Central Government Audit Service
Ministry of Finance

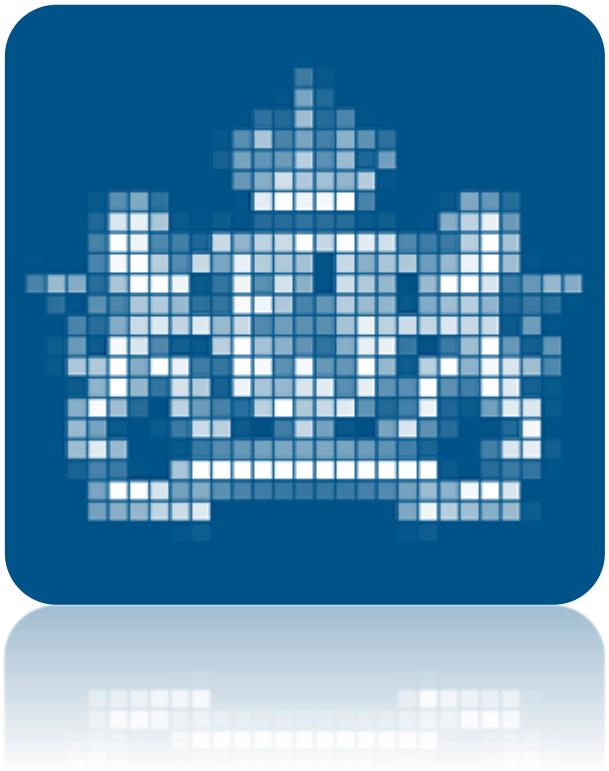
Тренінг з аудиту інформаційних технологій

День 1

Рурдьє Просе
Лодевік Янсен

Листопад 2019

Central Government Audit Service
Ministry of Finance



Порядок денний

- Вступ і навчальні цілі
- Вступ до IT та IT-аудиту/Початок IT-аудиту
- Види заходів контролю та рамкових основ аудиту
- Роздуми про перший день

Вступ

Лектори

Рурдьє Просе

- Старший IT-аудитор
- МН із Штучного інтелекту
- Магістр з IT-аудиту
- Сертифікований професіонал з безпеки інформаційних систем

Лодевік Янсен

- Керівник з IT-аудиту
- МН з Управління інформацією
- Магістр з IT-аудиту

Аудит в Нідерландському Уряді

Нідерландський Уряд

Національний уряд

Піднаціональний уряд

Нідерландський Уряд (Rijksoverheid)

- 11 міністерств
  - Міністерство закордонних справ (BZ)
  - Міністерство фінансів (FIN)
  - Міністерство безпеки та юстиції (J&V)
  - Та ін.

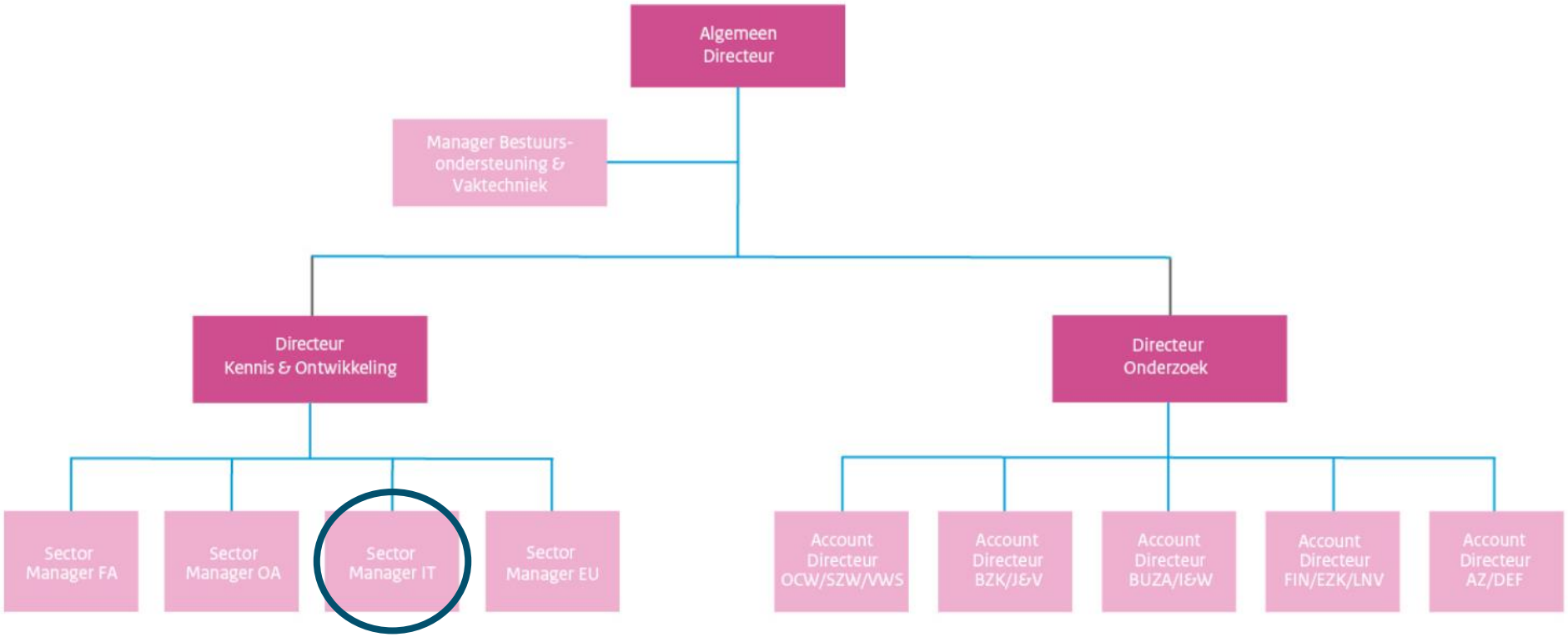
- 160 агентств та виконавчих організацій
- Податкова та митна адміністрація
  - Національний архів
  - Національний криміналістичний інститут
  - Центральне агентство судових зборів
  - Інспекція з охорони здоров'я
  - І так далі.

- 120 000 працівників
- 27 000 в Гаазі
  - 30 000 в Податковій та митній адміністрації

Про Центральну Урядову Службу Аудиту

- Утворена 1 травня 2012
- Об'єднання/злиття сильних сторін департаментів аудиту міністерств.
- Нагляд, координація та моніторинг з боку Міністерства фінансів, незалежне розміщення та робота для всіх міністерств.
- Близько 600 працівників (100 IT- аудиторів)

Про Центральну Урядову Службу Аудиту (II)



Планування аудиту в ЦУСА

Одне всеосяжне планування аудиту для усієї Служби аудиту

На основі:

- ❑ Аналізу ризиків
- ❑ Тенденцій та розвитку

І схвалюється:

- ❑ Аудиторським комітетом
- ❑ Комітетом генеральних секретарів міністерств

Усі завдання на один рік є одним із варіантів:

1. Передбачені законом
2. Змінні завдання
3. Завдання за дорученням ЄК

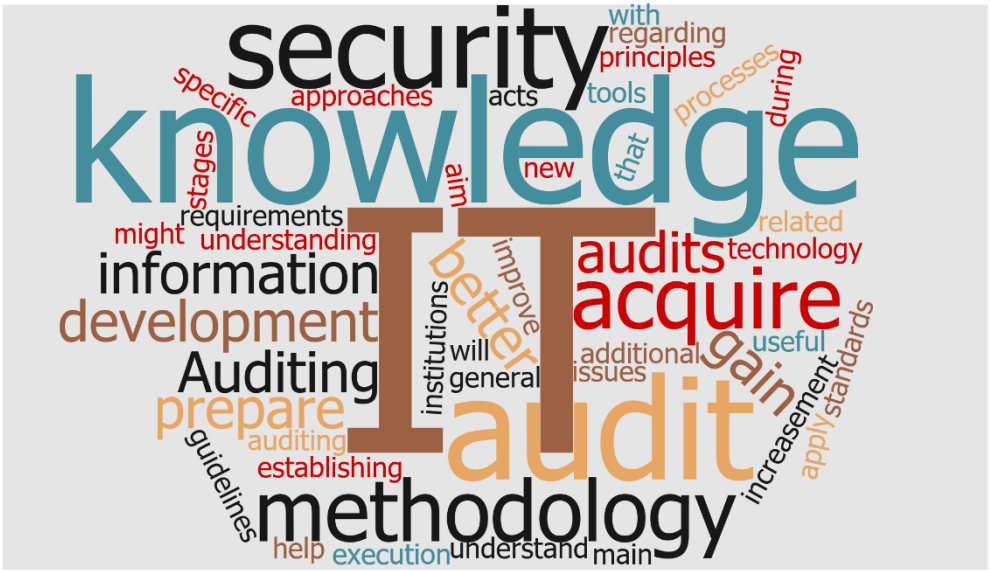
Переходимо до теми IT та IT-аудиту

- Що Вам вже відомо про IT?
- Що Вам вже відомо про аудит?
- Який досвід у Вас є у сфері IT-аудиту?

Навчальні цілі

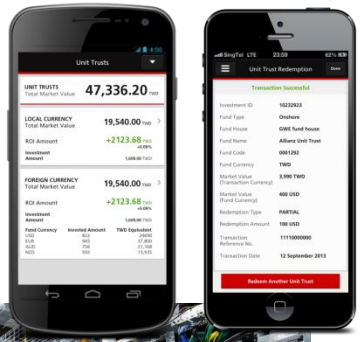
Навчальні цілі

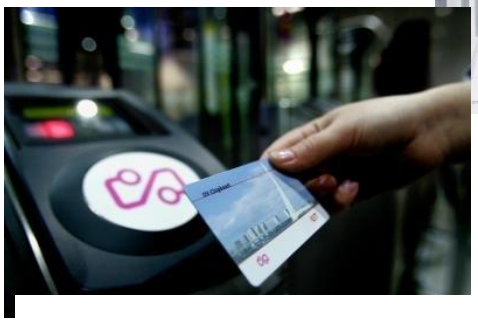
- Чого хочете навчитися?
- Що хочете спробувати на практиці?
- Що очікуєте від нас?

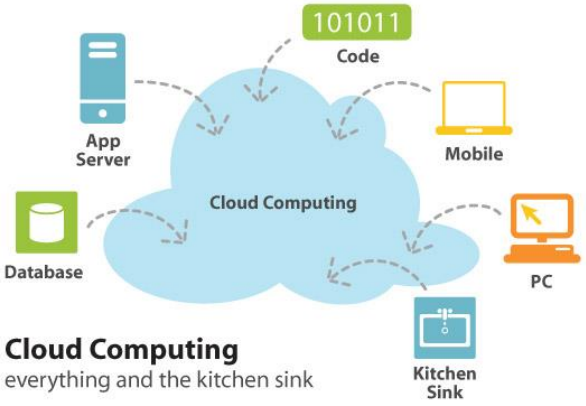


Представлення IT

Світ IT

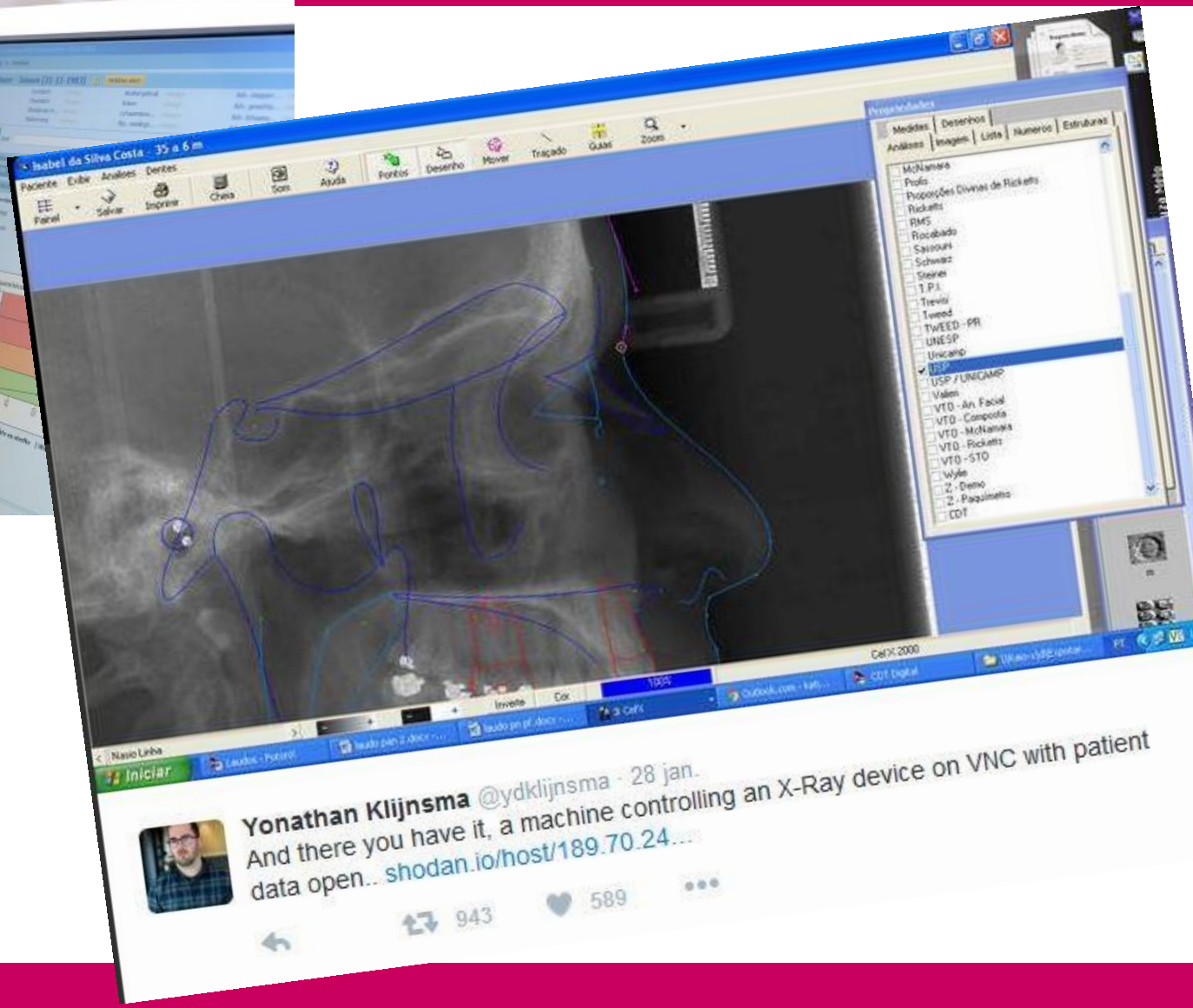


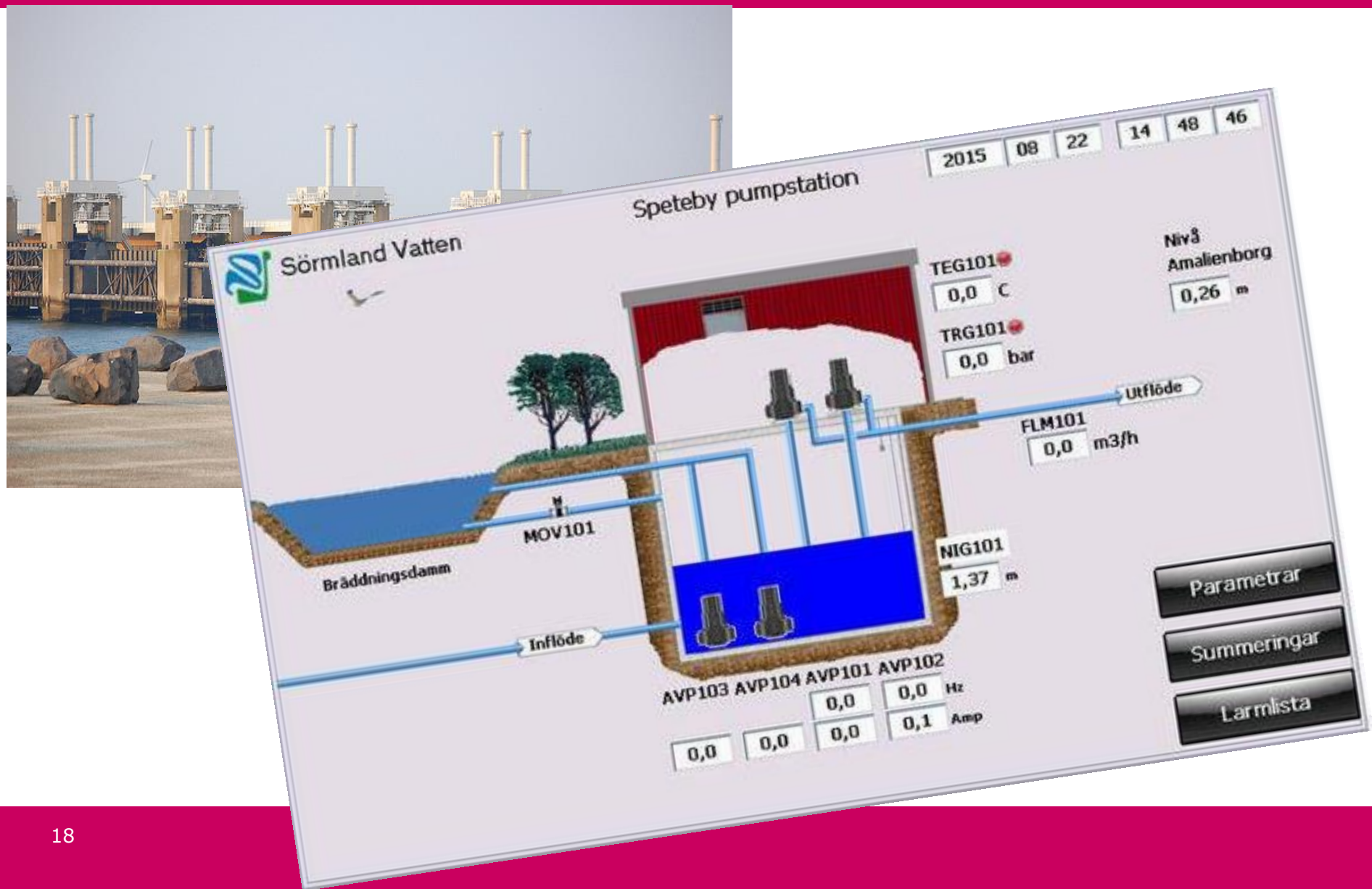




Можете назвати деякі нові напрямки у IT?


Vulnerability
Patch
Privacy
Threat
SIEM
Advanced
Secure
Risk
malware
Log
Risk-Management
CISO
Solution
Compliance
Configuration
Prevent
Identity
analytics.
Mobile
Detect
detection
cso
big
Value
Next-Gen
breach
Human
Cloud
Data
security
Scan
Unified
Business
code
CVSS
SCAP
Intelligence
Next-Generation
Standards
BYOD
Service
data
Authorization
Encryption
Enterprise


Yonathan Klijnsma @ydklijnsma · 28 jan.
And there you have it, a machine controlling an X-Ray device on VNC with patient data open.. shodan.io/host/189.70.24...
943
589


Speteby pumpstation
2015 08 22 14 48 46
Sörmland Vatten
TEG101
0,0 C
TRG101
0,0 bar
Nivå Amalienborg
0,26 m
Utflöde
FLM101
0,0 m3/h
MOV101
Bräddningsdamm
NIG101
1,37 m
Inflöde
AVP103 AVP104 AVP101 AVP102
0,0 0,0 Hz
0,0 0,0 0,0 0,1 Amp
Parametrar
Summeringar
Larmlista

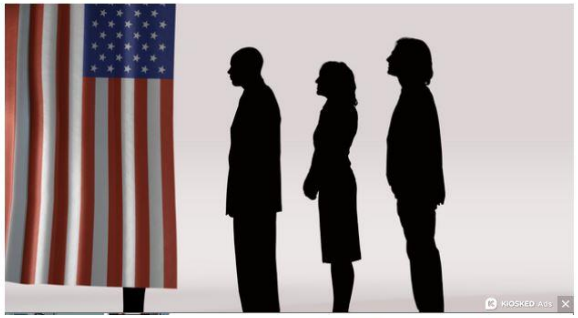
Bloomberg Businessweek

Markets Tech Pursuits Politics Opinion Businessweek

How Hackers Took Down a Power Grid

Ukraine was an easy target—but the U.S. has its own weaknesses.

Voting machines are still too easy to hack



MORE LIKE THIS

Open source: How e

Dutch spies tipped off NSA that Russia was hacking the Democrats, new reports claim

Netherlands intelligence penetrated Russia's US election hackers and alerted US counterparts, sources say.

dnn

The Stuxnet Attack On Iran's Nuclear Plant Was 'Far More Dangerous' Than Previously Thought

Michael B

Nov. 20,

Hacked patient records may be for sale online

IT в Нідерландському Уряді

Завдання – Ваша власна організація

Що б Ви хотіли перевірити аудитом і чому?

Які проблемні питання у Вас наразі виникають?

- Первинні урядові процеси
- Цифрова комунікація з громадянами і компаніями
- Внутрішні бізнес-процеси

IT в Нідерландському Уряді (I)

Первинні урядові процеси

Комунікація з громадянами і компаніями

Внутрішні бізнес-процеси

IT в Нідерландському Уряді(II)

Первинні урядові процеси	**Комунікація з громадянами і компаніями**	Внутрішні бізнес-процеси

DigiD

eHerkenning
Eenvoudig zaken doen met de overheid

Inloggen op Mijn DUO

Alles online geregeld

Financiering aanvragen, een wijziging doorgeven of uw gegevens bekijken? U regelt het zelf in Mijn DUO.

Inloggen Mijn DUO	DigiD
U kunt elke dag inloggen, alleen niet tussen 06.00 en 07.00 uur 's ochtends.	Wachtwoord of gebruikersnaam vergeten? DigiD helpt u verder.

Centraal Justitieel Incasso Bureau

Postadres > Postbus 1794, 8901 CB Leeuwarden

M

Verzenddatum : 23 apr 2009
Vervaldatum : 18 jun 2009

Informatie: www.cjib.nl
Telefoon: 058 - 2342 130

Mijn Kadaster

Agentschap Telecom
Ministerie van Economische Zaken

IT в Нідерландському Уряді(III)

Первинні урядові процеси | **Комунікація з громадянами і компаніями** | **Внутрішні бізнес-процеси**

Деякі приклади IT аудитів, що проводила Центральна урядова служба аудиту

- Тестування системи онлайн аукціону, що був застосований урядом для аукціонера Telecom щодо частот провайдерів Телекому
- Поради в частині автоматизації документальних процесів Міністерств
- Тестування безпеки смартфонів, які використовують держслужбовці
- Тестування безпеки автоматизованих систем подачі заяв громадянами, у яких зберігаються дані про повернені податки
- Тестування безпеки зв'язку через VPN
- Аудит мобільного додатку щодо попереджень
- Аудит безпеки хмаринкових та віртуальних технологій.
- Аудит інформаційних центрів
- Тестування програмних модулів у великих фінансових системах.

Об'єкти IT-аудиту

- Технічна інфраструктура (технічний аудит)
- Операційна інформаційна система (системний аудит)
- IT-процеси (напр. ITIL-аудити)
- Програмне забезпечення
  - Комерційне «з полиці» (COTS)
  - Стандартне програмне забещзечення з конфігурацією замовника
  - Спеціалізоване
- Системи безпеки
- Захист персональних даних.
- Сертифікація або акредитація.
- Шахрайство і судові аудити / розслідування.

Від IT до IT-аудиту

Від IT до IT - аудиту

Рамкова основа аудиту визначає критерії аудиту, яким має відповідати IT-система.

«Оцінка якості» IT систем та процесів, виходячи із меж проведення аудиту.

«IT аудит – це незалежна та об'єктивна оцінка надійності, безпеки (включаючи конфіденційність), ефективності та результативності автоматизованих інформаційних систем, організації автоматизованих департаментів, а також технічної та організаційної інфраструктури автоматизованих інформаційних процесів»

«Забезпечення додаткових гарантій шляхом оцінки (управління і контролю) одного або більше якісних аспектів об'єктів інформаційного забезпечення

*See slide 18

Від IT до IT-аудиту

IT-аудитор:

- Висловлює оціночне судження щодо IT в компанія / організаціях
- Кваліфікований для надання гарантій
- Експерт у сфері інформаційної безпеки, IT-контролю та узгодження бізнес-IT

Аспекти якості

- Конфіденційність: авторизація, ідентифікація, тощо.
- Правдивість: повнота і точність даних, автентичність.
- Доступність: безперервність, портативність, відновлення
- Не-відмова

- *Контрольованість: підтримка, зв’язок, безпека*
- *Результативність: рівень охоплення, зручність використання*
- *Ефективність: швидкість, зручність для користувача, повторне використання*

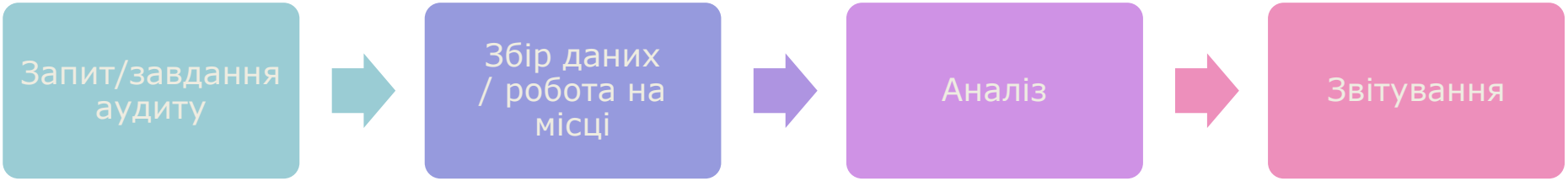
Завдання

- **Які аспекти якості ви використовуєте?**

- Конфіденційність: авторизація, ідентифікація, тощо.
- Правдивість: повнота і точність даних, автентичність.
- Доступність: безперервність, портативність, відновлення
- Не-відмова

- *Контрольованість: підтримка, зв’язок, безпека*
- *Результативність: рівень охоплення, зручність використання*
- *Ефективність: швидкість, зручність для користувача, повторне використання*

Етапи IT-аудиту



Від IT до IT-аудиту:

Запит/завдання на аудит

(початок IT-аудиту)

Запит/завдання на аудит (I)

У замовника можуть бути різні причини для запиту на IT-аудит, наприклад:

- Відповідність (‘Я маю дотримуватися ISO27001’)
- Нещодавнє порушення безпеки
- Отримати інформацію щодо поточного рівня безпеки
- Укладення угоди із новим IT партнером
- Планується встановлення нової IT системи

Запит/завдання на аудит (III)

Дизайн дослідження:

- Запитання замовника
- Мета аудиту
  - Який IT-ризик?
- Які аспекти якості, рамкова основа аудиту та критерії аудиту будуть використовуватися?
- Питання аудиту (дослідження)
- Вид аудиту
  - Звіт з надання гарантій
  - Звіт про фактичні знахідки

Запит/завдання на аудит (IV)

Питання, які необхідно включити в аудиторське завдання :

- **Межі (обсяг) об'єкту аудиту**
- Члени команди
- Планування
- Потенційні ризики в аудиторському завданні
- Підпис керівника аудиту
- Підпис замовника
- Договір про нерозголошення інформації

Не забудьте:

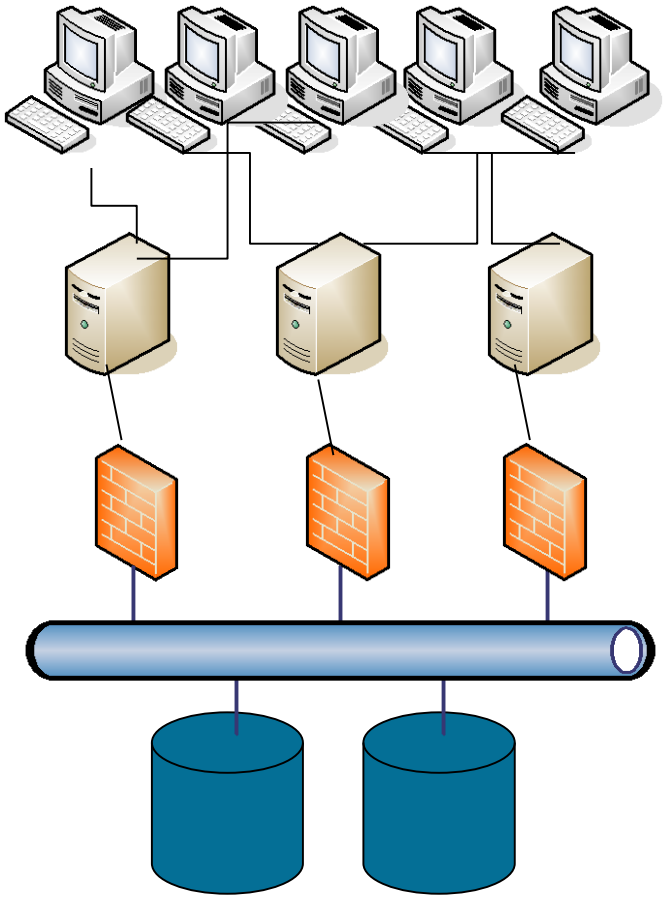
✓Зробити практичні заходи для проведення аудиту

✓Домовитися щодо збору та використання «вразливих» аудиторських доказів і даних

Запит/завдання на аудит(VI)

Обсяг (межі) в деталях:

- Які компоненти охоплюються, а які ні, і чому?
- Чи замовник володіє актуальною картинкою ситуації?
- Документи дизайну
- Узгодити обсяг із замовником/фінансовим аудитором

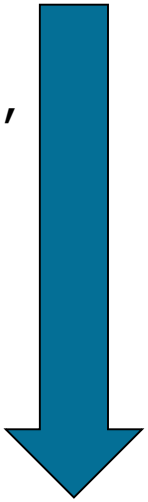


Від IT до IT-аудиту:

Як визначити обсяг

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)



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 підприємством та IT-архітектурою
- 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.

Управління інцидентами

Управління безпекою

Управління змінами

Управління випуском

- Працівника перевели із відділу закупівель у відділ продаж

Управління доступом

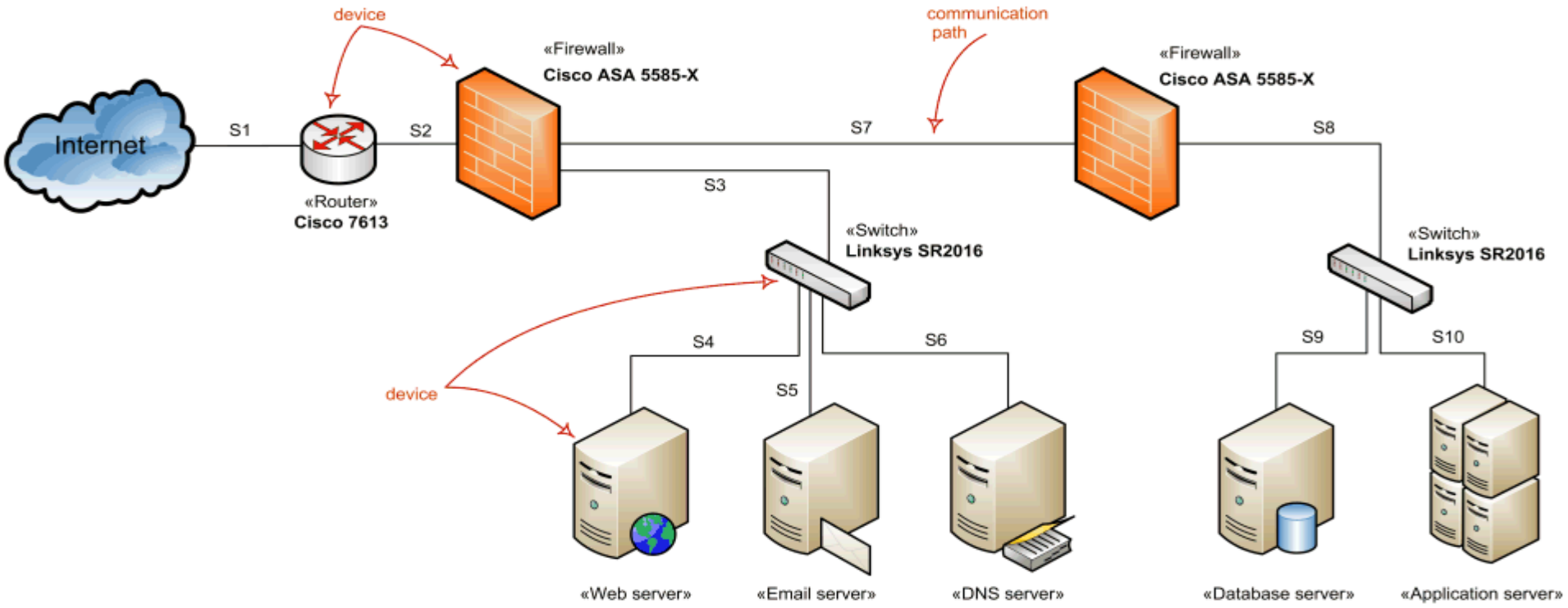
Вимога виконання

Об'єкти аудиту – застосунки

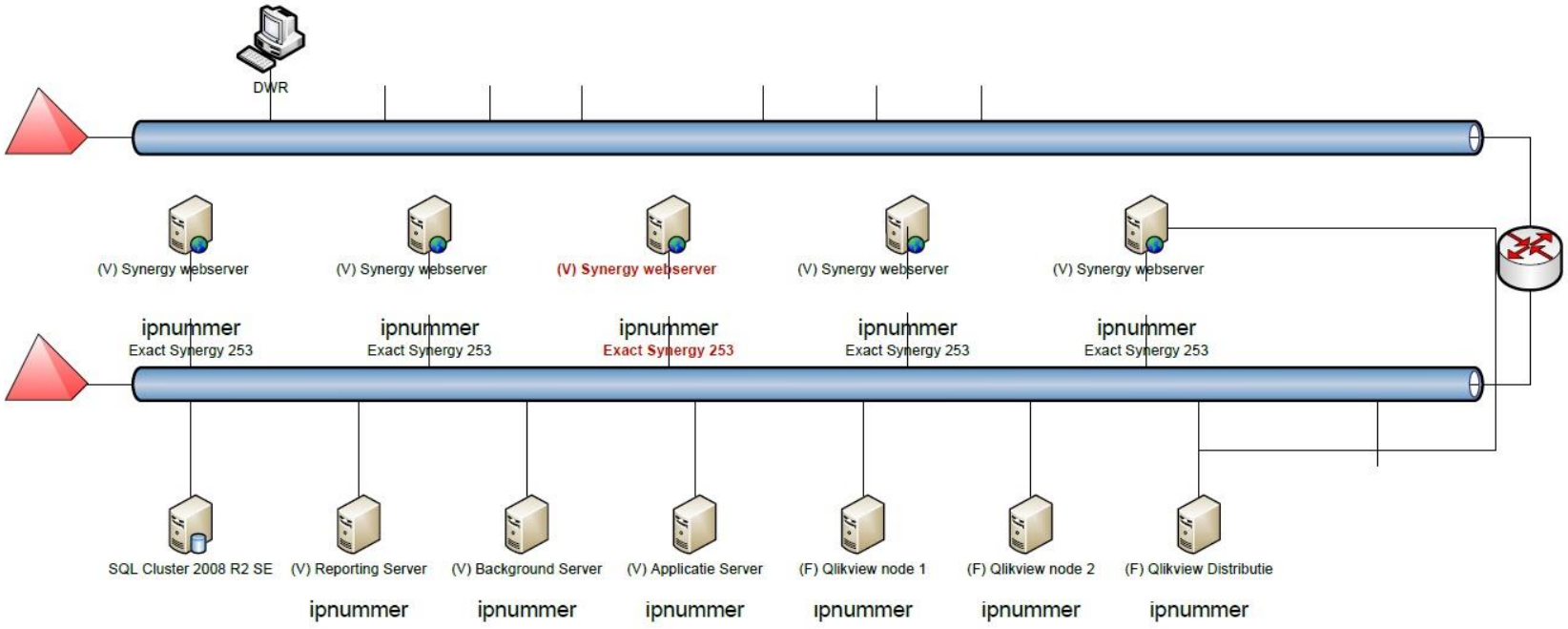
- Операційні системи: Windows / Linux / CentOS /
- Системи управління базами даних
- Системи управління документами
- Фінансові застосунки: SAP / Oracle
- Застосунки щодо закупівель
- Застосунки щодо заробітної плати

Об'єкти аудиту - інфраструктура

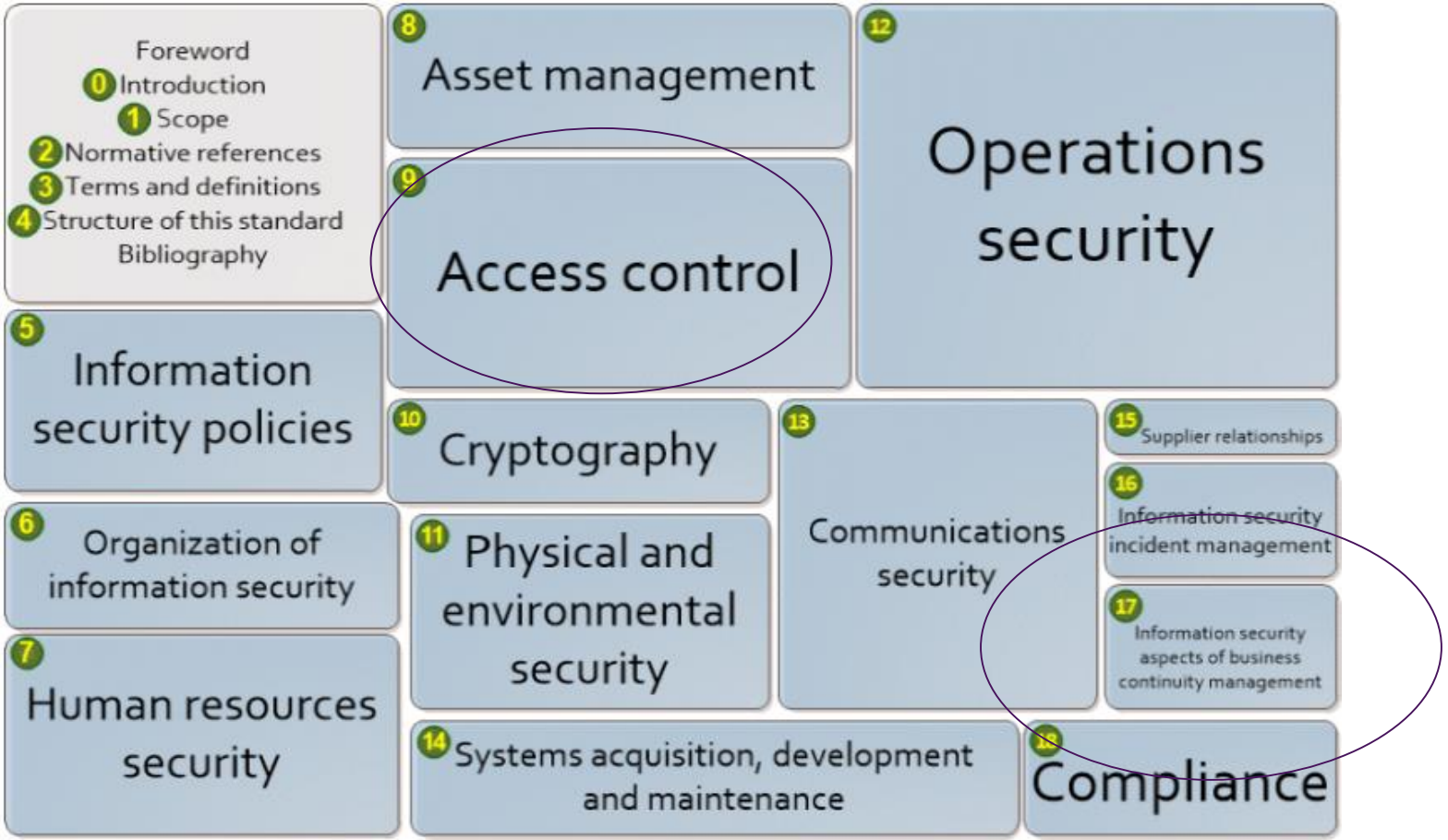
Аудит на рівні периметру: такі технічні компоненти як: міжмережевий екран, вирівнювач навантаження, веб-сервер, сервер застосунку, сервер бази даних.



Приклад визначення обсягу (I)



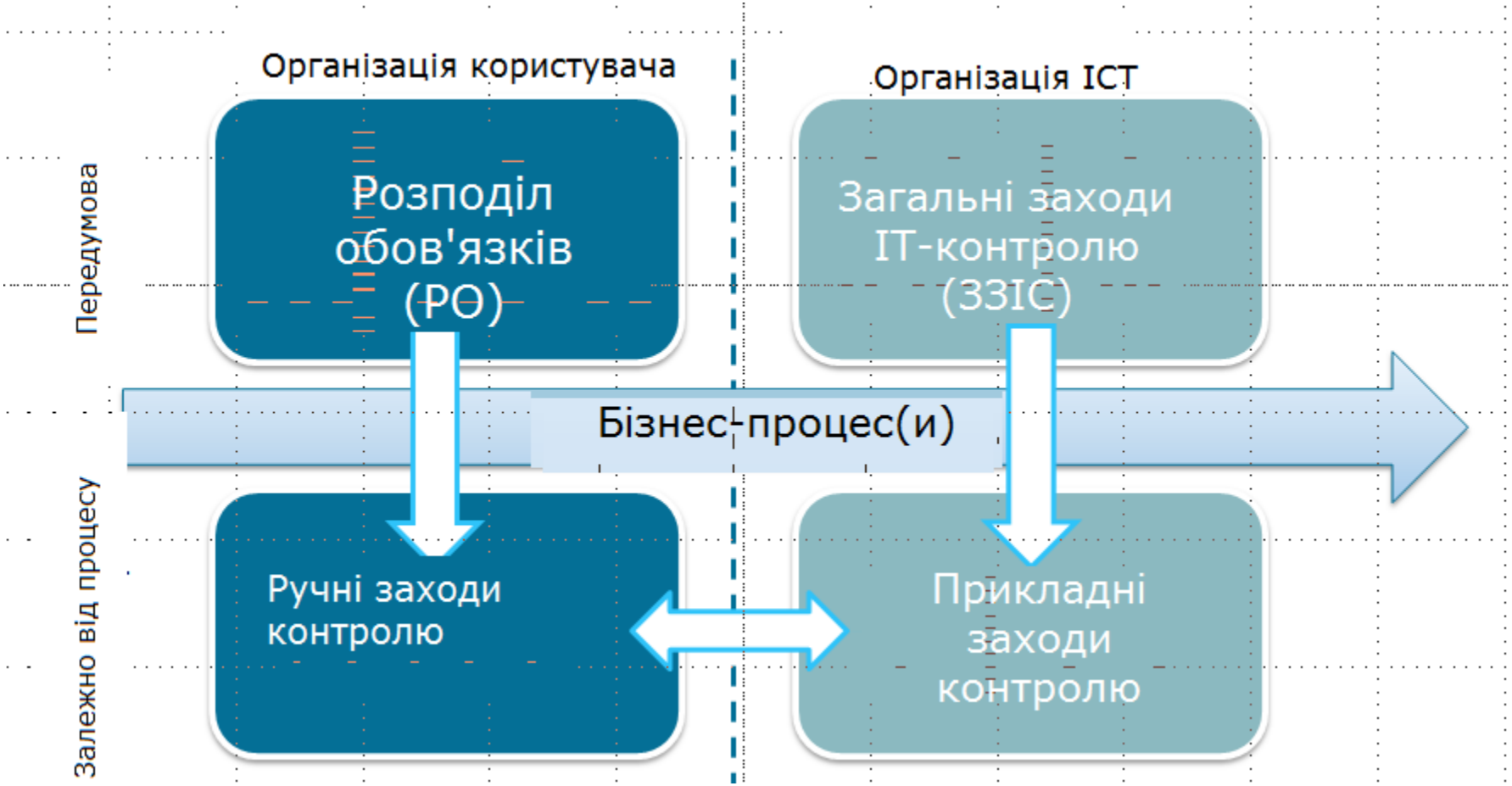
Приклад визначення обсягу(II)



Від IT до IT-аудиту:

Види заходів контролю

Види заходів контролю: модель контролю

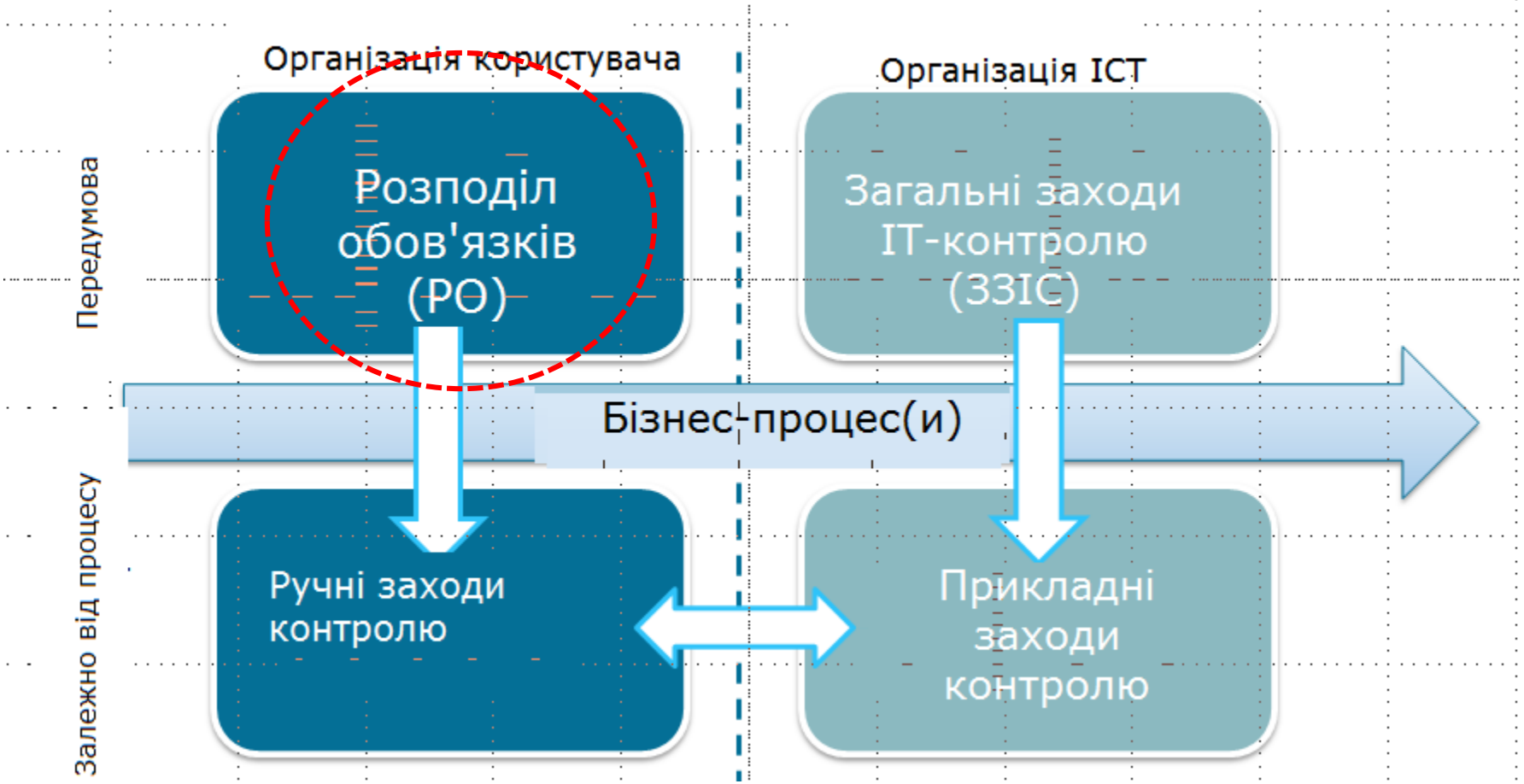


Огляд IT заходів контролю

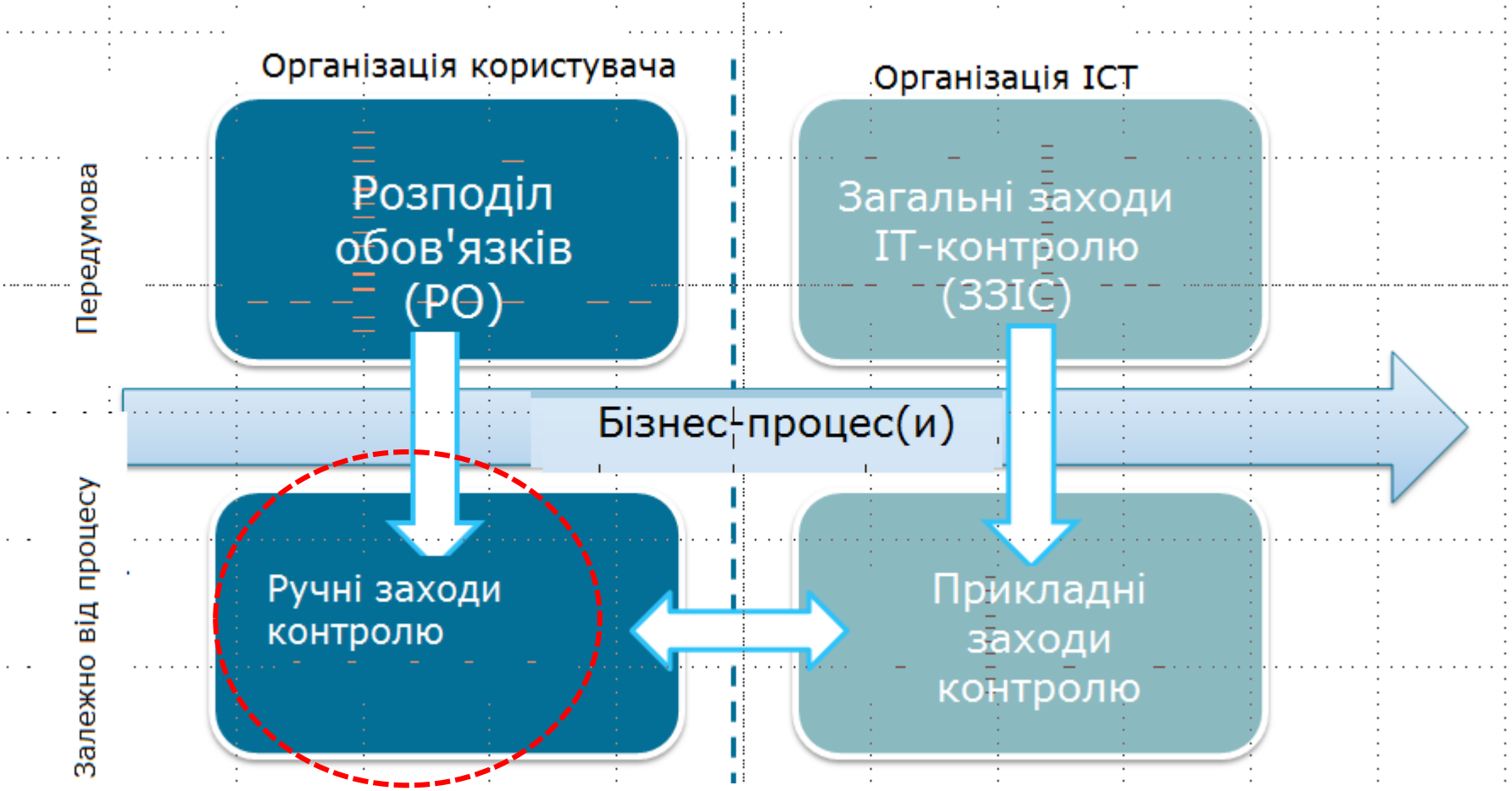
Коли йдеться про IT заходи контролю, фактично можна говорити про дві категорії. ***Контрольні заходи щодо прикладних програм (AC),*** які включені у “стандартні” бізнес процеси (напр. закупівлі, доходи тощо) і розроблені з метою автоматизації функції контролю, тоді як ***загальні заходи контролю (ITGC)***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

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

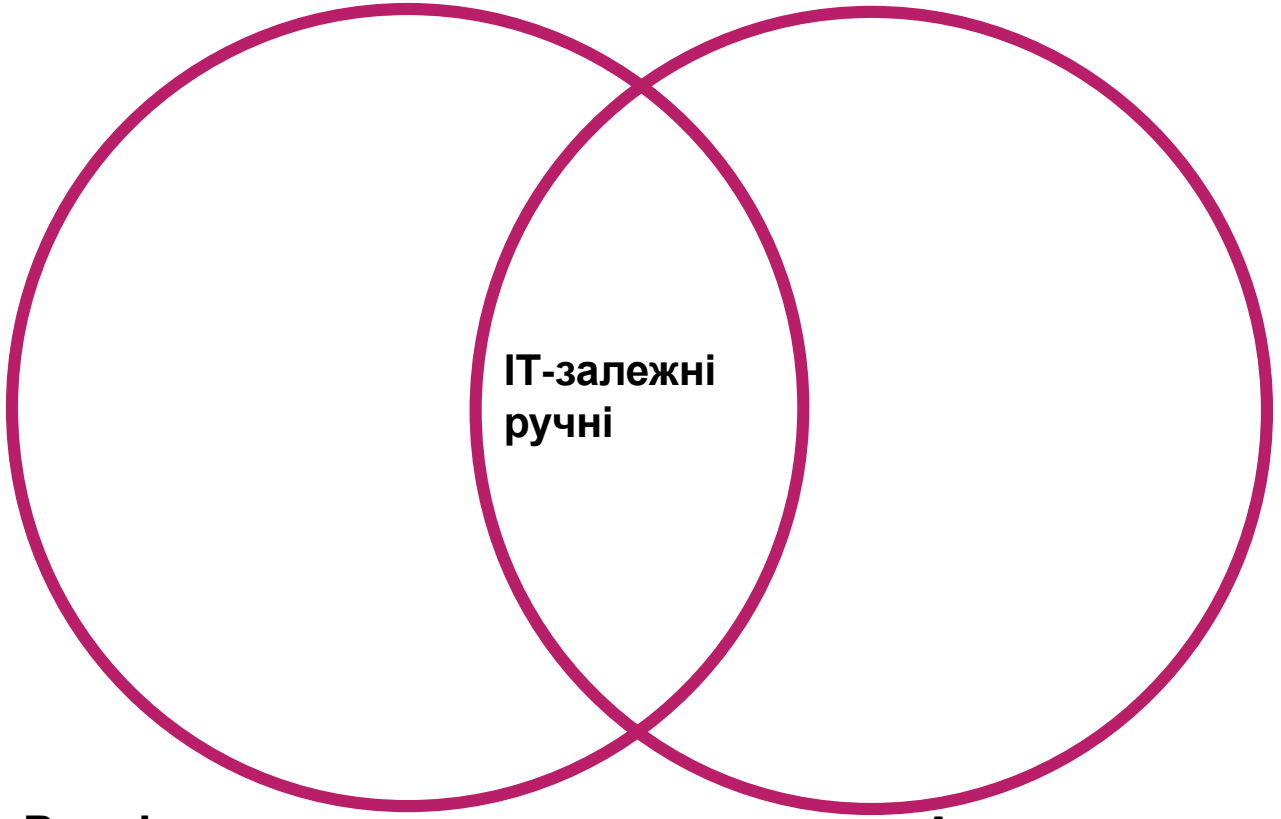
Розподіл обов'язків (РО)



Ручні заходи контролю



Автоматизовані проти ручних заходів контролю



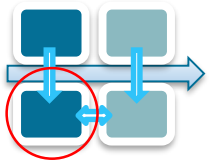
IT-залежні, ручні заходи контролю (прод.)

Види IT – залежних заходів контролю

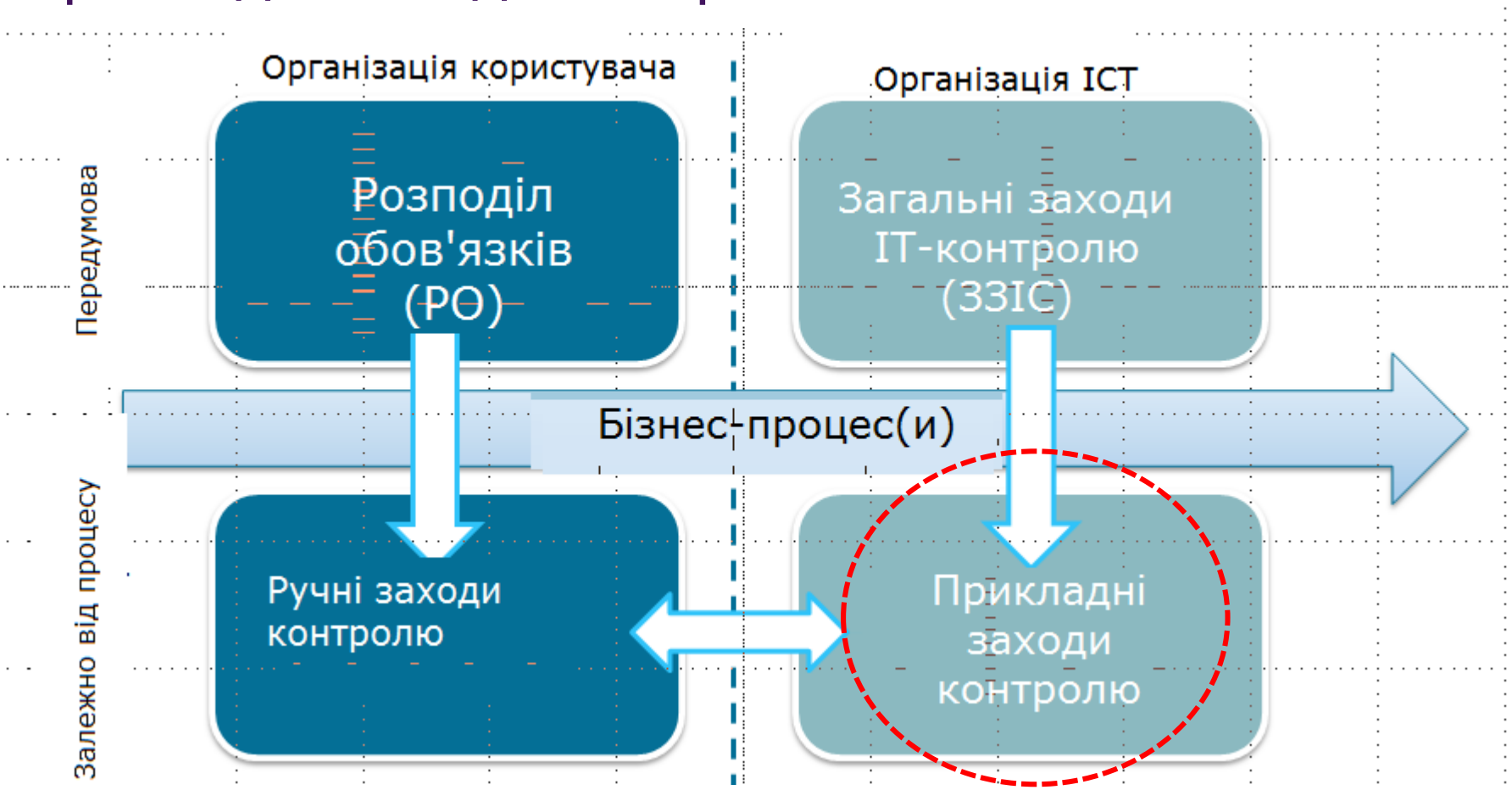
- Узагальнені системні стандартні звіти
- Звіти за запитом/спеціальні звіти

Тестування припущень

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



Прикладні заходи контролю



Прикладні заходи контролю - Завдання

У групах:

Види прикладних заходів контролю

Прикладні заходи контролю - Завдання

Прикладні заходи контролю – це заходи контролю за функціями вводу, обробки і видачі даних.

- Ввідні дані повні, точні та дійсні

  Авторизація вводу, Контроль за пакетом та балансування
- Забезпечення, щоб внутрішня обробка видавала очікувані результати

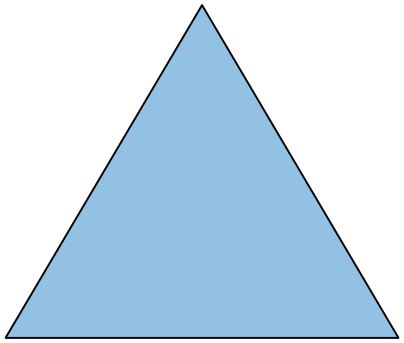
  Підтвердження даних та процедура редагування (напр, межі і діапазон перевірок)
- Забезпечення, щоб обробка досягала бажаних завдань

  Робочий процес, послідовність обробки

Прикладні заходи контролю:

Приклад: SAP 3-кутне зведення

Замовлення на покупку



Отримання товару

Рахунок

Загальні IT-заходи контролю

1. Управління змінами
2. Управління паролями
3. Управління доступом
4. Механізми безпеки
5. Резервне копіювання і відновлення

Від IT до IT-аудиту:

Фінансовий та IT-аудит

Фінансовий та IT-аудит

- Визначення обсягу для фінансового аудиту
- Що перевіряти -> Стратегія аудиту
- Інтегрований контроль


Питання фінансової звітності
Фінансовий річний звіт
Річний звіт
Нефінансова інформація
Процеси
Процес 1
Процес 2
Процес n
Прикладні / Ручні заходи контролю
Застосунки
Застосунок A
Застосунок B
Застосунок Z
Прикладні заходи контролю
Загальні заходи IT-контролю
IT інфраструктура
База даних
Операційна система
Мережа та фізична інфраструктура

Стратегія для матеріального фінансового потоку	Не покладається на заходи контролю (предметний підхід)	Покладається на заходи контролю (системний підхід)	
На які заходи контролю покладається ФА?	Ні на які	FA покладається на ручні заходи контролю	FA покладається на автоматизовані або програмні заходи контролю
Покладається на IT-процеси?	Ні		Так
Стратегія аудиту для IT-застосунків	Тільки предметні аудиторські процедури (ФА) Жодних процедур IT-аудиту.	Тільки перевіряє ручні заходи контролю (ФА) Жодних процедур IT-аудиту.	1. Повністю покладається на ITGC's* 2. Альтернативні IT-заходи контролю, наприклад, аналіз журналу, аналіз даних
Оцінка знахідок	Не застосовується до IT-аудитора	Не застосовується до IT-аудитора	Достатні Загальні заходи IT-контролю: надає гарантії про операційну ефективність автоматизованих/програмних заходів контролю Недостатні Загальні заходи IT-контролю : потрібні альтернативні процедури, щоб визначити, чи мав місце ризик

* ITGC рамкова основа

Приклад: Міністерство здоров'я, добробуту і спорту

Аудиторська група (ФА):

- Відповідальний бухгалтер
- Провідний IT-аудитор
- Бухгалтери
- IT-аудитори
- Помічник/ молодший бухгалтер

Від IT до IT-аудиту:

Рамкові основи аудиту

Рамкові основи аудиту (критерії)

Обговоріть у Вашій групі:

Які рамкові основи аудиту Ви використовуєте? І чому?

Рамкові основи аудиту (критерії) - джерела

Закони і постанови

Політики/Стратегії

Професійні асоціації

Міжнародні організації

Центри знань

Внутрішні вказівки та

Критерії, характерні для організації

Рамкові основи аудиту (критерії) в IT-аудиті

	Приклади рамкових основ для IT 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

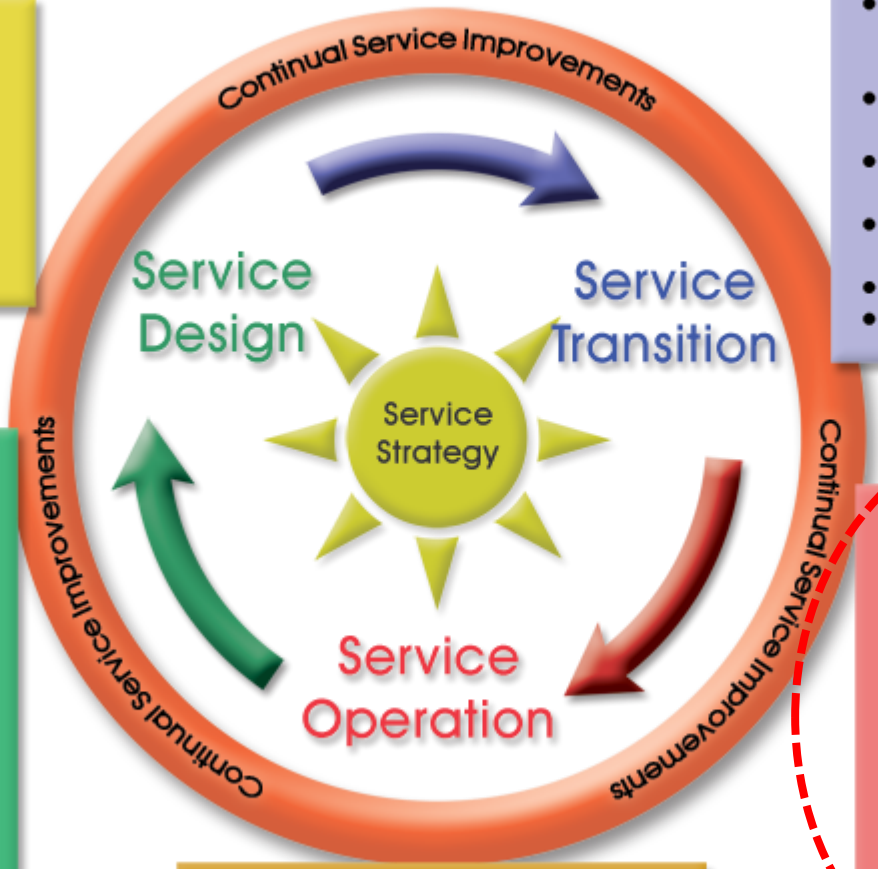
Залежно від об'єкту (цілі) аудиту пристосовуються стандарти/норми!

Рамки аудиту (критерії) в IT-аудиті

- CobIT (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)
- Постанови із захисту персональних даних (GDPR)
- Загальні IT заходи контролю

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

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

Prince 2: Рамкова основа для (IT) проектів

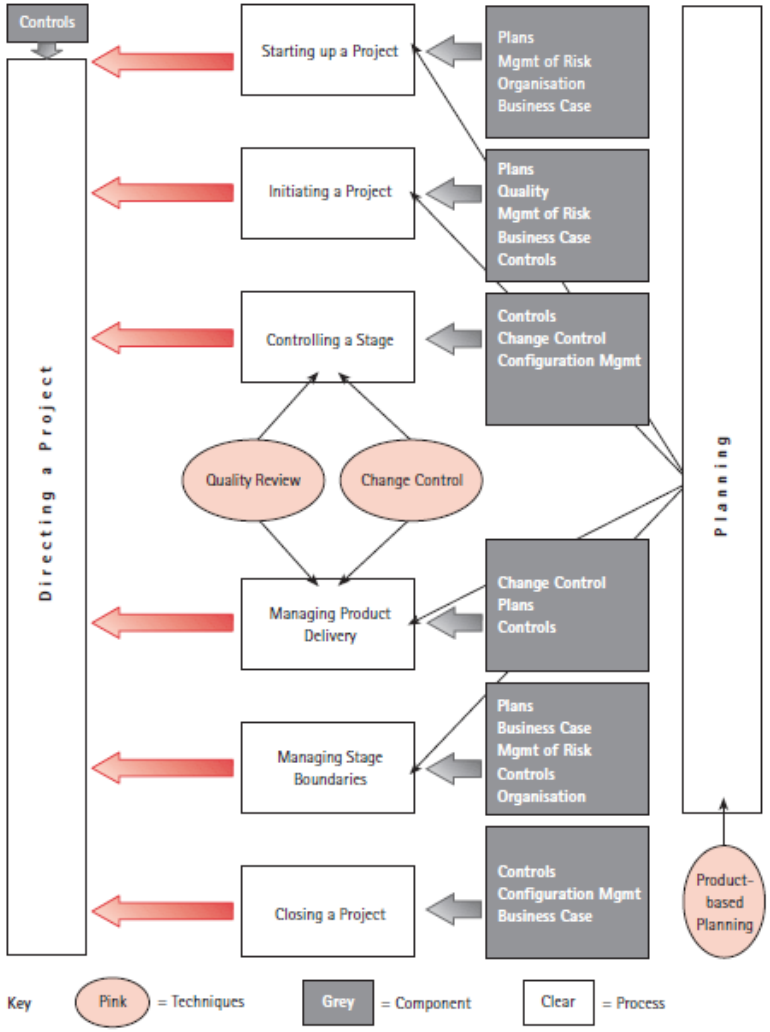


Figure 2.6 Use of PRINCE2 components and techniques in the processes

Adobe Acrobat Document

ISO27002: рамкова основа для Інформаційної безпеки

INTERNATIONAL STANDARD

ISO/IEC 27002

First edition
2005-06-15

Adobe Acrobat Document

Information technology — Security techniques — Code of practice for information security management

Technologies de l'information — Techniques de sécurité — Code de bonne pratique pour la gestion de la sécurité de l'information

Центр Інформаційної безпеки

https://www.cisecurity.org/cis-benchmarks/

CIS Center for Internet Security®

CIS Benchmarks

Download Our Free Benchmark PDFs

The CIS Benchmarks are distributed free of charge in PDF format to propagate their worldwide use and adoption as user-originated, de facto standards. CIS Benchmarks are the only consensus-based, best-practice security configuration guides both developed and accepted by government, business, industry, and academia.

View Our Extensive Benchmark List:

- + Desktops & Web Browsers
- + Mobile Devices
- + Network Devices
- + Security Metrics
- − Servers – Operating Systems
  - Amazon Linux
  - CentOS
  - Debian Linux Server
  - IBM AIX Server
  - Microsoft Windows Server
  - Novell Netware
  - Oracle Linux
  - Oracle Solaris Server
  - Red Hat Linux Server
  - Slackware Linux Server
  - SUSE Linux Enterprise Server
  - Ubuntu LTS Server
- + Servers – Other
- + Virtualization Platforms & Cloud
- + Other

Рамкові основи для загальних заходів IT-контролю GCAS

- На основі найкращих практик/ ISO27001/2

Change management
Category
W1. Change management
W1. Change management
W1.1 : Changes must be authorised
W1.2 : Changes must be tested
W1.3 : Changes must be approved subject to test results
W1.4 : Duties to apply for, approve and implement changes must be segregated
W1.5 : Periodic checks must be made for unauthorised changes
Logical access controls
Category
L.1 Password management
L1.1 : Passwords must be periodically changed
L1.2 : Passwords must be strong
L1.3 : Two-factor authentication must be used in untrusted zones
L1.4 : Applications must be locked when inactive
L1.5 : Passwords must be encrypted when saved
L1.6 : User accounts must be blocked after a pre-set number of five incorrect login attempts
L2. User controls
L.21 : Users and administrators must have only access those rights that are necessary for their work
L2.2 : User accounts and access rights must be authorised
L2.3 : Duties to apply for, approve and implement changes in user accounts and access rights must be segregated
L2.4 : Staff departures must be processed promptly
L2.5 : Admin accounts must be limited and the reasons for them explained in so far as necessary
L2.6 : User accounts and admin accounts must be strictly personal
L2.7 : User accounts must not have direct access to underlying components
L2.8 : User and admin accounts and access rights must be periodically evaluated and the findings must be followed up
L3. Component security
L3.1 : Insight into applications and underlying components must be up to date
L3.2 : Alerts must be automatically generated for new weaknesses and systems must be periodically checked for technical weaknesses
L3.3 : Systems must be patched and updated promptly
L3.4 : Systems must not use standard passwords or backdoor accounts
L3.5 : The operating system must not run unnecessary services
L3.6 : The internal network must be isolated from untrusted environments
L3.7 : Network traffic and components must be actively monitored
Overall outcome of Logical access controls
O1. Optional
Category
O1. Optional
O1.1 : The periodicity of backups and the type of data backed up must be consistent with the systems critical for the annual accounts
O1.2 : Backup data must be kept at a secure location where the integrity of the backup is assured
O1.3 : Ability to recover the backup must be periodically tested

Підбиття підсумків та замірювання настрою

Який був Ваш день?

Central Government Audit Service
Ministry of Finance

Чи є запитання?

Дякуємо за увагу!