of IT-audit:

- Methodology, fundamental principles, types of controls;

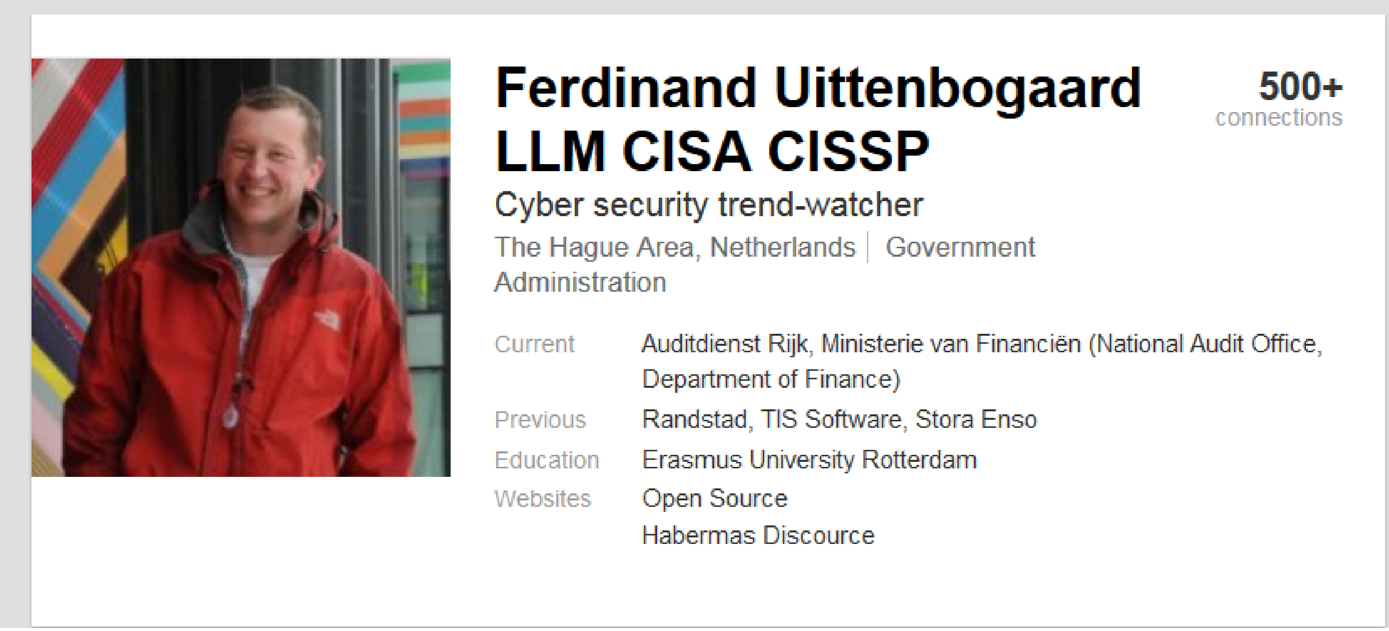
Rijksacademie voor Financiën,
Economie en Bedrijfsvoering
Ministerie van Financiën

Schedule:

Start - 10.00
Coffee-break -10.50
second session- 11.00
End - 11.50- 12:00

Introduction

- Who am I?
- LLM
- 10 years
- RE
- CISA
- CISSP
- CISM



Ferdinand Uittenbogaard LLM CISA CISSP

500+ connections

Cyber security trend-watcher

The Hague Area, Netherlands | Government Administration

Current	Auditdienst Rijk, Ministerie van Financiën (National Audit Office, Department of Finance)
Previous	Randstad, TIS Software, Stora Enso
Education	Erasmus University Rotterdam
Websites	Open Source Habermas Discource

- TB, TP, BS, Cyber Sec fan, PLA

About the Central Government Audit Service

- Established May 1st 2012

- Combining/merging strengths of the ministerial audit departments.

- Supervised, coordinated and monitored by Ministry of Finance, independently positioned and working for all ministries.

- Around 600 employees (100 IT-auditors)

Getting started

- What questions do you want to have answered at the end of the training?
- See document

Learning objectives

- What do you want to learn?
- What do you want to practice?
- What do you expect from us?

Topic Overview

1) The world of IT
2) IT Control Environment
3) IT Dependent Manual Controls
4) Application Controls
5) IT General Controls
6) Program Changes
7) Computer Operations
8) ITGC Walk-Through and Testing

The world of IT

- IT Governance
- Projects and Programs
- Processes and information systems
- IT-service management
- Infrastructure
- Information security

HealthIT
Health
Adoption
GreenIT
Flash
Malware
Broadband
HTML5
iPad
OpenWeb
MobileApps
Hive
GSM
Google
WOM
4G
Integrity
Microsoft
Nokia
Blog
Transparency
Phishing
SocialGaming
Twitter
Tweets
HyperLocal
Buzz
VisualSearch
TheCloud
Foursquare
WhiteSpaces
CrowdSourcing
NetNeutrality
Facebook
ContextAware
Tethering
YouTube
Like
Replies
Followers
Mobile
Oracle
Analytics
HP
BlackBerry
SmartPhones
Apple
Delicious
iPhone
Zynga
Dell
Scalable
Android
Posts
Content
Friends
OpenGov
MashUp
Java
SEO
Intel
IBM
WiFi
Yelp
Cisco
InlineAds

Topic Overview

1. The world of IT
2. IT Control Environment
3. IT Dependent Manual Controls
4. Application Controls
5. IT General Controls
6. Program Changes
7. Computer Operations
8. ITGC Walk-Through and Testing

IT audit definition

"An IT-audit is <u>independent</u> and <u>impartial</u> assessment of the <u>reliability</u>, <u>security</u> (including privacy), <u>effectiveness</u> and <u>efficiency</u> of automated information systems, the organization of the automation department and the technical and organizational infrastructure of the automated information processing. This activity applies to both operational systems and the systems under development" (Norea, 1992 p99; Strous, 1998)

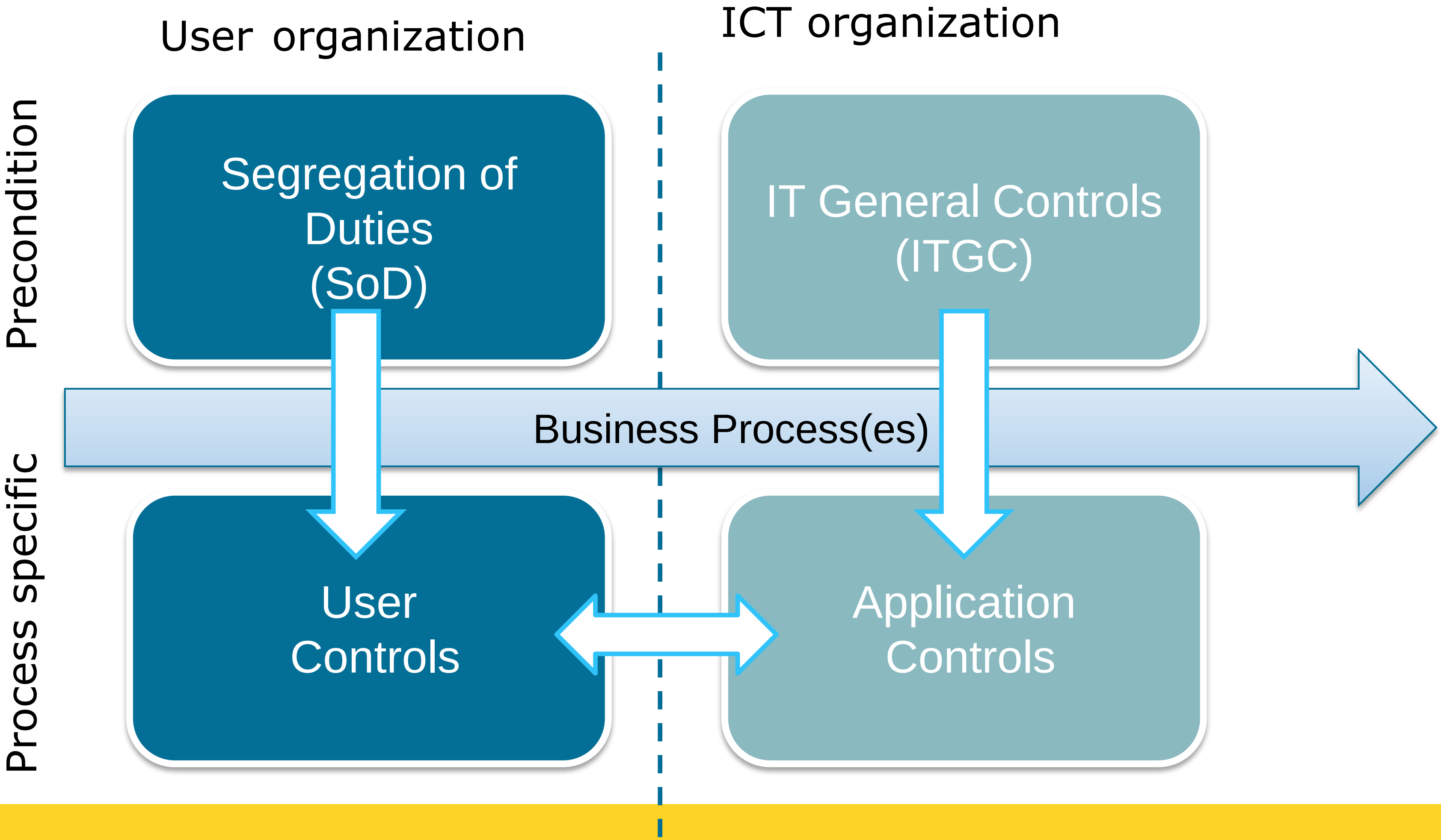
IT audit definition

“To provide additional assurance by assessing (the governance) of one or more <u>quality aspects</u> of the <u>objects</u> of information services”

Objects

- A process
- Procedures
- A system
- A project
- Milestone products
- IT-governance, policy and plans

Information system



User organization

ICT organization

Precondition

Process specific

Segregation of Duties (SoD)

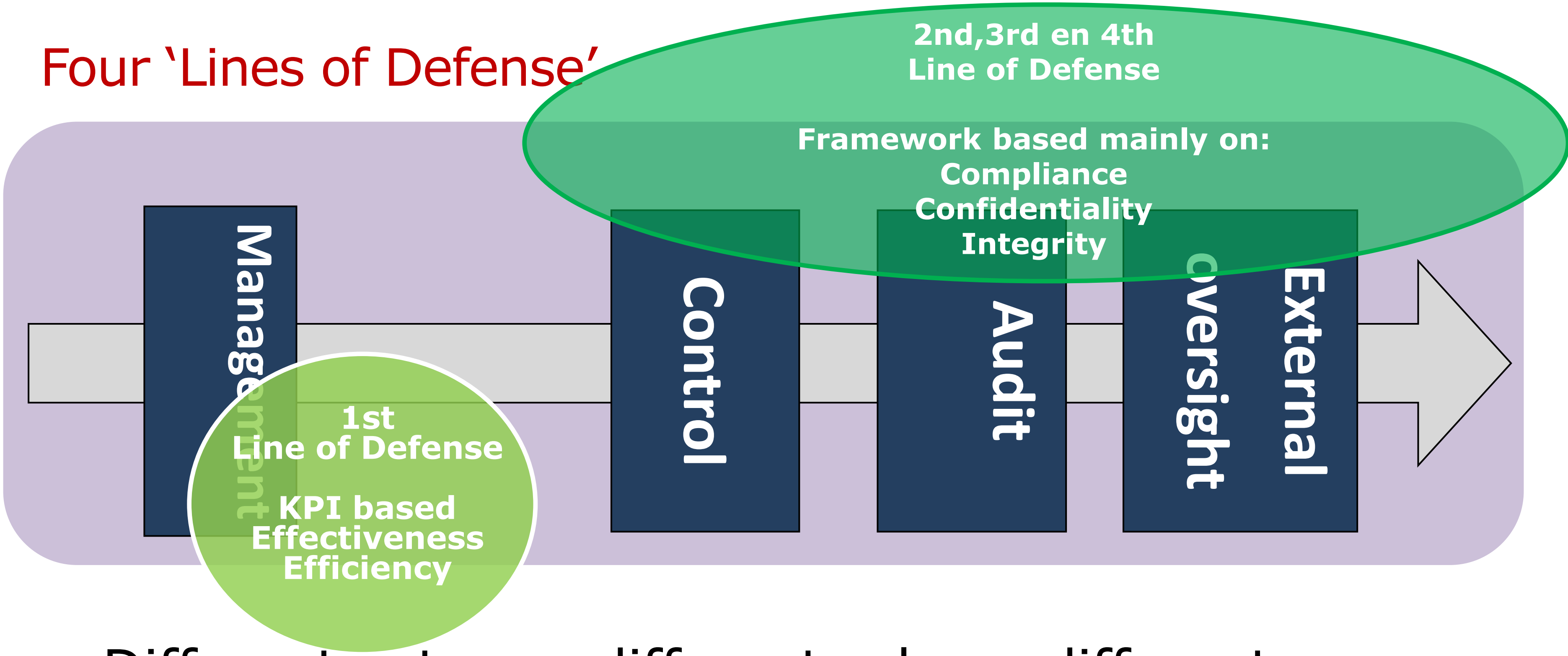
IT General Controls (ITGC)

Business Process(es)

User Controls

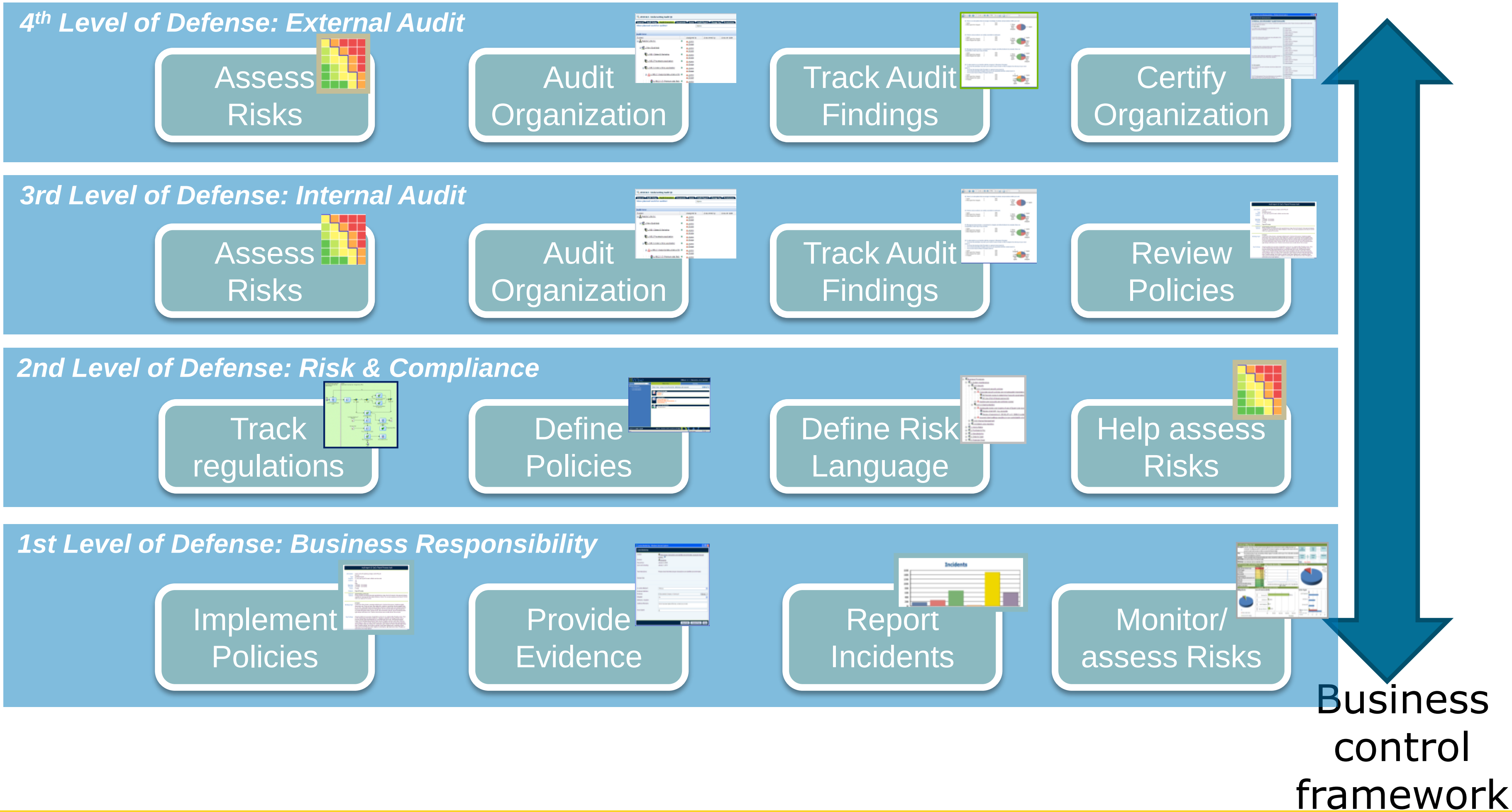
Application Controls

Four ‘Lines of Defense’



- Different actors – different roles – different responsibilities
- The need to integrate frameworks across lines of defense

Responsibilities for the lines of defense



4th Level of Defense: External Audit

- Assess Risks
- Audit Organization
- Track Audit Findings
- Certify Organization

3rd Level of Defense: Internal Audit

- Assess Risks
- Audit Organization
- Track Audit Findings
- Review Policies

2nd Level of Defense: Risk & Compliance

- Track regulations
- Define Policies
- Define Risk Language
- Help assess Risks

1st Level of Defense: Business Responsibility

- Implement Policies
- Provide Evidence
- Report Incidents
- Monitor/ assess Risks

Business control framework

Quality aspects

- Exclusiveness: authorization, identification etc.
- Integrity: completeness, accuracy, assurance
  - Authenticity:
  - Non-repudiation:
- Continuity: availability, recovery
- Controllability: SMART
- *Effectiveness: coverage rate, usability*
- *Efficiency: speed, user friendliness, reusability*
- *Governance: maintenance, connectivity, security*

Norms (references) in IT-audit

- Prince2 (project management)
- ITIL (IT service management)
- ISO27001 (Information Security)
- CobIT (provides norms/standards based on good IT-governance best practice)
- Etc.

Dependable on the audit object(ive) norms/references are customized!

Why is it Important to Audit IT Controls?

Why is it Important to Audit IT Controls? (Cont.)

- In our days many organizations depend heavily on IT;
- Internal Auditors are expected to evaluate IT controls;
- IT controls affect the reliability of electronic audit evidence.

General IT Considerations

Understand the IT Environment at the Entity Level:

- Identify significant applications and infrastructure

Purpose:

- Relationship between significant processes and applications
- Relationship between applications and infrastructure

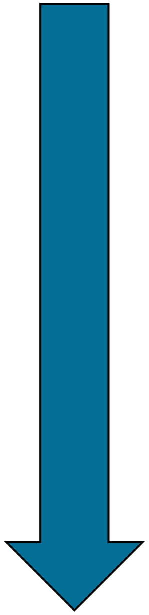
The IT landscape

4. Organization (branch, governance, tasks)

3. Processes (HR, Finance, Procurement etc.)

2. Applications (SAP, Windows, project software etc.)

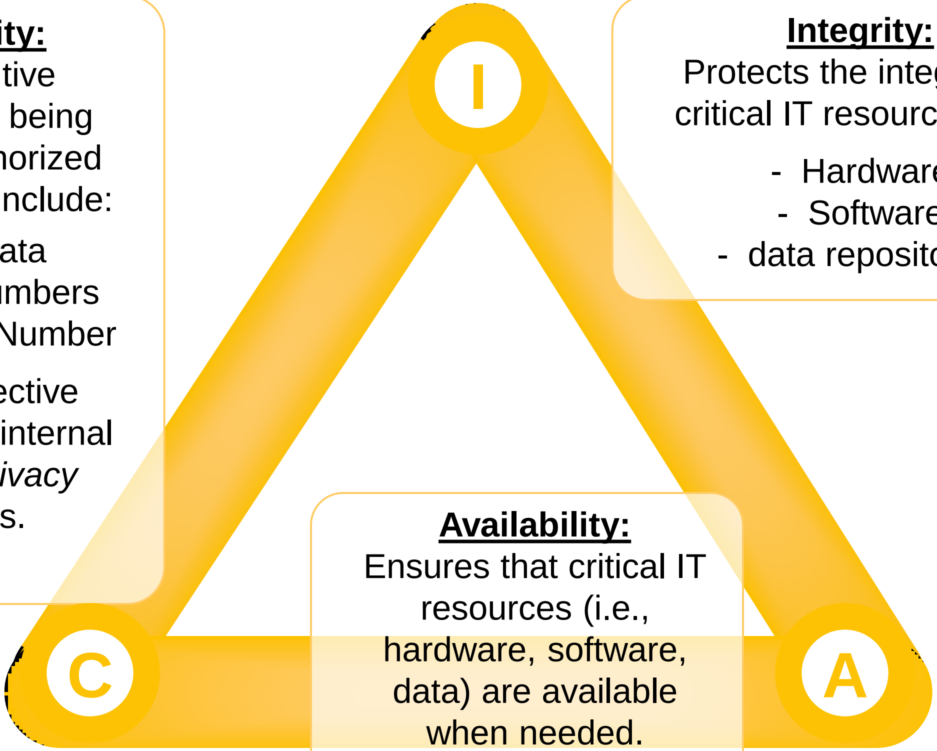
1. Infrastructure (databases, firewall etc.)



Most risks in IT take place on level 2 and 1!

IT Controls Objectives

IT controls are designed to meet control objectives related to *Information Security* requirements. The core objectives, often referred to as *C-I-A*, can be depicted as follows:



Confidentiality:
Protects sensitive information from being viewed by unauthorized users. Examples include:

- Financial Data
- Credit Card Numbers
- Social Security Number

Note: This objective directly relates to internal and external *Privacy* requirements.

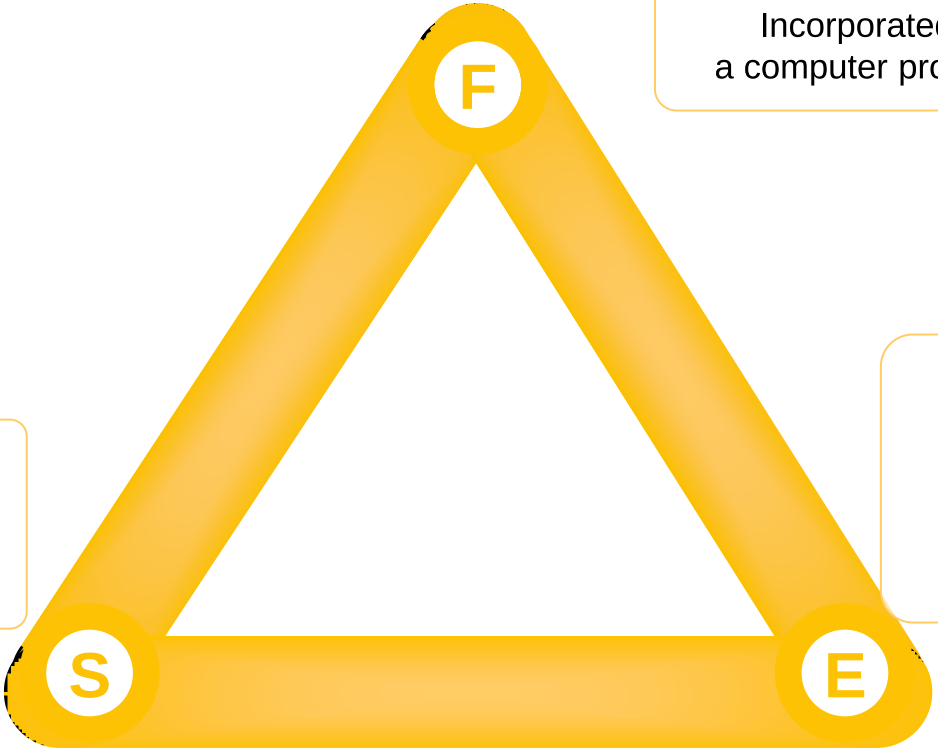
Integrity:
Protects the integrity of critical IT resources like:

- Hardware
- Software
- data repositories

Availability:
Ensures that critical IT resources (i.e., hardware, software, data) are available when needed.

But also

***Information Security* requirements have a negative correlation with other requirements for computer programs.**



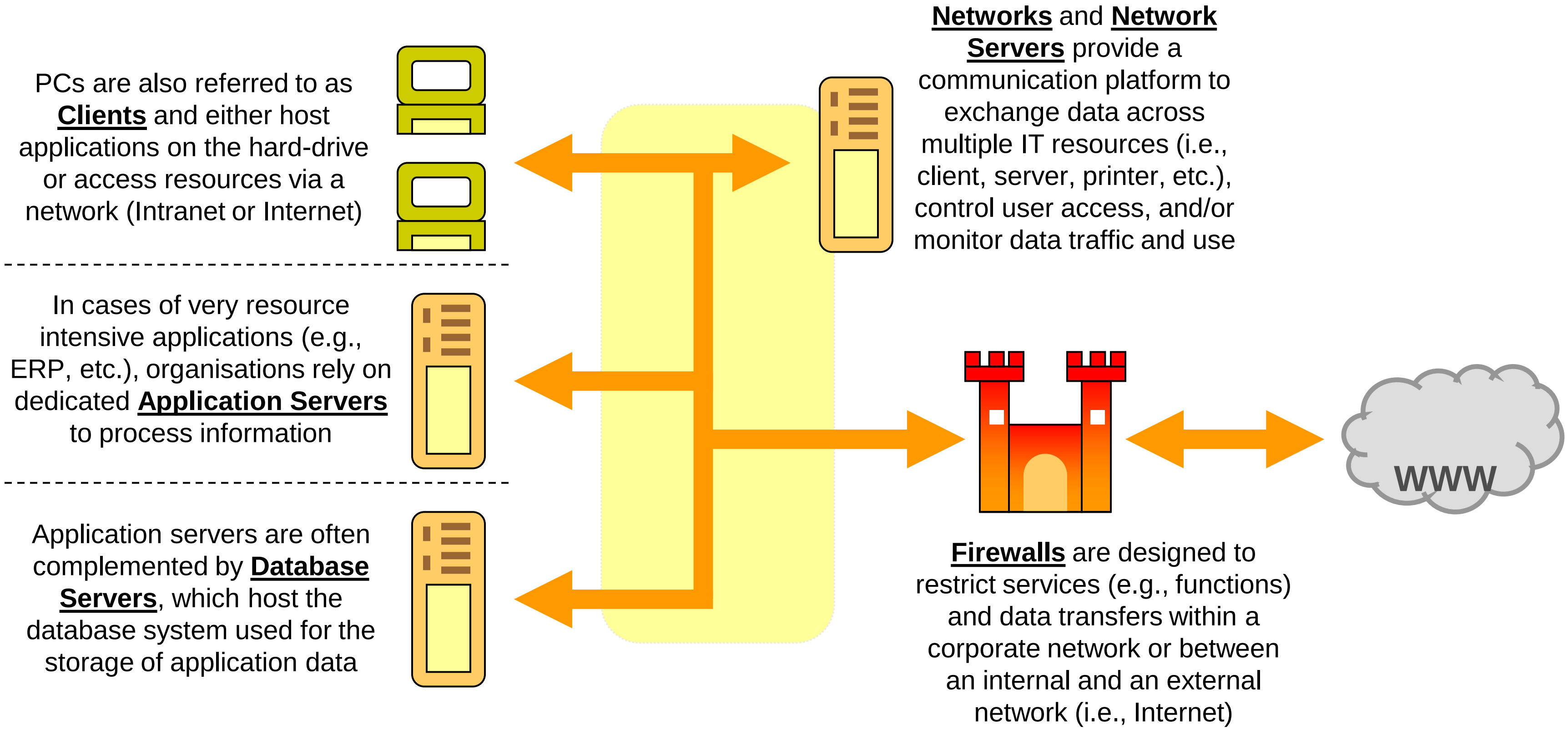
Functionality:
The functions that are
Incorporated in
a computer program.

Ease of use:
The usability of a
computer program.

Security
Level of security
measures taken in a
computer program

IT Topology & Terminology

The IT architecture in organizations can differ based on particular business needs. The following graph provides a simplified overview of common key components and terminologies:



PCs are also referred to as **Clients** and either host applications on the hard-drive or access resources via a network (Intranet or Internet)

In cases of very resource intensive applications (e.g., ERP, etc.), organisations rely on dedicated **Application Servers** to process information

Application servers are often complemented by **Database Servers**, which host the database system used for the storage of application data

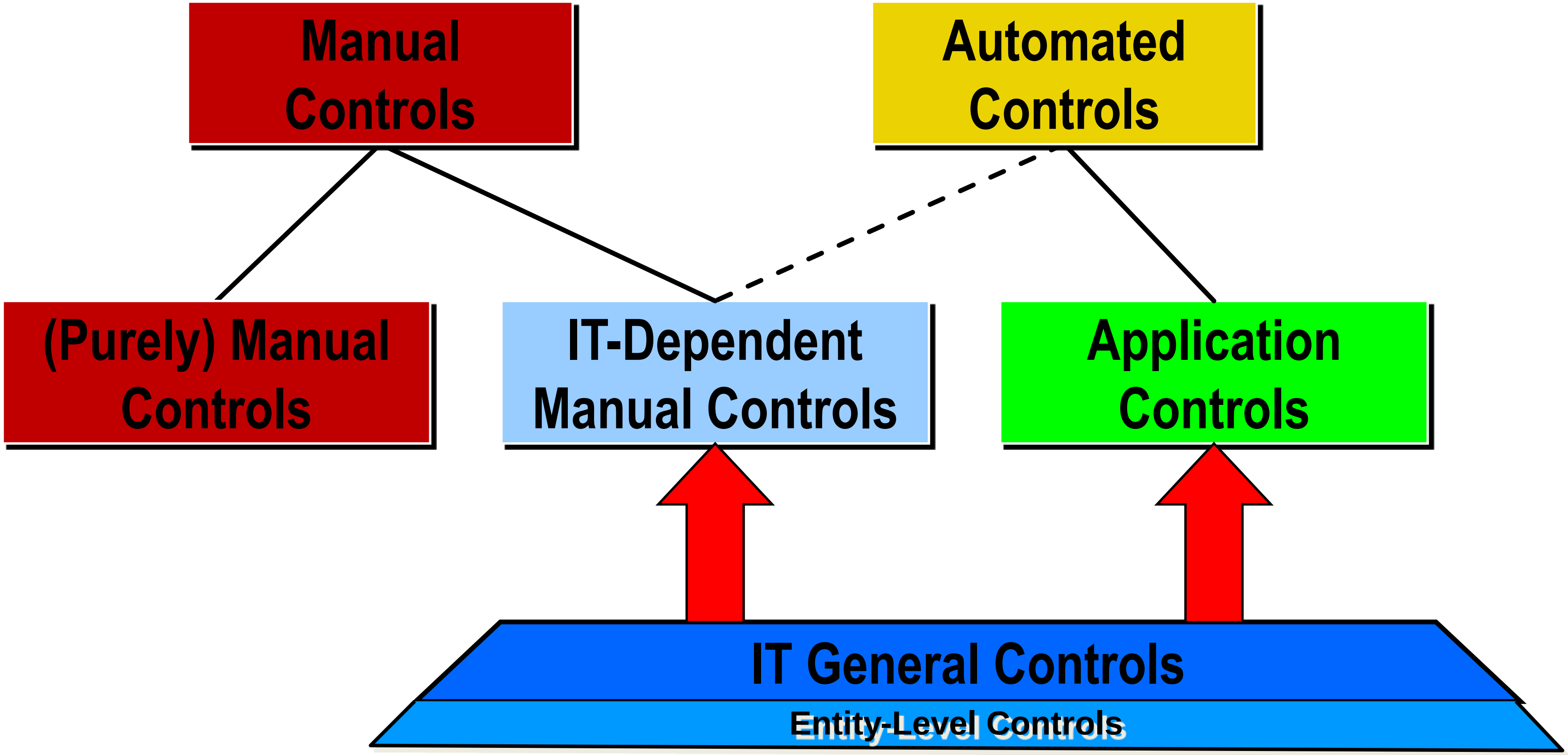
Networks and **Network Servers** provide a communication platform to exchange data across multiple IT resources (i.e., client, server, printer, etc.), control user access, and/or monitor data traffic and use

Firewalls are designed to restrict services (e.g., functions) and data transfers within a corporate network or between an internal and an external network (i.e., Internet)

IT Control Overview

When referring to IT controls, there are essentially two categories of controls that can be considered. *Application Controls* (AC), which are embedded in “standard” business process (e.g., Procurement, Revenue, etc), are designed to automate control functions, while *IT General Controls* (ITGC) support control requirements within standard IT support processes.

Classification of Controls



Manual Controls

Automated Controls

(Purely) Manual Controls

IT-Dependent Manual Controls

Application Controls

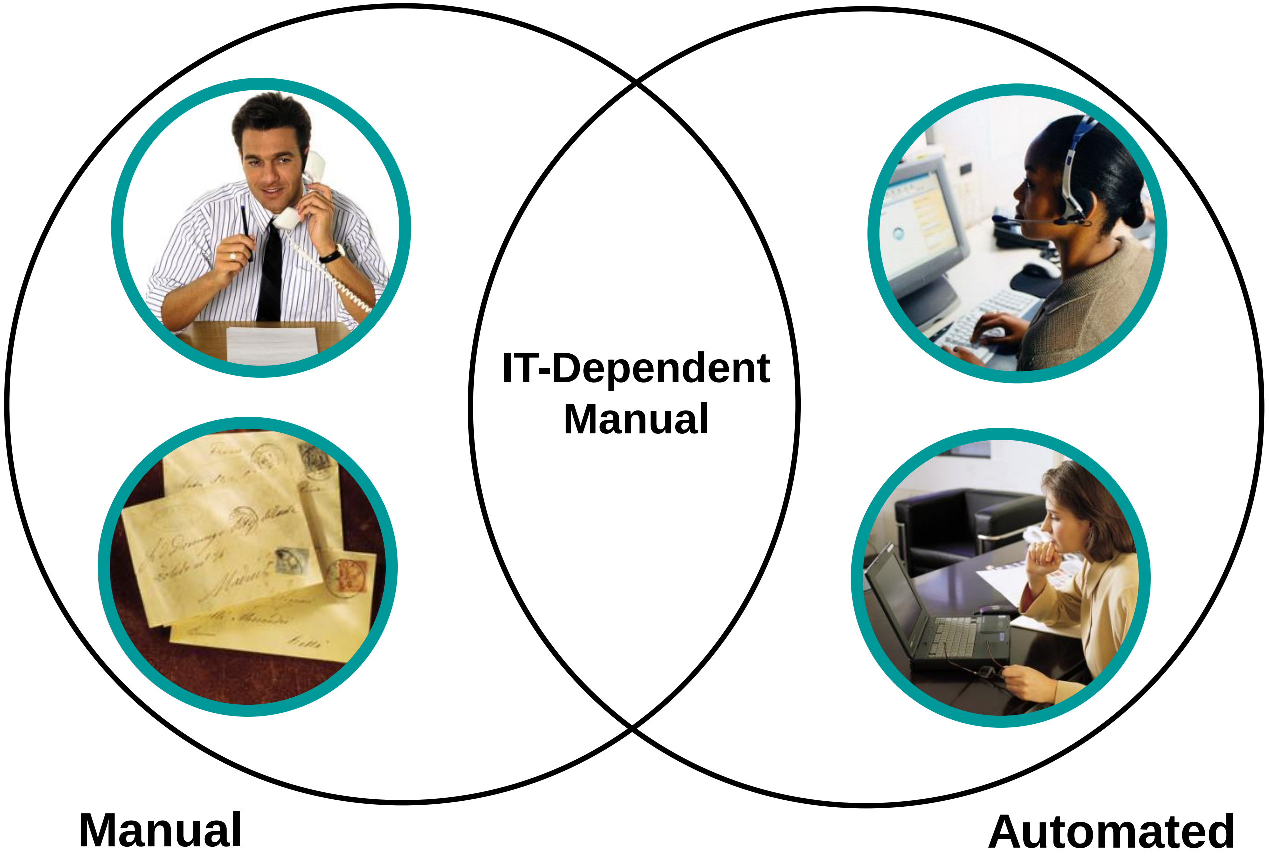
IT General Controls

Entity-Level Controls

Topic Overview

1. The world of IT
2. IT Control Environment
3. IT Dependent Manual Controls
4. Application Controls
5. IT General Controls
6. Program Changes
7. Computer Operations
8. ITGC Walk-Through and Testing

Automated Vs Manual Controls



IT-Dependent Manual

Manual

Automated

Automated Vs Manual Controls (Cont.)

Control Technique	Automated Component	Manual Component
❖ Authorisation: Approval of transactions executed in accordance with management's general or specific policies and procedures.	❖ Online routing and online evidence of approval	❖ Manual approval form with manual signatures
❖ Exception/Edit Report: Generation of a report to monitor something; the results are investigated to resolution.	❖ Automated output control based on exception identified during processing of data.	❖ Review and timely resolution of exceptions
❖ Interface Controls: Complete and accurate transfer of data between systems.	❖ Automated monitoring of data transmission and error correction	❖ Review and timely resolution of exceptions

Automated Vs Manual Controls (Cont.)

Control Technique	Automated Component	Manual Component
❖ Segregation of Duties: Separation of the duties and responsibilities for authorising transactions, recording transactions, and maintaining custody.	❖ System access in accordance with job responsibilities	❖ Job responsibilities appropriately segregated
❖ System Access: Limitations on the abilities that users have within a computer information system - processing environment, as determined and defined by access rights configured in the system.	❖ Authentication and Access Control Lists ❖ Access system parameters in line with Job responsibilities	❖ Approvals of authorizations ❖ Periodic review and follow-up of User Access Profiles

IT-Dependent Manual Controls

- Controls performed by a person, who rely upon automated output;
- Mostly detect controls that rely upon computer-generated information or computer functionality;
- Example: management reviews a weekly exception report and follows up on significant exceptions. Because management relies on the computer-produced report to identify exceptions, we also determine that there are controls in place to ensure that the exceptions report is complete and accurate.

IT-Dependent Manual Controls (Cont.)

Types of IT-Dependent Controls

- System-generated standard reports
- Queries/ad-hoc reports

Testing Considerations

- What is report used for?
- How used in control?
- Completeness, accuracy, integrity, and existence
- Re-performance of calculations

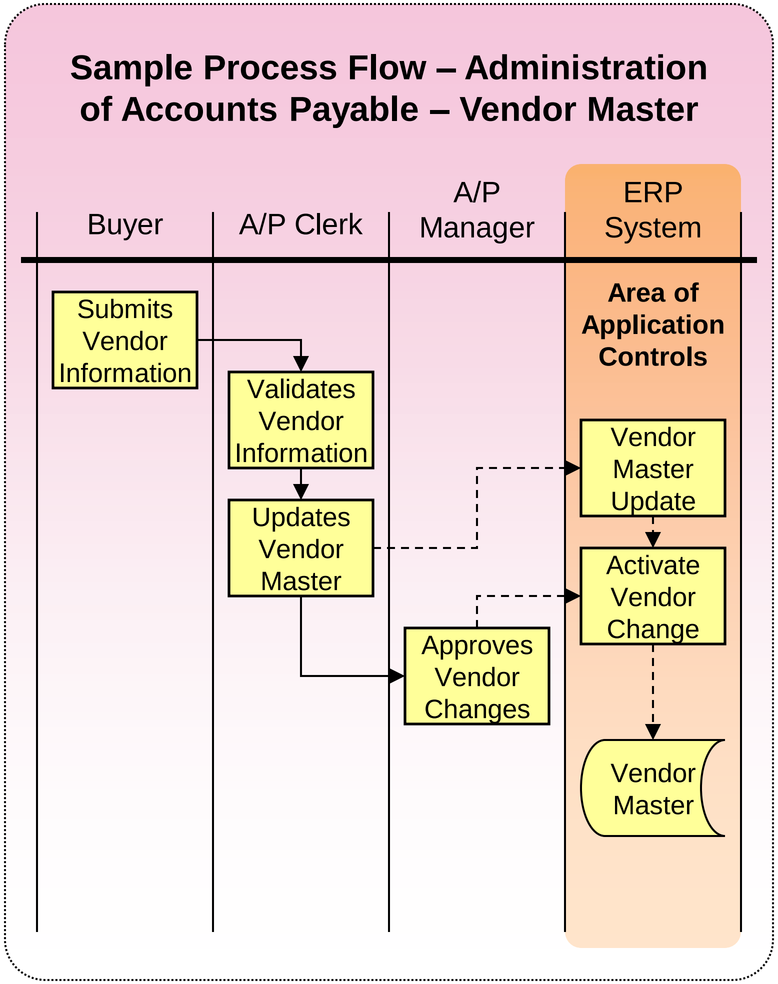
Topic Overview

1. The world of IT
2. IT Control Environment
3. IT Dependent Manual Controls
4. Application Controls
5. IT General Controls
6. Program Changes
7. Computer Operations
8. ITGC Walk-Through and Testing

Application Controls

Application Controls are system-enabled controls within standard business processes, which are intended to enforce specific work requirements. *Application Controls* are usually preventive in nature. Examples include:

- Logical access controls
- Date entry / field validations (e.g., validation of entered credit card numbers)
- Workflow rules (e.g., electronic routing and sign-off of purchase requests)
- Field entries being enforced based on pre-defined values (e.g., pricing information)
- Work steps being enforced based on pre-defined status transitions (e.g., open > reviewed > closed)
- Automated audit logs
- Automated calculations



Sample Process Flow – Administration of Accounts Payable – Vendor Master

Procurement Process Examples

- Procurement Requisitions Notes are approved online based on management-approved authorization limits;
- Procurement Orders are generated only for approved Procurement Requisition Notes;
- Invoices are paid only after a three-way match to Purchase Order and Goods Received Note/Delivery Note.

Inadequate Application Control Design

Consider Improvement Recommendations:

- Alternative application controls
- Other manual controls

Walk-Through of IT Application Controls

Purpose:

- To confirm our understanding of the process procedures;
- To confirm that the controls have been placed in operation;
- To compare the end user’s understanding of how the application controls function to how they actually work.

Application Controls Testing

We are concerned with the following components of application controls:

- Configuration settings and custom automated controls;
- Master data controls and access
- Control overrides;
- Segregation of duties and function access;
- Interface control.

Application Controls Testing (Cont.)

How to test application controls:

- Will vary based on type of application (i.e. SAP, JD Edwards);
- Will vary depending on whether the application is an off-the-shelf vs. customized.

Basic testing steps:

- Confirm configuration set-up;
- Run test transactions through the application;
- Test security access to set-up/configuration functions;
- Test change management.

Topic Overview

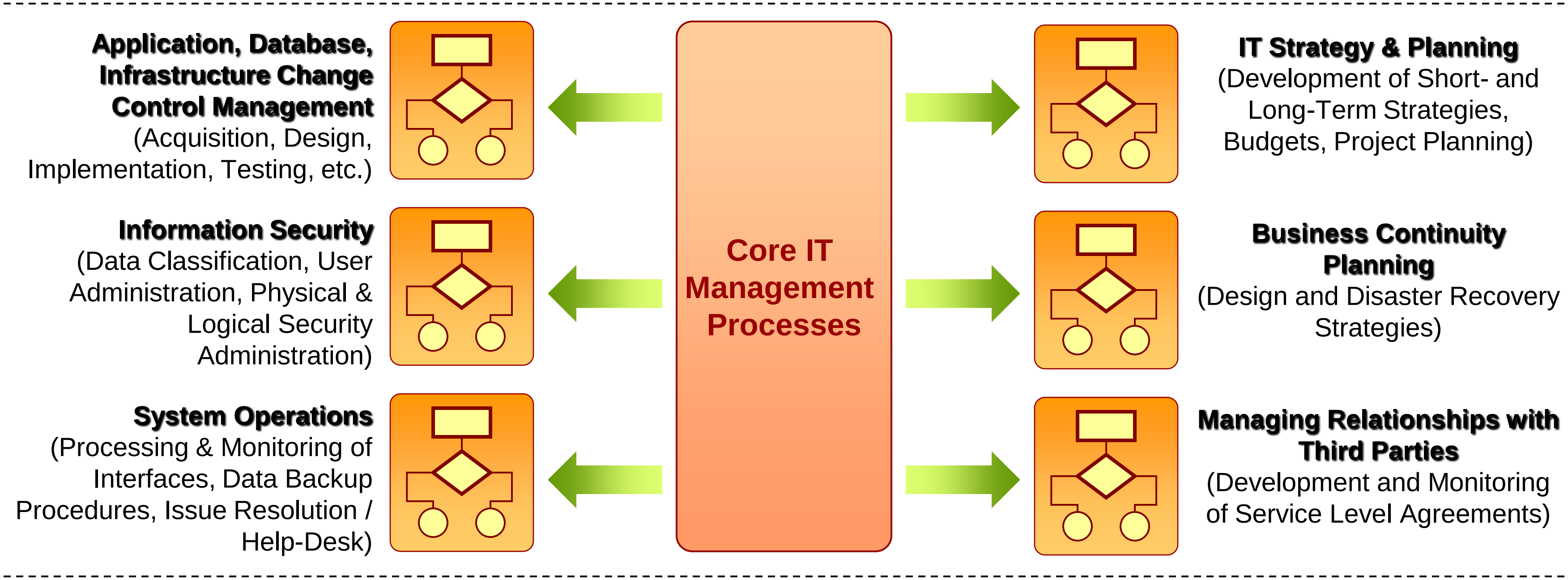
1. The world of IT
2. IT Control Environment
3. IT Dependent Manual Controls
4. Application Controls
5. IT General Controls
6. Program Changes
7. Computer Operations
8. ITGC Walk-Through and Testing

IT General Controls (ITGC) – Definition

- Defined as “controls that have a pervasive impact on the systems supporting the process being audited, including controls on which other controls (either manual or automated) are dependent.”;
- They are the processes that the IT function uses to manage and control the IT environment (people, processes, and technology);
- IT general controls give reliance that an IT process is operating consistently over time.

IT General Controls Overview

***IT General Controls* (ITGC) are designed to preserve *Confidentiality, Integrity* and *Availability* objectives. ITGCs are critical to support the integrity of IT-enabled processes, data, and application functions and are embedded within the following traditional IT management functions / processes. ITGCs can be manual or automated:**



Core IT Management Processes

Application, Database, Infrastructure Change Control Management
(Acquisition, Design, Implementation, Testing, etc.)

Information Security
(Data Classification, User Administration, Physical & Logical Security Administration)

System Operations
(Processing & Monitoring of Interfaces, Data Backup Procedures, Issue Resolution / Help-Desk)

IT Strategy & Planning
(Development of Short- and Long-Term Strategies, Budgets, Project Planning)

Business Continuity Planning
(Design and Disaster Recovery Strategies)

Managing Relationships with Third Parties
(Development and Monitoring of Service Level Agreements)

Testing IT General Controls

- Testing an application control or IT-dependent manual control normally gives assurance that the control operated effectively at that (single)point in time;

- How do we gain assurance that these controls have operated in a consistent and reliable fashion over the financial year, or that they will continue to operate going forward? (impossible)

- Auditors evaluate and test IT general controls.

Key IT General Controls

- Access to programs and data
- Program change
- Computer operations

Topic Overview

1. The world of IT
2. IT Control Environment
3. IT Dependent Manual Controls
4. Application Controls
5. IT General Controls
6. Program Changes
7. Computer Operations
8. ITGC Walk-Through and Testing

Access to Programs and Data

- Security control mechanisms;
- Powerful system or user IDs;
- Security control procedures;
- Segregation of duties.

Access to Programs and Data—Security Control Mechanisms

Objective: Determine that logical and physical access to IT computing resources is appropriately restricted.

Key control elements and testing considerations:

- Access to computing facilities is physically secured and limited to authorized individuals.
- Unique user IDs are used to provide individual accountability.
- Passwords with robust syntax are in place.
- Effective logging mechanisms and management review activities are in place.

Program Changes - Authorized Changes and Relevant Procedures

Objective: Determine that controls are in place to ensure that any changes to the systems/applications have been properly authorized by an appropriate level of management.

Key control elements and considerations:

- The organization established a formal change management process.
- All change requests to systems/applications are formally documented.
- Audit trail of changes that can be traced and vouched to originating requests

Program Changes—Testing of Program Changes

Objective: Determine that controls are in place to ensure that changes to applications and systems are tested, validated, and approved before being placed into production.

Key control elements and considerations:

- Separate testing environment from production was established.
- Only a limited number of people should have access to move authorized changes into production.

Topic Overview

1. The world of IT
2. IT Control Environment
3. IT Dependent Manual Controls
4. Application Controls
5. IT General Controls
6. Program Changes
7. Computer Operations
8. ITGC Walk-Through and Testing

Methods of Testing Computer Operations

- Backup/recovery;
- Backup restoration testing;
- Access to backup media and offsite storage;
- Problem management.

Computer Operations—Backup/Recovery

Objective:

Determine that management has implemented appropriate backup and recovery procedures so that data, transactions, and programs can be recovered.

Key control elements and testing considerations:

- Responsibility for performing backups is assigned to IT operations personnel;
- Backup schedule and program/data retention requirements are formally defined and in place;
- Backups are sent offsite to an environmentally and physically secure location where they can be retrieved timely if ever the need arises.

Computer Operations—Access to Backup Media/Offsite Storage

Objective:

Determine that appropriate controls are in place over the backup media for systems and applications, including that only authorized people have access to the tapes and tape storage.

Key control elements and testing considerations:

- Backup media is maintained locally and remotely offsite is secured from unauthorized access.
- Use of physical and logical data-access controls are in place to prevent unauthorized users from gaining access to backup data.

Computer Operations—Problem Management

Objective:

Determine that management has defined and implemented, in a timely manner, problem management procedures to record, analyze, and resolve incidents, problems, and errors for systems and applications.

Key control elements and testing considerations:

- There is a formal monitoring of the production environment.
- Logging and reporting of all incidents in production are tracked until appropriately resolved.
- All user-identified incidents/failures are reported, logged, and investigated until resolved.

Topic Overview

1. The world of IT
2. IT Control Environment
3. IT Dependent Manual Controls
4. Application Controls
5. IT General Controls
6. Program Changes
7. Computer Operations
8. ITGC Walk-Through and Testing

ITGCs Testing

Objective: Evaluate the design and operating effectiveness of controls.

Design effectiveness:

- Document IT general controls.
- Walk through IT general controls or inquiry and observation.
- Evaluate any design deficiencies.

Operational effectiveness:

- Test controls.
- Evaluate any operational deficiencies.

Effective ITGC Controls

Overall, when pervasive ITGCs are operating as intended, they:

- **Do** provide a basis for reliance that the systems are operating consistently over time and should continue to operate going forward
- **Do not** provide the basis for reliance that data processing and reports are correct

Physical and Environmental Controls (Cont.)

Threats and Vulnerabilities:

- **Environmental threats (earthquakes, fires, floods, terrorism, vandalism etc.)**
- **Failure of supporting utilities (electric power, air conditioning, heating, communication lines etc.)**
- **Unauthorized physical access**
  - Theft of equipment, computer devices, physical and electronic files, documents etc
  - Disclosure, modification and improper physical access to information and data
  - Tampering electronic devices and vandalism
  - Circumvention of internal logical controls and delayed processing
- **Human Errors**
- **Hardware Errors**

Physical and Environmental Controls (Cont.)

Safeguards and Controls:

- Physical security policies and procedures
- Electronic access control systems
- Intrusion detection and alarm systems
- Manned Receptions, Guards, Security Patrols
- Fire detection and suppression systems and response procedures
- Uninterrupted Power Supply (UPS), emergency generators
- Temperature, humidity monitoring systems and air conditioning
- Cable shielding and equipment tempest protection
- Equipment operation and maintenance procedures
- Many others …

Logical Access Controls

- Access is the ability to do something with a computer resource (e.g., use, change, or view);
- Access control is the means by which the ability is explicitly enabled or restricted in some way (usually through physical and system-based controls);
- Logical access controls can prescribe not only who or what (e.g., in the case of a process) is to have access to a specific system resource but also the type of access that is permitted.

Logical Access Controls (Cont.)

- Access Criteria (criteria for granting or denying access)
  - Identity
  - Roles
  - Location
  - Time
  - Transaction
- Common Access Modes
  - Read access
  - Write access
  - Execute access

Typical Tests of Logical Access Controls

- Identify the population of new or current users and select a sample;
- Verify access is authorized/appropriate for role;
- Identify the population of terminated users that have left during the audit period and select a sample of those users;
- Verify access has been removed or disabled.

Identification & Authentication

Identification is the means by which a user provides a claimed identity to the system

Authentication is the means of establishing the validity of this claim

- Something the individual knows (a secret -- e.g., a password, Personal Identification Number (PIN)
- Something the individual possesses (a token -- e.g., an ATM card or a smart card)
- Something the individual is (a biometric -- e.g., such characteristics as a voice pattern, handwriting dynamics, or a fingerprint)

Thank you for your attention!