Rijksacademie voor Financiën,
Economie en Bedrijfsvoering
Ministerie van Financiën

Навчання з IT-аудиту
День 2

Київ, грудень 2017

Манфред ван Кестерен
Яспер Венеман

Rijksacademie voor Financiën,
Economie en Bedrijfsvoering
Ministerie van Financiën

- Початок - 10.00
- Перерва на каву 11:20-11:40
- Обід 13:00-14:00
- Перерва 15:15-15:25
- Завершення 16:15

Порядок денний

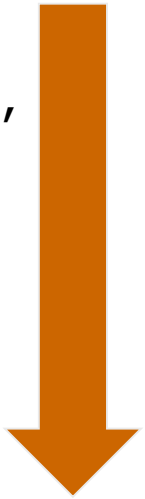
- **Управління IT**
  - Об'єкти аудиту в IT-управлінні
- Рамки IT-аудиту
  - COBIT, ITIL, Prince2, ISO27002
- Цілі IT заходів контролю
  - Конфіденційність, правдивість, доступність
- IT ризики
- Модель IT-контролю
  - Розподіл обов'язків
  - Ручні заходи контролю
  - Заходи контролю на рівні прикладної програми
  - Загальні IT-заходи контролю

Об'єкти аудиту в IT-управлінні (I)

Корпоративний рівень	Рівні		Види контролю
Стратегічний рівень	**Бізнес-рівень**	**Рівень безпеки**	Заходи контролю щодо користувача
	Рівень користувача		
Тактичний рівень	**Прикладний рівень**		Заходи контролю щодо прикладної програми
Операційний рівень	**Проміжний рівень**		Загальні заходи IT-контролю
	Системний рівень		
	Мережевий рівень		
	Фізичний рівень		
	УПРАВЛІННЯ IT-СЛУЖБОЮ		

Об'єкти аудиту в IT-управлінні (II)

4. Організація (відділення, управління і контроль, завдання)
3. Процеси (управління постачальниками, технічна підтримка, тощо)
2. Прикладні програми (SAP, Windows, проектне програмне забезпечення, тощо)
1. Інфраструктура (бази даних, міжмережевий екран, тощо)



Найбільше ризиків в IT мають місце на 2 і 1 рівнях!

Об'єкти аудиту – організація

- Аудити на *стратегічному і тактичному* рівнях міністерства, агентств і підрядних організацій.

- Аудити щодо управління і контролю, ризику та дотримання правил, архітектури, управління портфоліо.

- ❑ Стратегічне узгодження бізнесу і IT
- ❑ Управління архітектурою підприємства
- ❑ Управління портфоліо
- ❑ Джерела рішень
- ❑ Управління і контроль

Об'єкти аудиту: IT процеси і процедури

Аудити на *операційному* рівні міністерства, агентств та підрядних організацій. IT-департамент відповідає за виконання низки IT процесів і процедур.

- Працівник: “Мій аккаунт заблоковано”
- Виявлено підозрілу мережеву діяльність у файлі входу на міжмережевий екран
- Запущено новий веб-сайт.

- Працівника перевели із відділу закупівель у відділ продаж

Управління інцидентами

Управління безпекою

Управління змінами

Управління випуском

Управління доступом

Вимога виконання

Об'єкти аудиту – застосунки

- Операційні системи: Windows / Linux / CentOS /
- Системи управління базами даних
- Системи управління документами
- Фінансові застосунки: SAP / Oracle
- Застосунки щодо закупівель
- Застосунки щодо заробіної плати

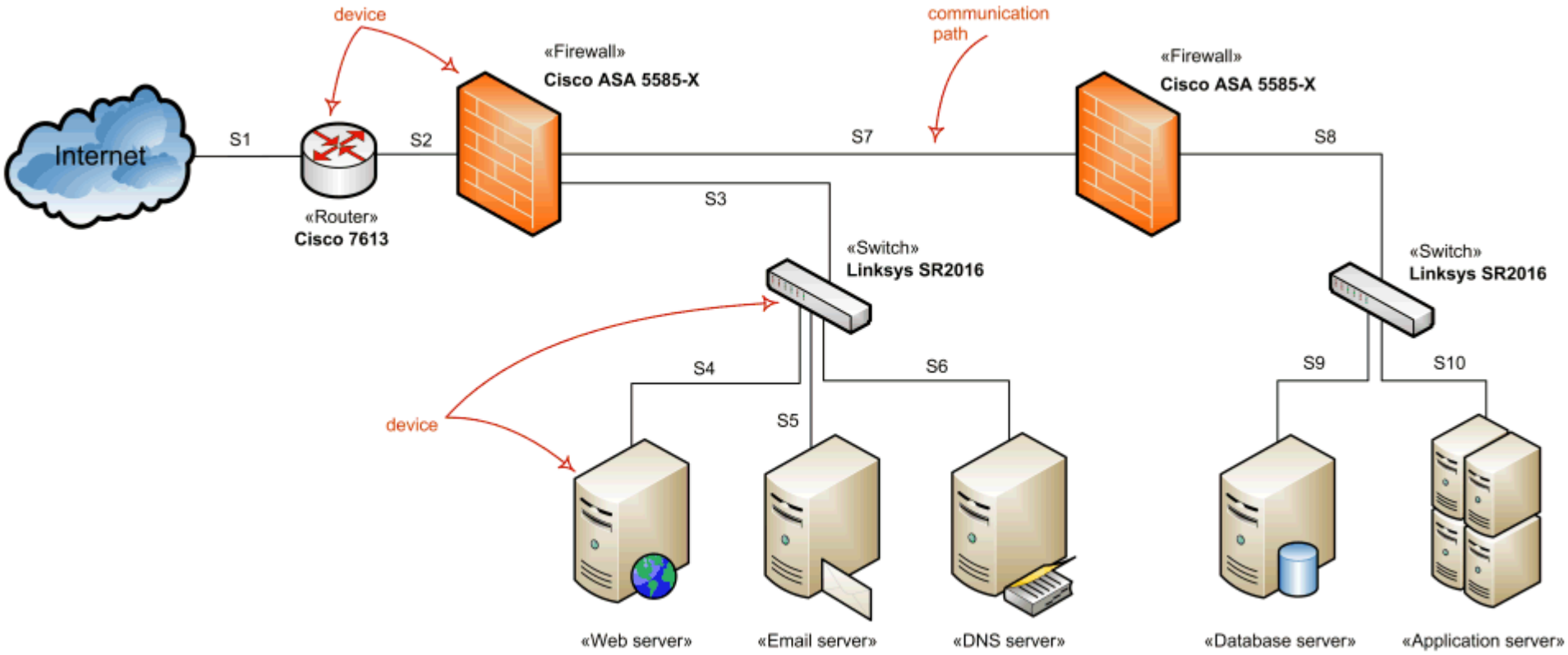
UNIX®

Apache

WordPress

Об'єкти аудиту - інфраструктура

- Аудит на рівні периметру: такі технічні компоненти як: міжмережевий екран, вирівнювач навантаження, веб-сервер, сервер застосунку, сервер бази даних.



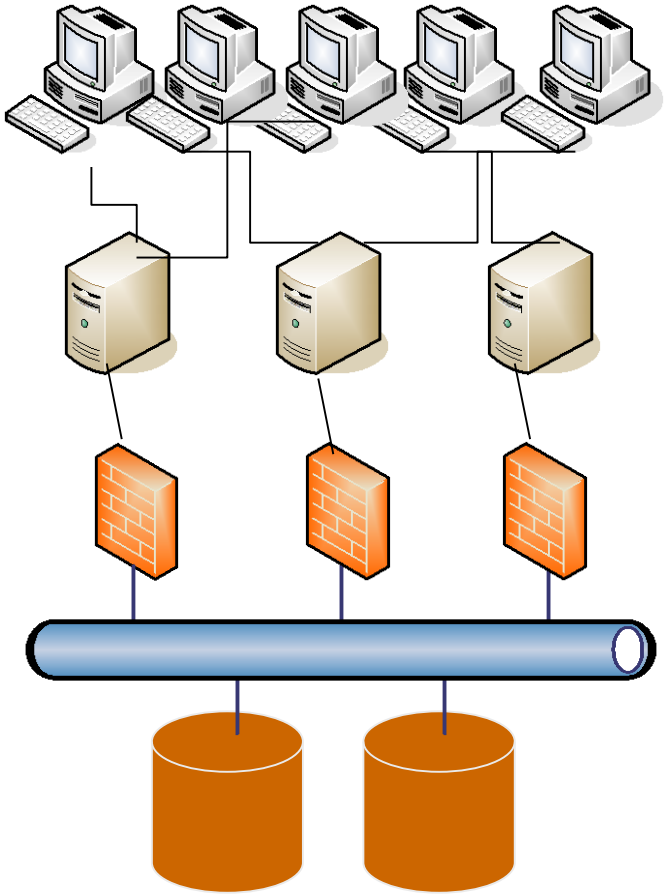
Загальні IT спостереження

Зрозуміти IT середовище на рівні установи:

- Визначити важливі прикладні програми та інфраструктуру

Ціль:

1. Зв’язок між організаційними підрозділами і процесами
2. Зв’язок між процесами і прикладними програмами
3. Зв’язок між прикладними програмами та інфраструктурою



Порядок денний

- Управління IT
  - Об'єкти аудиту в IT-управлінні
- **Рамки IT-аудиту**
  - COBIT, ITIL, Prince2, ISO27002
- Цілі IT заходів контролю
  - Конфіденційність, правдивість, доступність
- IT ризики
- Модель IT-контролю
  - Розподіл обов'язків
  - Ручні заходи контролю
  - Заходи контролю на рівні прикладної програми
  - Загальні IT-заходи контролю

Рамки аудиту (стандарти) в IT-аудиті

- CobIT (забезпечує нормами/стандартами на основі найкращих практик належного IT-управління)
- ITIL (управління IT-службою)
- Prince2 (управління проектом)
- ISO27001/2 (Безпека інформації)
- Найкращі практики провайдерів програмного забезпечення (CIS; NIST)
- Тощо.

Залежно від об'єкту (цілі) аудиту пристосовуються стандарти/посилання!

Рамки аудиту (стандарти) в IT-аудиті

	Приклади рамок аудиту
4. Організація	ITIL, COBIT, Prince2
3. Процеси	ITIL, COBIT, ISO27001/2,
2. Прикладні програми	Рамки для конкретних прикладних програм SAP, Apache. Критерії від постачальника
1. Інфраструктура	Орієнтири від CIS & NIST Критерії від постачальника.

Залежно від об'єкту (цілі) аудиту пристосовуються стандарти/рамкові основи!

COBIT 5 Process Reference Model

Processes for Governance of Enterprise IT

Evaluate, Direct and Monitor

- **EDM01** Ensure Governance Framework Setting and Maintenance
- **EDM02** Ensure Benefits Delivery
- **EDM03** Ensure Risk Optimisation
- **EDM04** Ensure Resource Optimisation
- **EDM05** Ensure Stakeholder Transparency

Adobe Acrobat Document

Align, Plan and Organise

- **APO01** Manage the IT Management Framework
- **APO02** Manage Strategy
- **APO03** Manage Enterprise Architecture
- **APO04** Manage Innovation
- **APO05** Manage Portfolio
- **APO06** Manage Budget and Costs
- **APO07** Manage Human Resources
- **APO08** Manage Relationships
- **APO09** Manage Service Agreements
- **APO10** Manage Suppliers
- **APO11** Manage Quality
- **APO12** Manage Risk
- **APO13** Manage Security

Build, Acquire and Implement

- **BAI01** Manage Programmes and Projects
- **BAI02** Manage Requirements Definition
- **BAI03** Manage Solutions Identification and Build
- **BAI04** Manage Availability and Capacity
- **BAI05** Manage Organisational Change Enablement
- **BAI06** Manage Changes
- **BAI07** Manage Change Acceptance and Transitioning
- **BAI08** Manage Knowledge
- **BAI09** Manage Assets
- **BAI10** Manage Configuration

Deliver, Service and Support

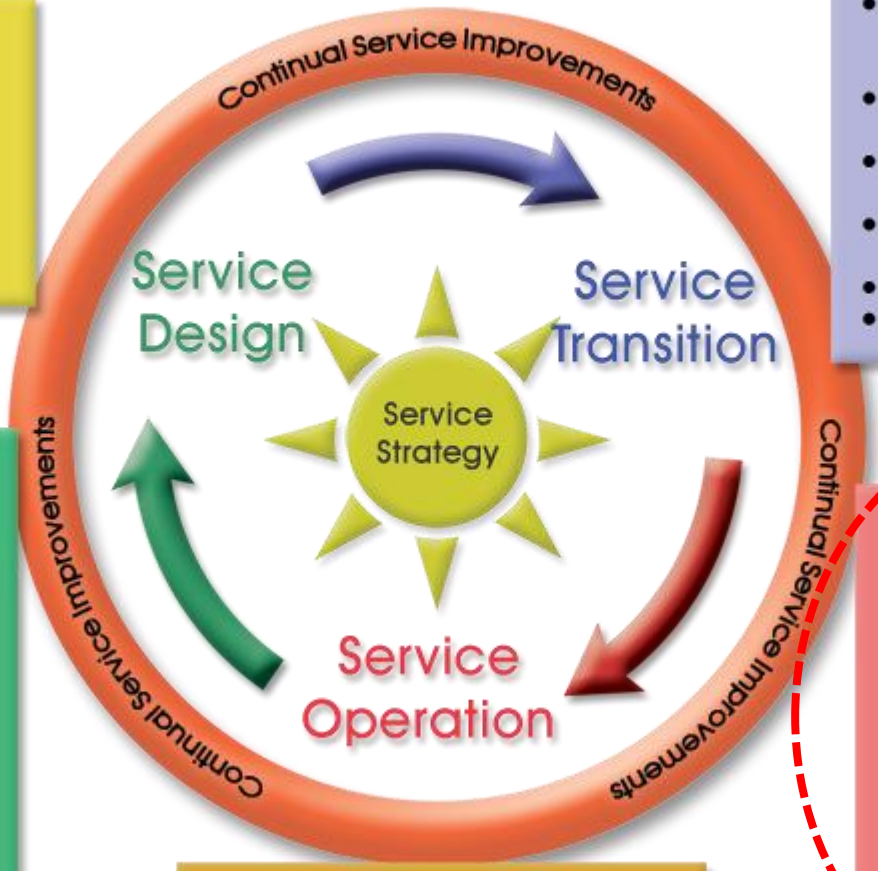
- **DSS01** Manage Operations
- **DSS02** Manage Service Requests and Incidents
- **DSS03** Manage Problems
- **DSS04** Manage Continuity
- **DSS05** Manage Security Services
- **DSS06** Manage Business Process Controls

Monitor, Evaluate and Assess

- **MEA01** Monitor, Evaluate and Assess Performance and Conformance
- **MEA02** Monitor, Evaluate and Assess the System of Internal Control
- **MEA03** Monitor, Evaluate and Assess Compliance With External Requirements

Processes for Management of Enterprise IT

ITIL® SERVICE LIFECYCLE



Service Strategy
- Service Portfolio Management
- Financial Management
- Demand Management
- ROI

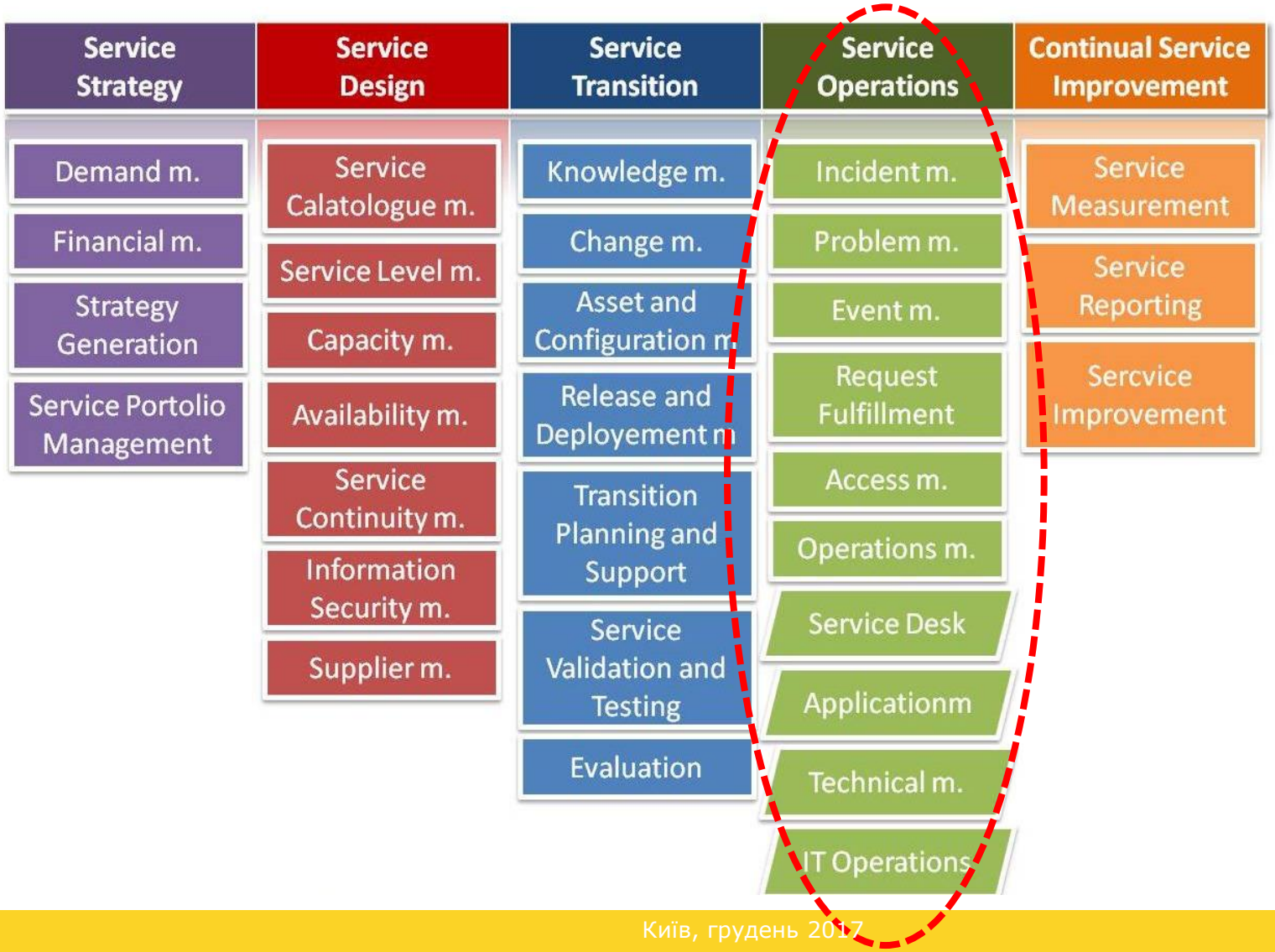
Service Transition
- Transition Planning and Support
- Change Management
- Service Asset and Configuration Management
- Release and Deployment Management
- Service Validation Management
- Service Validation and Testing
- Evaluation
- Knowledge Management

Service Design
- Service Catalog Management
- Service Level Management
- Capacity Management
- Availability Management
- IT Service Continuity Management
- Information Security Management

Service Operation
- Event Management
- Incident Management
- Request Fulfillment
- Problem Management
- Access Management

Functions
- Service Desk
- Technical Management
- Application Management
- Operations Management

Continual Service Improvements
- Seven Step Improvement


Service Strategy
Service Design
Service Transition
Service Operations
Continual Service Improvement
Demand m.
Financial m.
Strategy Generation
Service Portolio Management
Service Calatologue m.
Service Level m.
Capacity m.
Availability m.
Service Continuity m.
Information Security m.
Supplier m.
Knowledge m.
Change m.
Asset and Configuration m.
Release and Deployement m
Transition Planning and Support
Service Validation and Testing
Evaluation
Incident m.
Problem m.
Event m.
Request Fulfillment
Access m.
Operations m.
Service Desk
Applicationm
Technical m.
IT Operations
Service Measurement
Service Reporting
Sercvice Improvement

Prince 2: Рамки для IT-проектів

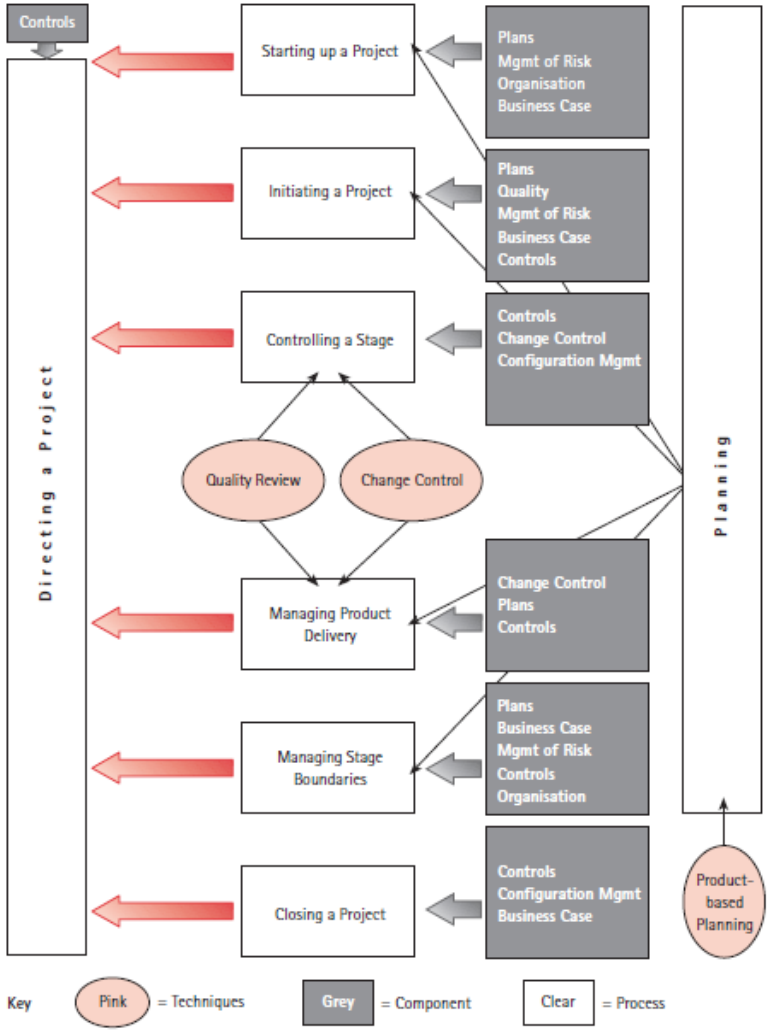
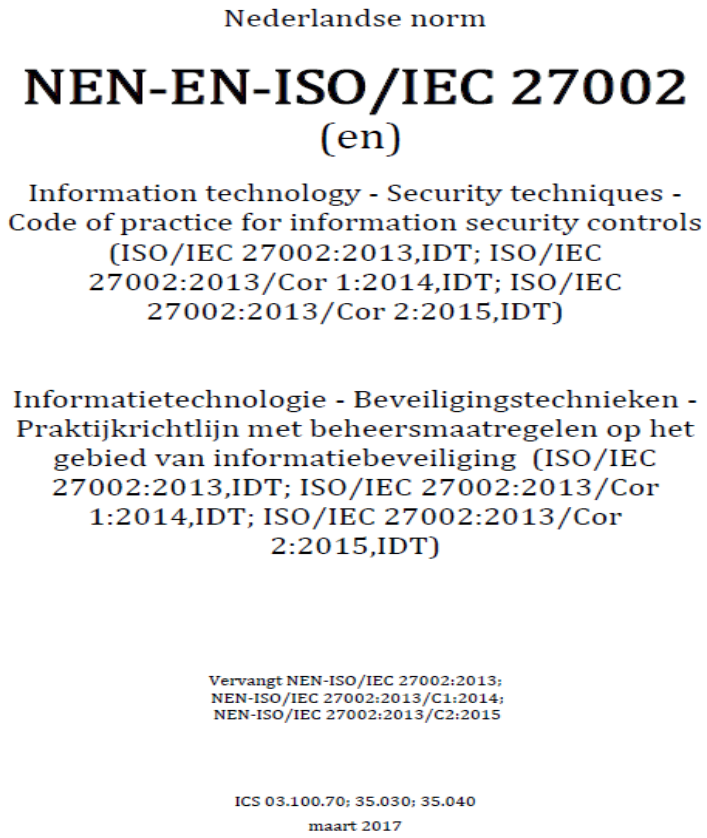


Figure 2.6 Use of PRINCE2 components and techniques in the processes

Adobe Acrobat Document

ISO27002: рамкові основи для безпеки інформації



Nederlandse norm

NEN-EN-ISO/IEC 27002

(en)

Information technology - Security techniques - Code of practice for information security controls (ISO/IEC 27002:2013,IDT; ISO/IEC 27002:2013/Cor 1:2014,IDT; ISO/IEC 27002:2013/Cor 2:2015,IDT)

Informatietechnologie - Beveiligingstechnieken - Praktijkrichtlijn met beheersmaatregelen op het gebied van informatiebeveiliging (ISO/IEC 27002:2013,IDT; ISO/IEC 27002:2013/Cor 1:2014,IDT; ISO/IEC 27002:2013/Cor 2:2015,IDT)

Vervangt NEN-ISO/IEC 27002:2013; NEN-ISO/IEC 27002:2013/C1:2014; NEN-ISO/IEC 27002:2013/C2:2015

ICS 03.100.70; 35.030; 35.040

maart 2017

Порядок денний

- Управління IT
  - Об'єкти аудиту в IT-управлінні
- Рамки IT-аудиту
  - COBIT, ITIL, Prince2, ISO27002
- **Цілі IT заходів контролю**
  - Конфіденційність, правдивість, доступність
- IT ризики
- Модель IT-контролю
  - Розподіл обов'язків
  - Ручні заходи контролю
  - Заходи контролю на рівні прикладної програми
  - Загальні IT-заходи контролю

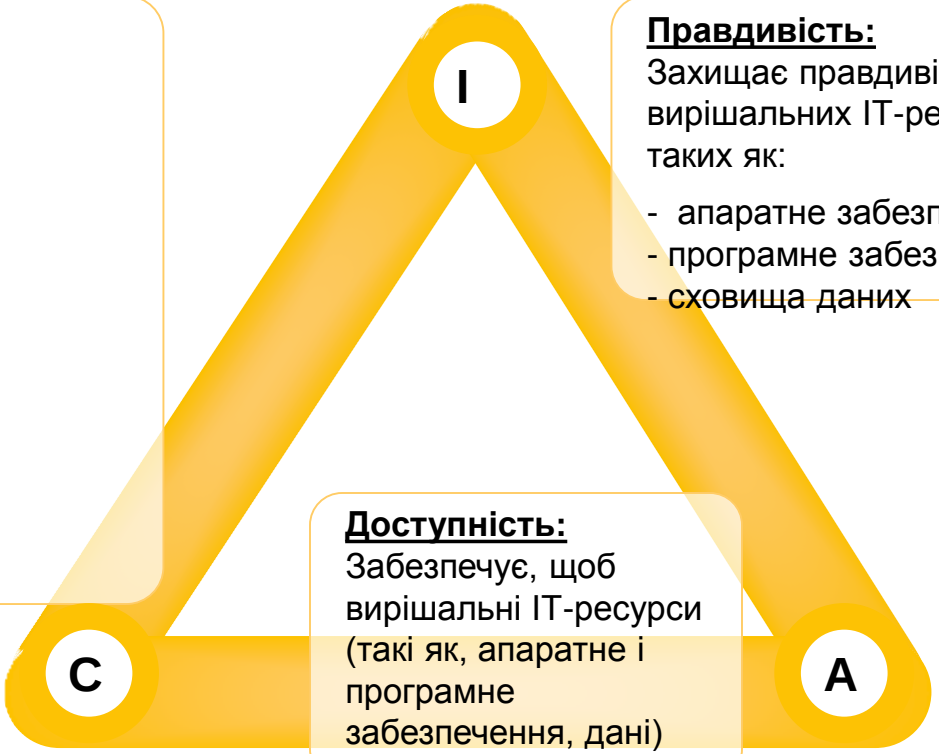
Цілі IT-заходів контролю

IT-заходи контролю розроблені для досягнення цілей контролю, пов'язаних з вимогами *Безпеки інформації.* Ключові цілі, які часто називають *C-I-A*, можна відобразити наступним чином:

Конфіденційність:
Захищає вразливу інформацію від перегляду неавторизованими користувачами.
Приклади:

- Фінансові дані
- Номери кредиток
- Номер соцстрахування

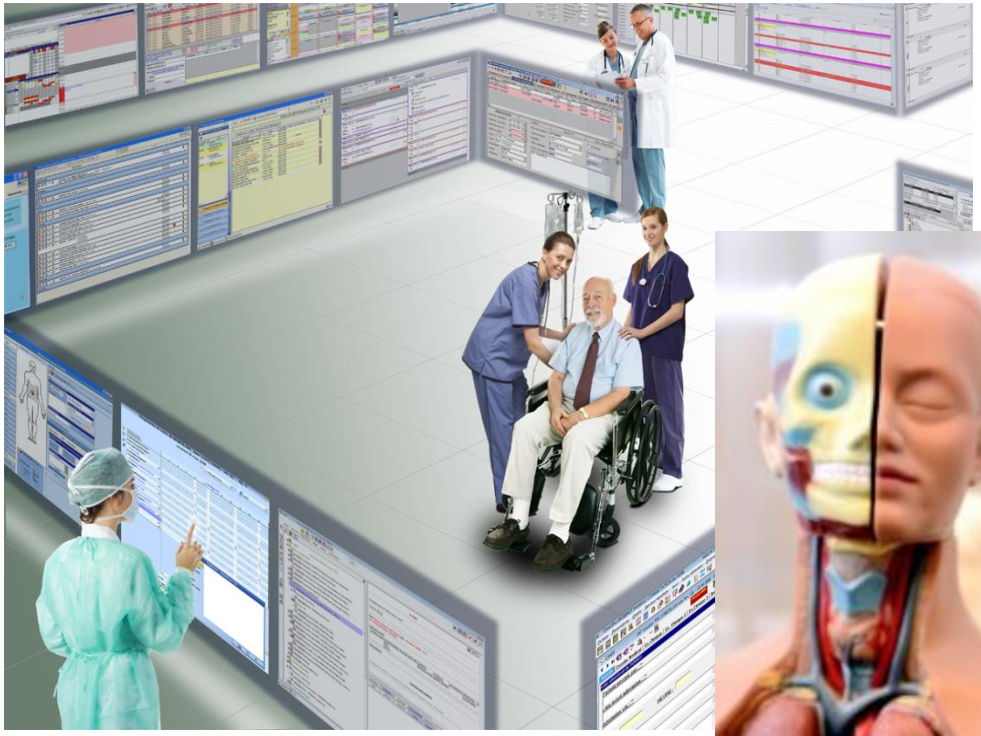
Примітка: Ця ціль прямо пов'язана із внутрішніми і зовнішніми вимогами щодо *Приватності*

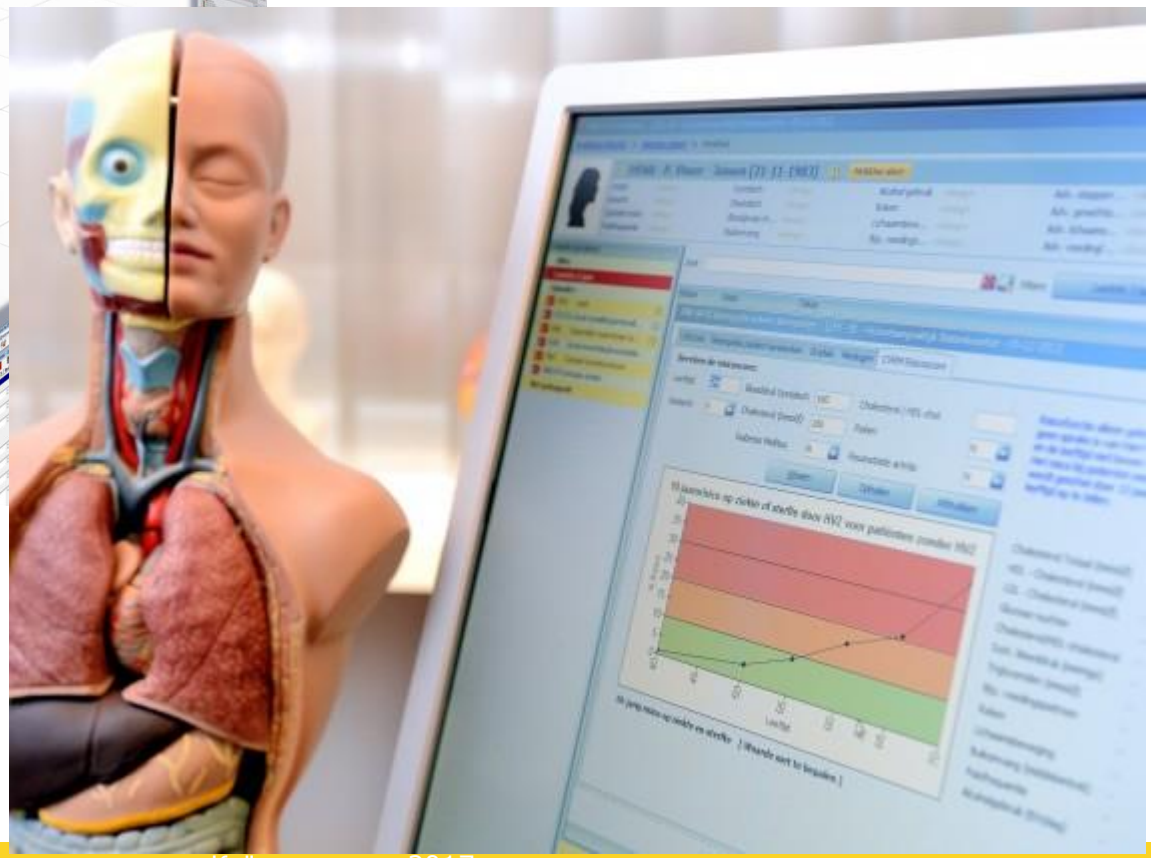


Правдивість:
Захищає правдивість вирішальних IT-ресурсів, таких як:

- апаратне забезпечення
- програмне забезпечення
- сховища даних

Доступність:
Забезпечує, щоб вирішальні IT-ресурси (такі як, апаратне і програмне забезпечення, дані) були доступними у потрібний час.





Dutch State Treasury Agency
Ministry of Finance

Home | News | Subjects | Organisation

search

Sitemap

Agency News

Reopening 3-year bond raises € 2.985 billion

9 June 2015

The reopening of the 3-year 'DSL 0.00% 15 April 2018' today raised an amount of € 2.985 billion.

Dutch State reopens 3-year bond

3 June 2015

On Tuesday 9 June 2015 the Dutch State will reopen the 'DSL 0 % 15 April 2018'.

Reopening 5-year bond raises EUR 2.35 billion

26 May 2015

The reopening of the 5-year 'DSL 0.25% 15 January 2020' today raised an amount of € 2.35 billion.

› More news

Spotlight

Subjects

- Guarantee scheme Propertize
- Funding policy
- Capital markets
- Money markets
- Risk management
- US Dollar Dutch State Bond
- Auction methods
- Primary Dealers
- Dutch Direct Auction
- CACs
- Multiplatform
- Settlement
- Debt securities Antilles
- Treasury banking
- Payment systems

Results most recent auctions

Dutch State Loan (DSL)

Auction date:	09-06-2015
Amount issued:	€ 2.985 bn

Volume of state debt

Position at the end of May 2015 in billion euros

Bonds	330.718
Treasury bills	14.710
Commercial paper	1.719
Private loans	4.505
Other	0
Total	**351.652**

Statistical Information

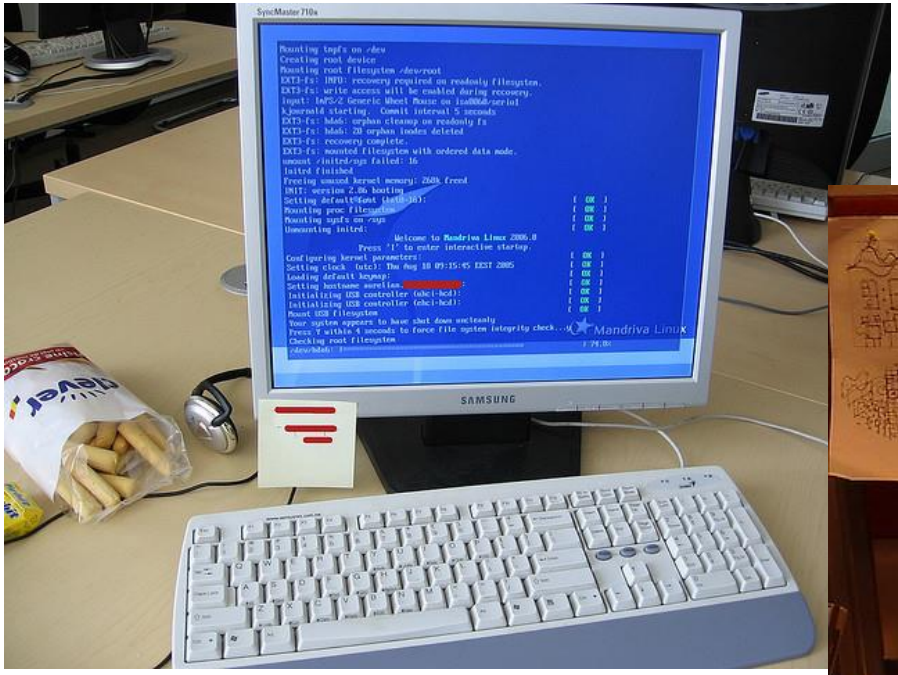
This link to Statistical Information gives you more detailed information on the volume of State debt and other relevant data.

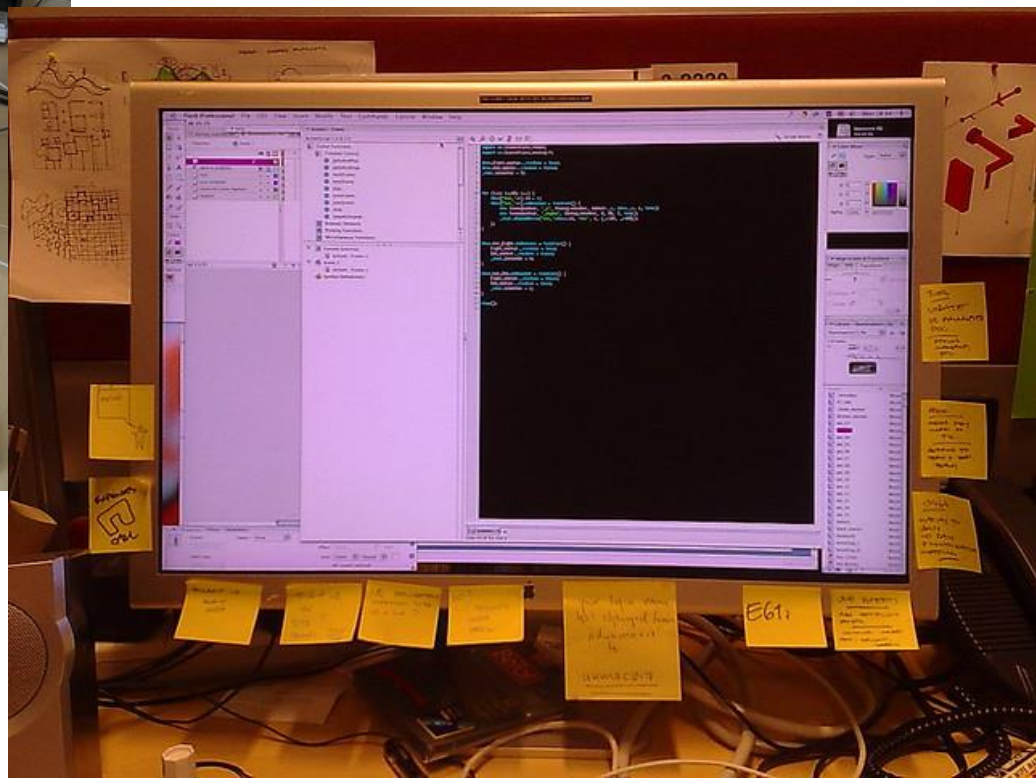
Contact information

The DSTA is part of the Dutch Ministry of Finance.

The DSTA is responsible for:

- the management and funding of the State debt
- organisation of treasury banking for the public sector
- the payment systems for the central government


SyncMaster 710s
SAMSUNG
Mandriva Linux



Порядок денний

- Управління IT
  - Об'єкти аудиту в IT-управлінні
- Рамки IT-аудиту
  - COBIT, ITIL, Prince2, ISO27002
- Цілі IT заходів контролю
  - Конфіденційність, правдивість, доступність
- **IT ризики**
- Модель IT-контролю
  - Розподіл обов'язків
  - Ручні заходи контролю
  - Заходи контролю на рівні прикладної програми
  - Загальні IT-заходи контролю

IT-ризики

IT середовища, IT-системи і IT-організації можуть бути дуже складними

Обережно визначайте обсяг IT-аудиту:

- Об'єкти аудиту
- Чи будете ви проводити аудит дизайну, наявності чи операційної ефективності заходів контролю?

Узгодьте це з клієнтом!

IT-ризики

Після визначення обсягу вам треба визначити Робочу програму IT-аудиту на основі:

Цілей аудиту

Об'єктів аудиту

Ризиків

Відповідних рамкових основ

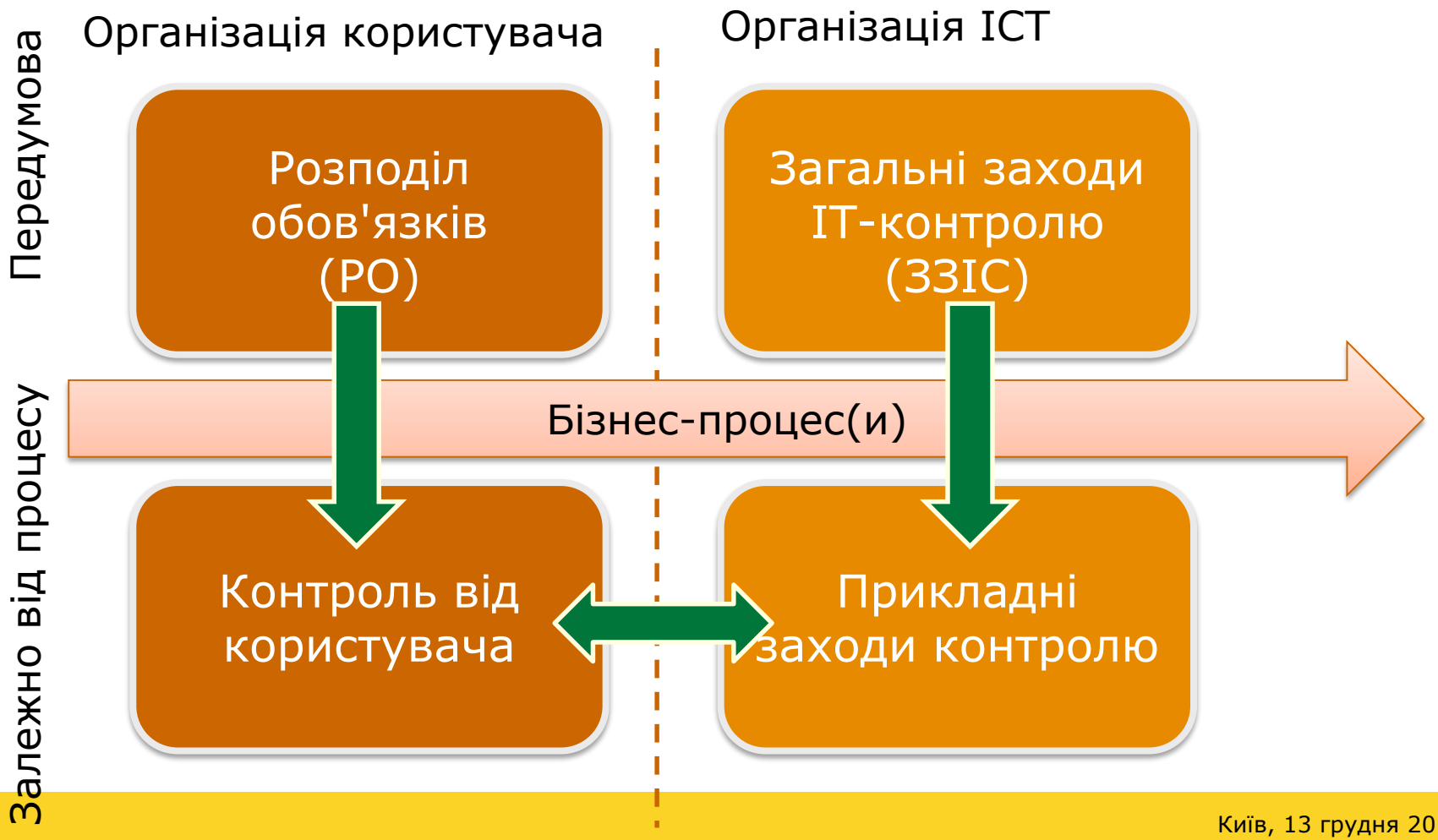
IT ризики

- Визначення обсягу вашого IT-аудиту
- “Розуміння бізнесу”
- Визначення і оцінка усіх ризиків, про які ви можете подумати
- Класифікація ризиків на високі, середні і низькі
- Визначення, чого можна досягнути в часових та бюджетних рамках
- Вибір заходів контролю, які ви очікуєте в IT-організації та IT-системі від міжнародних рамкових основ, напр., ISO 27001:2013 та ISO 27002:2013
- Побудова ваших рамкових основ і робочої програми, уточнення «що» і «як»
- Обговорення з клієнтом

Порядок денний

- Управління IT
  - Об'єкти аудиту в IT-управлінні
- Рамки IT-аудиту
  - COBIT, ITIL, Prince2, ISO27002
- Цілі IT заходів контролю
  - Конфіденційність, правдивість, доступність
- IT ризики
- **Модель IT-контролю**
  - Розподіл обов'язків
  - Ручні заходи контролю
  - Заходи контролю на рівні прикладної програми
  - Загальні IT-заходи контролю

Модель IT-контролю

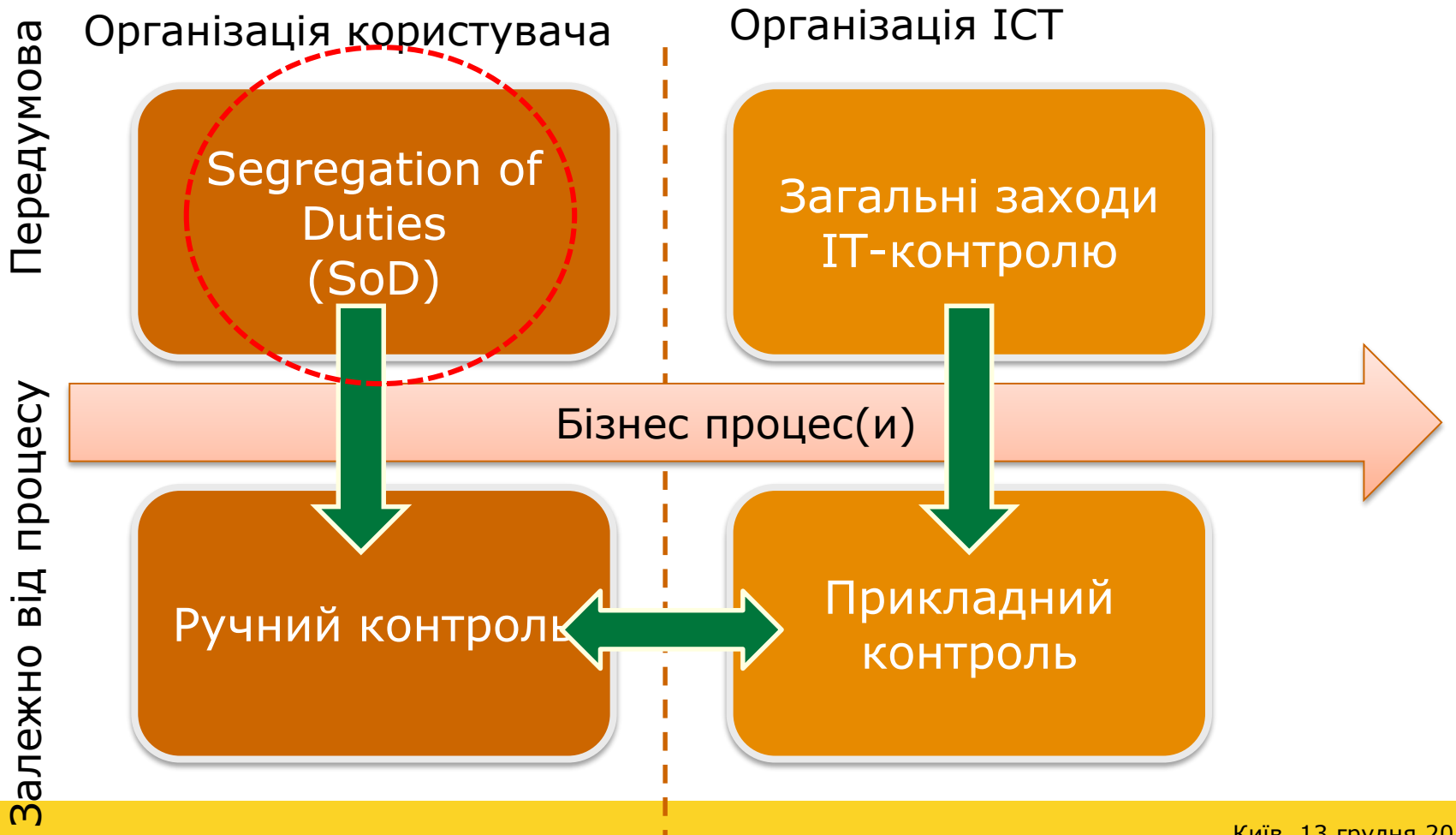


Огляд IT заходів контролю

Коли йдеться про IT заходи контролю, фактично можна говорити про дві категорії. ***Контрольні заходи щодо прикладних програм (AC),*** які включені у “стандартні” бізнес процеси (напр. закупівлі, доходи тощо) і розроблені з метою автоматизації функції контролю, тоді як ***загальні заходи контролю (ITGC)*** забезпечують підтримку вимог контролю в межах стандартних IT процесах підтримки.

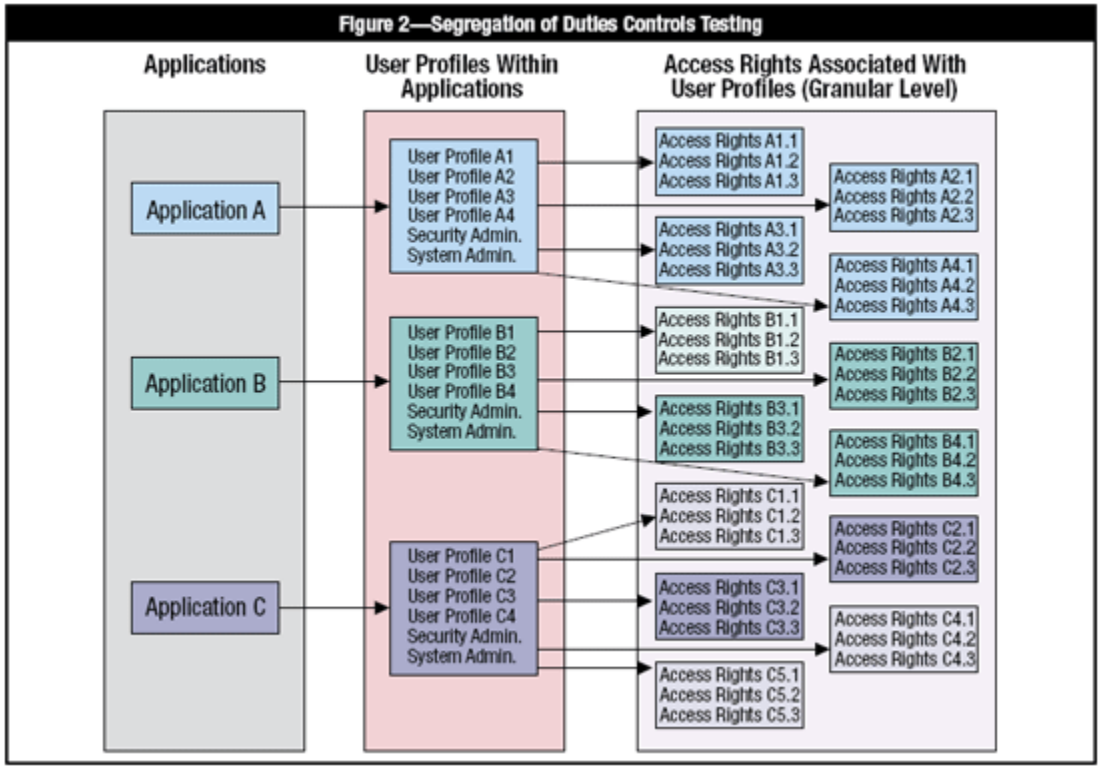
Аудитори тестують ***дизайн*** і ***операційну ефективність*** заходів контролю

Розподіл обов'язків

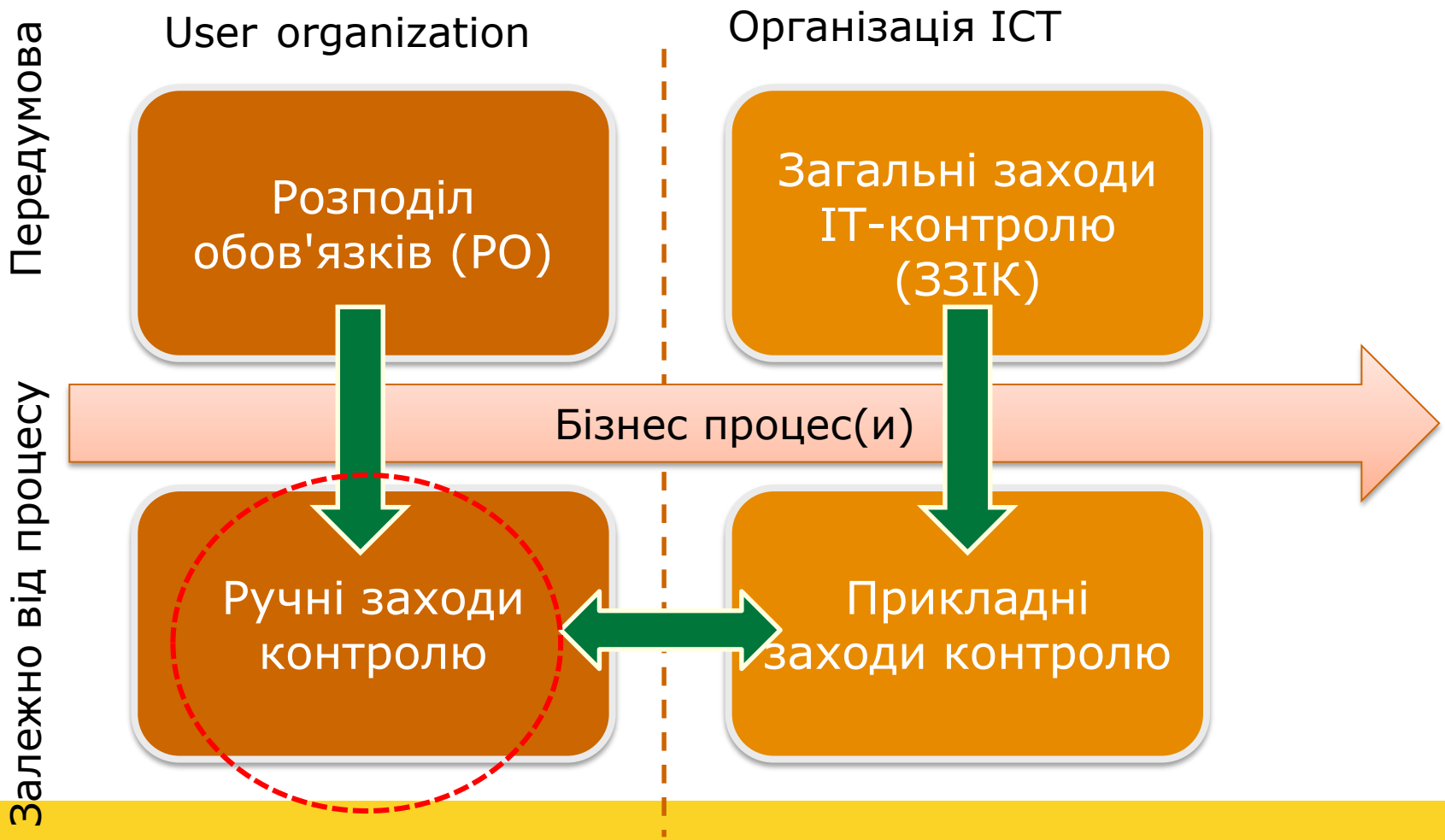


Розподіл обов'язків (РО)(II)

Актуальний погляд на права доступу користувача визначальний для виявлення можливих конфліктів РО



Ручні заходи контролю

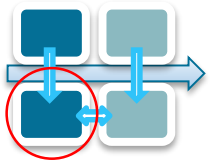


Автоматизовані проти ручних заходів контролю

IT-залежні ручні

Ручні

Автоматизовані



Автоматизовані проти ручних заходів контролю (продовж.)

Інструменти контролю	Автоматизований компонент	Ручний компонент
• Авторизація: Підтвердження проведення трансакцій відповідно до загальноприйнятих управлінських або особливих політик та процедур	• Онлайнова передача та підтвердження про затвердження	• Ручна форма затвердження, що передбачає особистий підпис
• Звіт про Виключення: підготовка звіту з метою моніторингу чогось; результати відображаються у рішенні	• Автоматизовані заходи контролю вживаються у випадку виявлення виключень в ході обробки даних	• Перегляд та своєчасне рішення щодо виключень
• Контроль інтерфейсу: повна та правильна передача даних між системами	• Автоматизований моніторинг передачі даних та коригування помилки	• Перегляд та своєчасне прийняття рішення у випадку виключення

IT-залежні, ручні заходи контролю (прод.)

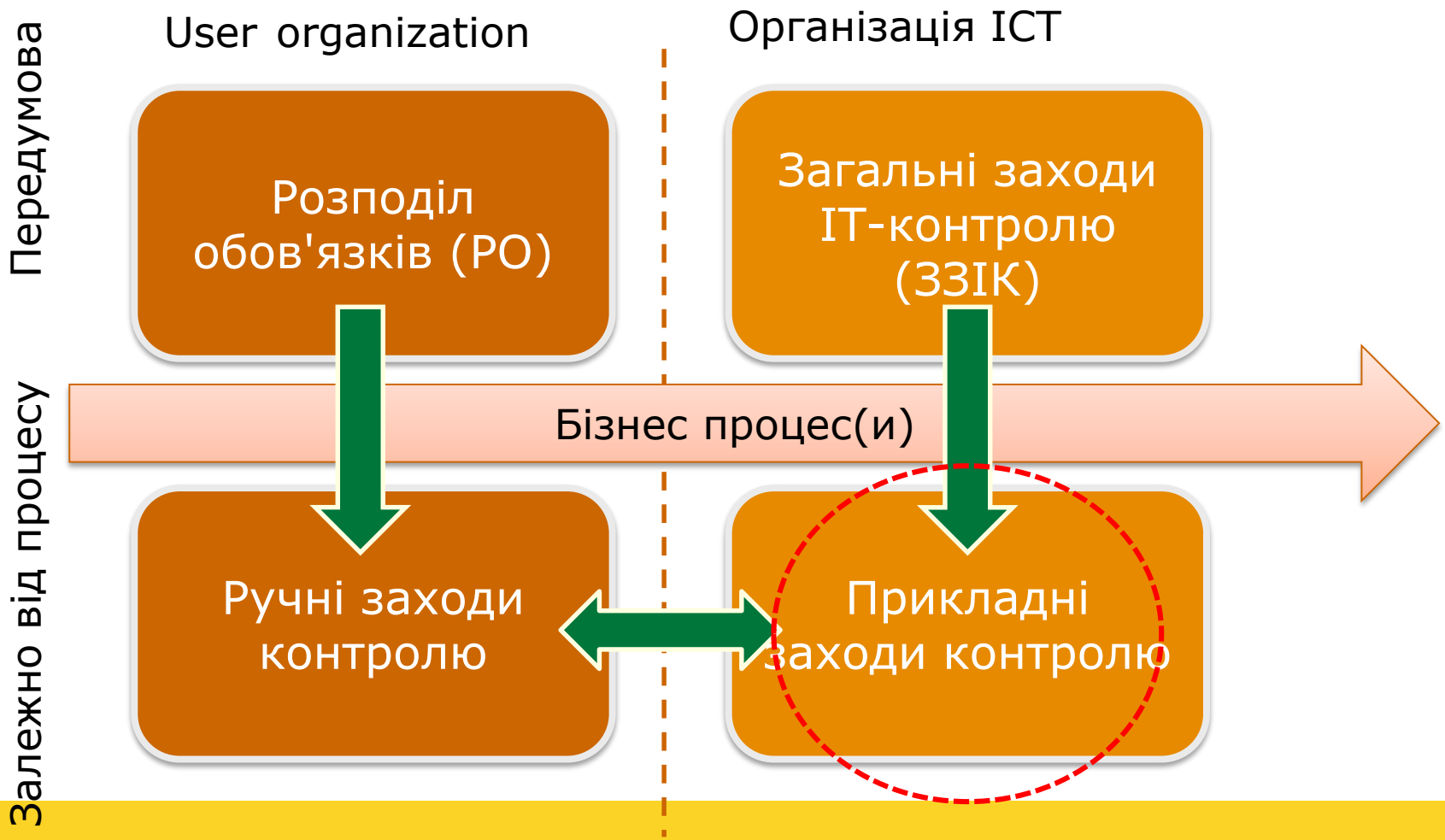
Види IT – залежних заходів контролю

- Узагальнені системні стандартні звіти
- Звіти за запитом/спеціальні звіти

Тестування припущень

- Для чого звіт використовується?
- Як використовується у контролі?
- Повнота, правильність, незалежність та існування
- Перегляд розрахунків

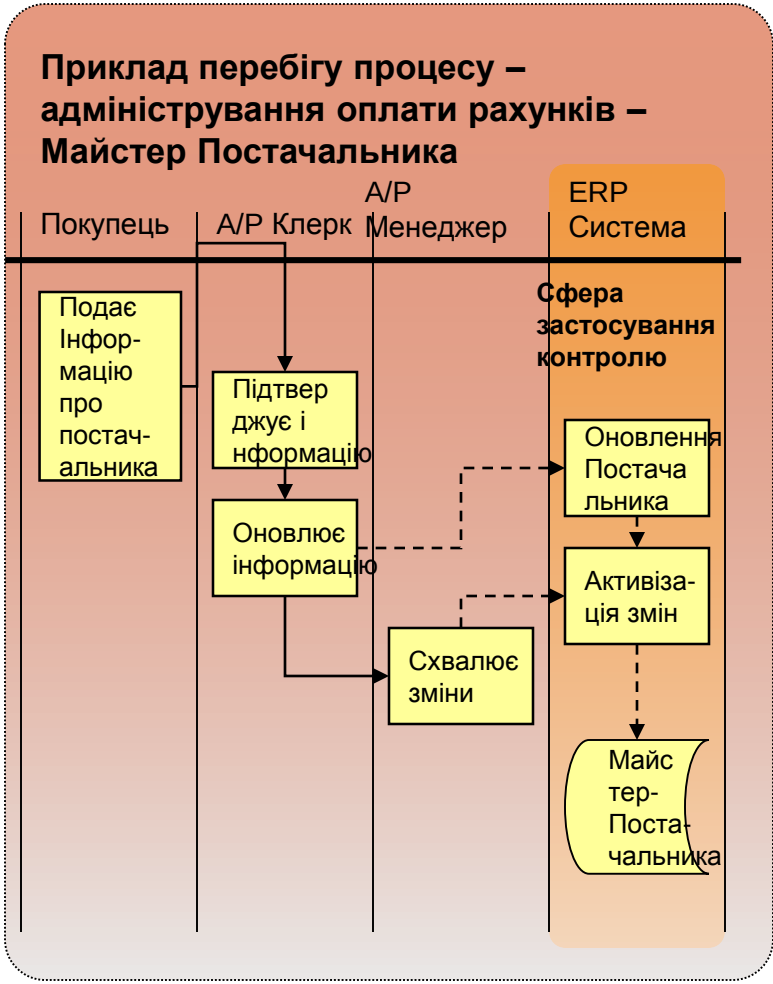
Прикладні заходи контролю



Контрольні заходи на рівні прикладної програми

Контрольні заходи на рівні прикладної програми – це системні заходи контролю в межах стандартних бізнес-процесів, які спрямовані на посилення конкретних практичних вимог. Такі *контрольні заходи* по своїй суті як правило носять попереджувальний характер. Приклади включають:

- Контроль логічного доступу
- Внесення даних / заповнення полів, що перевіряються (наприклад, перевірка даних номеру кредитної картки)
- Правила документообігу (напр. електронний обіг та передача вимог закупівлі)
- Поля, що є обов'язковими, виходячи із попередньо визначених показників (напр. цінова інформація)
- Передбачені робочі кроки, що попередньо визначають статус переходу (напр. відкрити > переглянути > закрити)
- Автоматизовані аудиторські записи
- Автоматизовані розрахунки



Тестування заходів контролю на рівні прикладної програми

Особливу увагу звертаємо на наступні компоненти заходів контролю на рівні прикладної програми:

- Параметри конфігурації та автоматизовані заходи контролю користувачів;

- *напр., заявки на закупівлі схвалювалися онлайн на основі погоджених керівництвом лімітів для погодження;*

- *напр., рахунки оплачуються тільки у випадку трикратного збігу із Замовленням на купівлю, Підтвердженням отримання товару/Довідці про постачання;*

- Заходи контролю щодо основних даних та доступ;

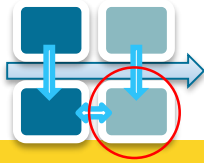
- напр., зміни, подані в обліковому записі клієнта має погодити інший працівник до того, як зміни стануть остаточними;

- Анулювання контролю;

- Розподіл обов'язків та функціональний доступ;

- напр., працівнику не дозволяється подавати рахунок і погоджувати той самий рахунок

- Контроль інтерфейсу



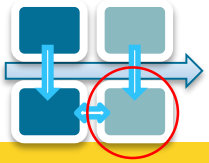
Тестування заходів контролю на рівні прикладної програми (прод.)

Як тестувати:

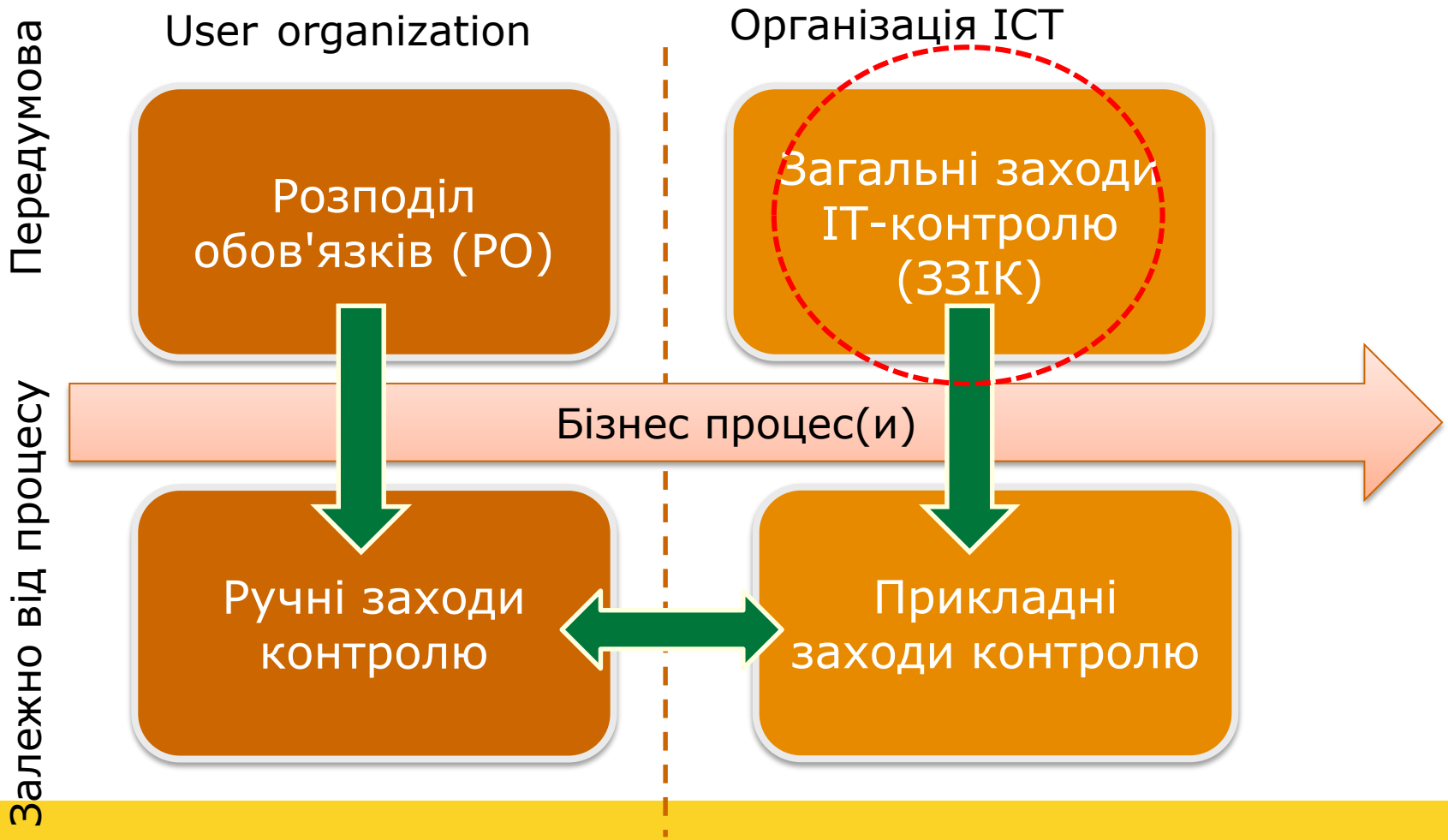
- Залежно від виду прикладної програми
- Залежно від того, чи прикладна програма «з полиці», чи адаптована

Основні кроки тестування:

- Підтвердження параметрів конфігурації;
- Проведення тестування через програмний модуль;
- Тестування безпеки доступу до функцій конфігурації / параметрів;
- Тестування управління змінами.



Загальні IT-заходи контролю

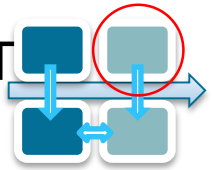


Загальні IT-заходи контролю (ITGC) – Визначення

- За визначенням “Загальні IT-заходи контролю (ITGC) – це заходи контролю, які застосовуються до усіх компонентів, процесів і даних системи для даної організації або середовища інформаційних технологій (IT). Цілі ITGCs полягають у забезпеченні належного розвитку і застосування прикладних програм, а також незалежності програми, файлів даних і компютерних операцій.”;

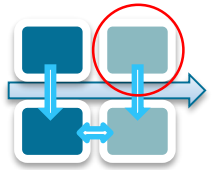
- Це процеси, які використовує IT функція для управління та контролю IT середовища (люди, процеси, технології);

- Загальні контрольні заходи IT забезпечують впевненість, що IT процеси функціонують послідовно в часі.



Найвідоміші загальні IT-заходи контролю

1. **Управління доступом (ACC)** ☑
2. **Управління змінами (CHA)** ☑
3. **Управління IT операціями (OPS)** ☑
4. **Управління інцидентами (INC)**
5. **Управління проблемами (PRO)**
6. Управління рівнем обслуговування (SLM)
7. Управління постачальниками (SUP)
8. Управління інфраструктурою (INF)
9. **Управління наявністю (AVA)**
10. **Управління безперервністю (CTY)**
11. **Управління конфігурацією (CON)**
12. **Управління спроможністю (CAP)**
13. Управління безпекою (SEC)



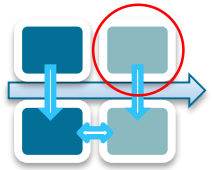
Тестування загальних IT-заходів контролю

- Як набути упевненості, що ці заходи контролю функціонували послідовним і надійним способом протягом фінансового року, і чи в тому, що вони продовжать так функціонувати?
- Аудитори оцінюють і тестують загальні IT-заходи контролю.

- Ціль: Оцінити дизайн і операційну ефективність заходів контролю.

❑ Ефективність дизайну:
  - ✓ Документування загальних IT-заходів контролю.
  - ✓ Проходження через загальні IT-заходи контролю або запит і спостереження.
  - ✓ Оцінка будь-яких недоліків дизайну.

❑ Операційна ефективність:
  - ✓ Тестування заходів контролю.
  - ✓ Оцінка будь-яких операційних недоліків.



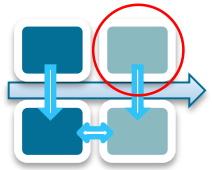
Ключові загальні IT-заходи контролю

1. Управління доступом (ACC)

2. Управління змінами (CHA)

Управління доступом (ACC)

- Механізми контролю безпеки;
- Потужна система або Ідентифікація даних користувачів;
- Процедури контролю безпеки;

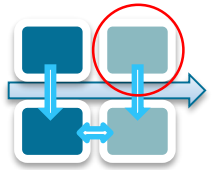


Управління доступом —Механізми контролю безпеки

<u>Ціль</u>: Визначити, що логічний і фізичний доступ до IT комп'ютерних ресурсів належним чином обмежений.

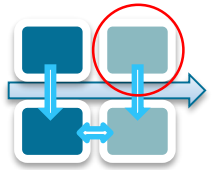
<u>Ключові елементи контролю та ідеї для тестування</u>:

- Доступ до комп'ютерних засобів фізично забезпечено і обмежено авторизованими особами.
- Унікальні дані ідентифікації користувачів використовуються для забезпечення індивідуальної відповідальності
- Надійні і складні вимоги до паролів
- Ефективні механізми входу та заходи з управлінського огляду запроваджено



Управління доступом – Типові тести заходів контролю за логічним доступом

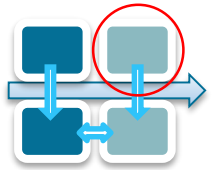
- Визначити множину нових або існуючих користувачів та зробити вибірку;
- Перевірити чи доступ авторизований/відповідний ролі;
- Визначити множину користувачів, що залишили установу в ході періоду аудиту та зробити вибірку;
- Оцінити, чи був втрачений, обмежений або скасований доступ *(хто приєднався, перевівся і пішов)*



Управління змінами – Авторизовані зміни і відповідні процедури

- **Ціль:** Визначити, що контрольні заходи запроваджено, щоб гарантувати належну авторизацію змін у системах/прикладних програмах відповідним рівнем керівництва.

- **Ключові елементи контролю та ідеї для тестування:**
  - Організація запровадила формальний процес управління змінами.
  - Усі запити на зміни у системах/прикладних програмах формально документуються
  - Аудиторський слід змін можна відстежити і співвіднести до первинних запитів.



Управління змінами – Тестування змін програми

- **<u>Ціль</u>:** визначити, що контрольні заходи запроваджено, щоб гарантувати тестування, підтвердження і схвалення змін до прикладних програм і систем до запуску у виробництво.

- **<u>Ключові елементи контролю та ідеї для тестування</u>:**
- Запроваджено окреме від виробництва середовище тестування
- Тільки обмежена кількість осіб повинна вносити зміни у виробництво.

Rijksacademie voor Financiën,
Economie en Bedrijfsvoering
Ministerie van Financiën

Чи є запитання?

Дякуємо за увагу!