Central Government Audit Service
Ministry of Finance

Тренінг з аудиту інформаційних технологій

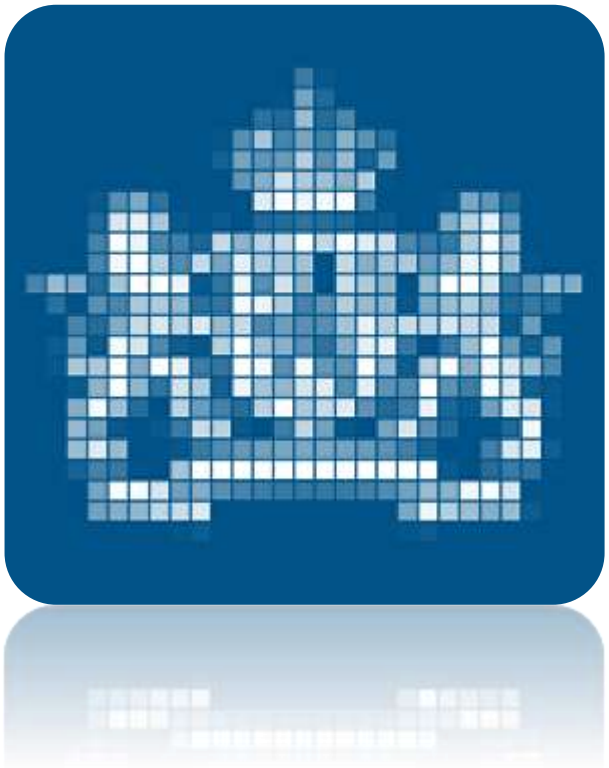
День 2

Рурдьє Просе
Лодевік Янсен

Лютий 2021

Auditdienst Rijk
Ministerie van Financiën

Central Government Audit Service
Ministry of Finance



Порядок денний

- Вікторина та запитання про заходи IT-контролю (завдання 1)
- Представлення аудиторських основ та збору даних
- Представлення ключових заходів загального IT-контролю

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	ФА покладається на ручні заходи контролю	ФА 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

Від IT до IT-аудиту:

Рамкові основи аудиту

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

	Audit framework examples
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

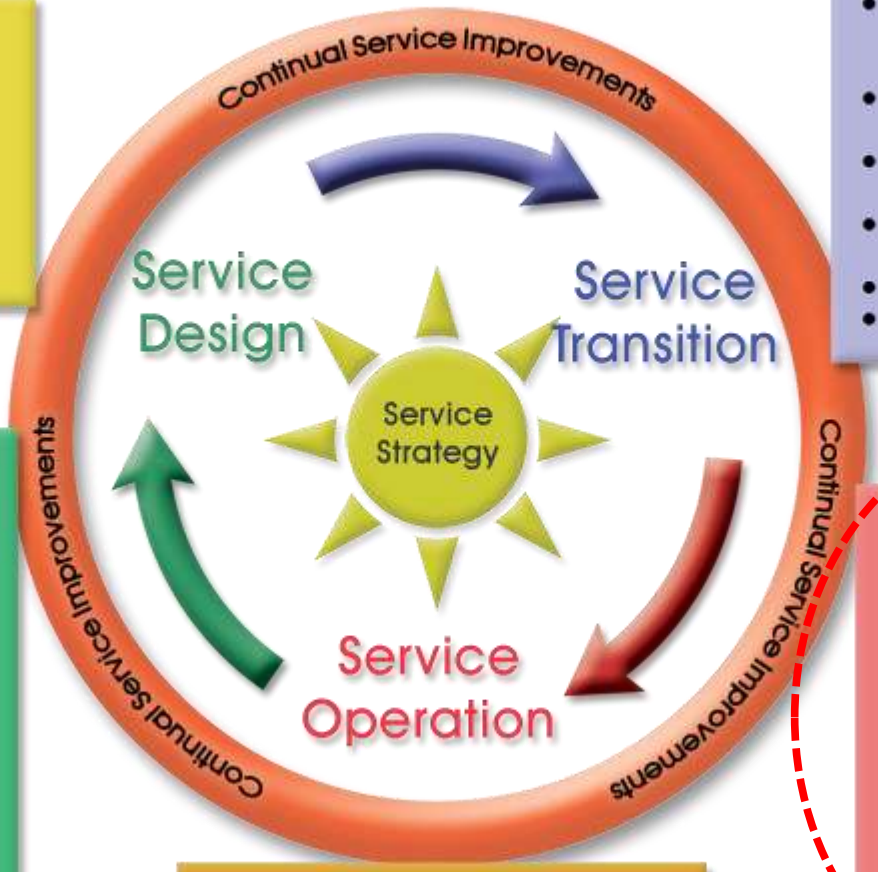
Залежно від об'єкту (цілі) аудиту пристосовуються стандарти/норми!

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

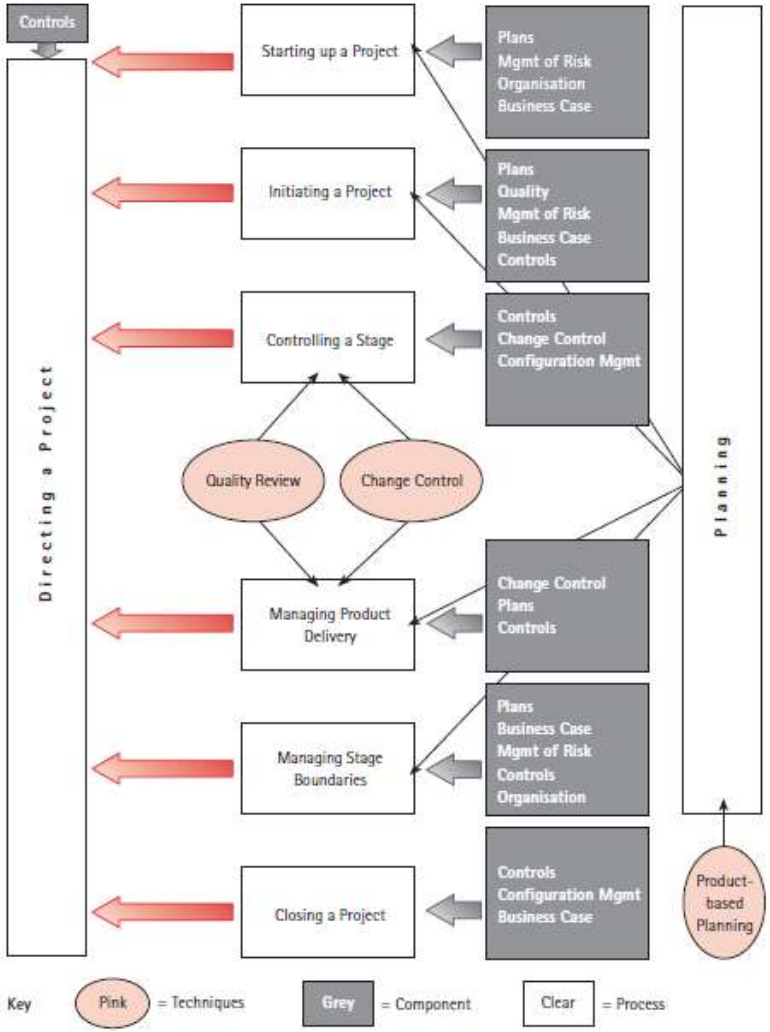


Figure 2.6 Use of PRINCE2 components and techniques in the processes

Adobe Acrobat Document

ISO27002: рамкова основа для Інформаційної безпеки

INTERNATIONAL STANDARD

ISO/IEC 27002

First edition
2005-06-15

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

Ключові загальні заходи ІТ-контролю

Ключові загальні заходи IT-контролю

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

Завдання

1. **Причини для тестування ключових загальних заходів IT-контролю?**

2. **Які ризики пов'язані з цими заходами контролю?**

Ризики використання IT

- Довіра до систем чи програм, які неточно опрацьовують дані, опрацьовують неточні дані, чи і те, і інше
- Неавторизований доступ (безпека/привілеї)
- Неавторизовані зміни (дані/системи/програми)
- Неналежне ручне втручання
- Потенційна втрата даних чи нездатність отримати доступ до даних, як необхідно

Рамкова основа загальних заходів IT-контролю

- 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

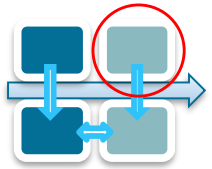
Microsoft Excel-werkblad

Управління доступом —Механізми контролю безпеки

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

<u>Ризики виникають з:</u>

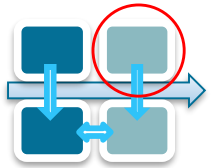
- Автентифікації (як користувачі ідентифікують себе)
- Налаштування безпеки (як IT-середовище обмежує доступ)
- Управління правами доступу



Управління доступом — Визначити ризик

Міркування

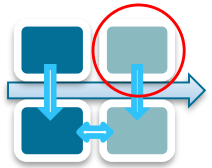
- Кількість користувачів
- Складність прав
- Простота розуміння прав доступу
- Централізація управління доступом
- Використання ролей/профілі користувачів
- Частота плинності кадрів



Управління доступом —Механізми контролю безпеки

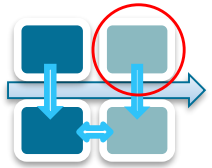
Ключові елементи контролю та тестування міркувань:

- Доступ до комп'ютерного забезпечення фізично захищений та обмежений авторизованими особами.
- Унікальні дані ідентифікації користувачів використовуються для забезпечення індивідуальної підзвітності
- Вимоги щодо надійних та складних паролів
- Ефективні механізми входу та заходи з управлінського огляду запроваджено



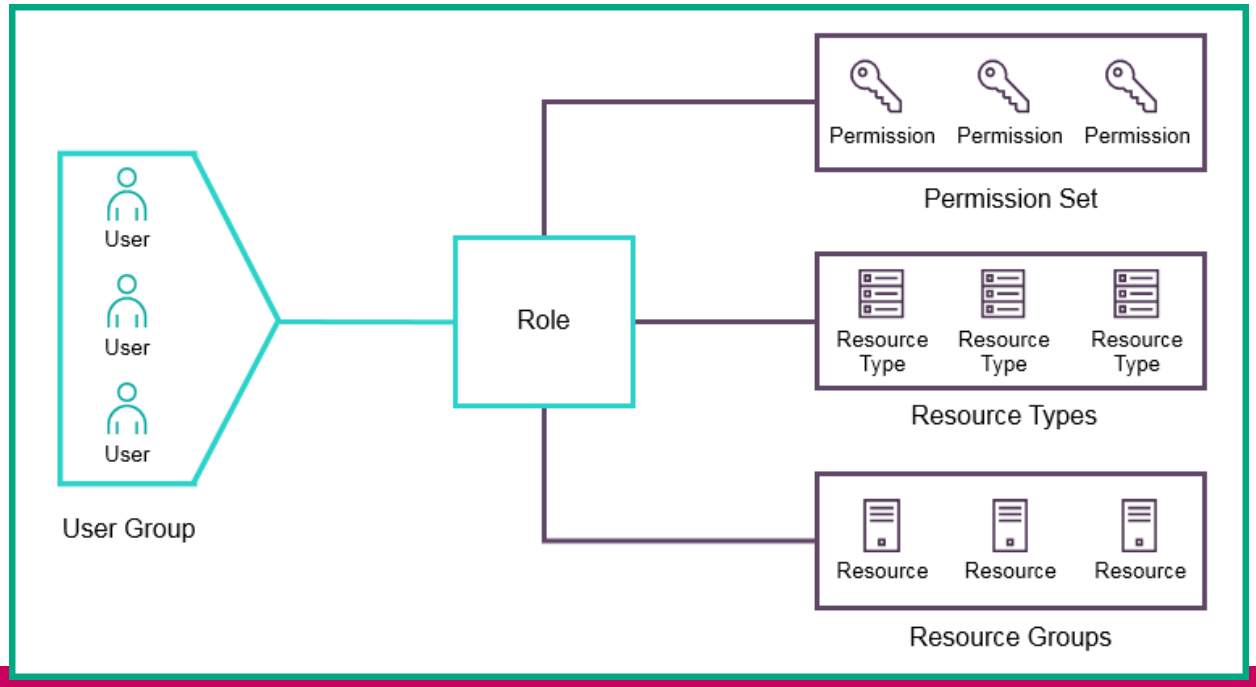
Управління доступом – Заходи контролю щодо користувача

1. Користувачі та адміністратори повинні мати тільки ті права доступу, які необхідні їм для роботи
2. Облікові записи та права доступу користувачів повинні бути авторизованими
3. Розподіл обов'язків повинен бути запровадженим для застосування, схвалення та запровадження змін в облікових записах користувачів та правах доступу
4. Має швидко опрацьовуватися звільнення персоналу
5. Облікові записи адміністраторів мають бути обмеженими і поясненими
6. Облікові записи користувачів та адміністраторів мають бути суворо особистими.
7. Облікові записи користувачів повинні не мати прямого доступу до основоположних компонентів.
8. Облікові записи та права доступу користувачів та адміністраторів повинні періодично оцінюватися і відстежуватися



Управління доступом - Запровадження (I)

- Процедури з надання доступу
- Періодична оцінка прав
- Контроль доступу відповідно до ролі



Управління доступом – Запровадження (II)

- Матриця контролю доступу

Діяльність	Адміністратор	Наглядач	Керівник
Створити обліковий запис користувача	X		
Видалити обліковий запис користувача	X		
Схвалити обліковий запис користувача		X	
Переглянути журнал			X
...			

Користувач	Роль
Лодевік	Адміністратор
Рурдьє	Керівник
..	..

Управління доступом – Запровадження(III)

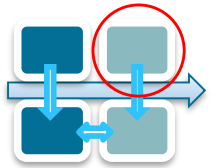
- **Активна директорія (каталог)**
  - Управління користувачами
  - Автентифікація та авторизація
  - Правила щодо паролів

Управління змінами – Авторизовані зміни відповідні процедури

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

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

- 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.

Управління змінами - критерії

1. Зміни повинні бути авторизовані
2. Зміни повинні бути протестовані
3. Зміни повинні бути схвалені за результатами тестування
4. Обов'язки із застосування, схвалення та запровадження змін повинні бути розділені
5. Неавторизовані зміни повинні періодично перевірятися

Робота на місці

Збір даних

На основі дизайну дослідження виберіть, які методи збору даних ви будете використовувати:

Набір інструментів (IT) аудитора:

- Камеральне дослідження
- Інтерв'ю
- Спостереження
- Семінар
- Огляди (напр.: Limesurvey)
- Механічна обробка
- Тестування в ході виконання
- Аналіз даних
- Тощо…

Документація дизайну

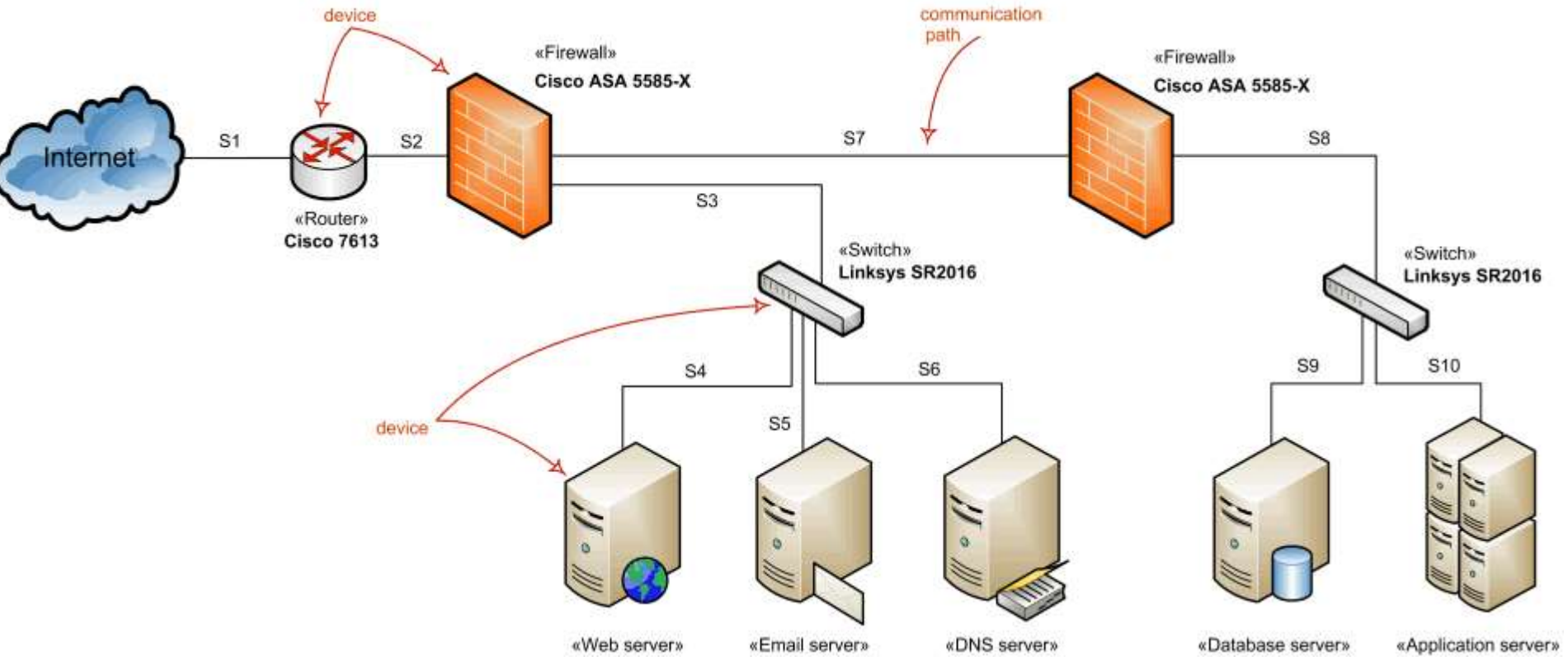
- Мапа мережевої інфраструктури
- Технічний дизайн
- Функціональний дизайн
- Документ з ініціювання проекту
- Документи архітектури
- Процедури
- Вказівки щодо загартування
- Угоди/звіти про рівень обслуговування
- Організаційна схема

Документи дизайну

- Функціональна, з використанням кейсів архітектура -> Що слід зробити?
- Технічна для рішень архітектура -> Як це запроваджується?

Мета: зрозуміти систему, доповнюйте інтерв'ю за потреби

Мапа мережевої інфраструктури



Документація з операційної ефективності

- Файли конфігурації
- Записи журналу
- Скріншоти
- Налаштування
- Результати механічної обробки
- Результати тестування
- Інспектування доказів (напр., управління змінами)
- Відповідність (повторне виконання)

Підготовлений замовником список

- Список необхідних документів для аудиту
- Іноді такий самий, як минулого року, іноді конкретизується під час прийняття завдання

Спостереження

- Налаштування
- Переконайтеся, що ви дивитеся на правильне середовище, сервер, та ін.

Кількість тестів

Частота заходів контролю	**Кількість тестів**
Щорічний	1
Щоквартальний	2
Щомісячний	3
Щотижневий	5
Щоденний	25

Кейс (збір даних)

- Яким був би ваш аудиторський підхід?
- Які методи збору даних ви б використали (і не використали)?
- Чому?

1. Управління патчами
2. Безпека мобільних застосунків

Оцінка і аналіз

Інтерпретація і оцінка знахідок (I)