Що ви обираєте?

Основи аудиту інформаційних технологій (IT-аудит)

В умовах стрімкого розвитку інфраструктури та поглиблення інформатизації господарських процесів ефективність діяльності підприємств, установ та організацій дедалі більше залежить від інформаційних технологій (ІТ), що використовуються в системах управління.

Все більшого значення набуває регулярне проведення в системі управління організації (установи) аудиту інформаційних технологій (ІТ-аудиту).

IT-аудити є ключовим компонентом для забезпечення якості інформаційних систем та прикладного програмного забезпечення. Без надійних інформаційних систем та результативних IT-заходів контролю, організація не взмозі правильно виконувати операції/транзакції та узагальнювати надійну фінансову звітність, що, своє чергою, впливає на рівень досягнення поставлених перед нею завдань та цілей

IT-аудит - це незалежна і неупереджена оцінка:

- надійності, безпеки (включаючи безпеку персональних даних), результативності та ефективності автоматизованих інформаційних систем,
- технічно-організаційної інфраструктури обробки автоматизованої інформації.

Ця діяльність поширюється як на діючі операційні системи, так і на системи, які розробляються.

Середовище/світ IT

- IT управління
- Проекти та програми
- Процеси та інформаційні системи
- Управління IT-послугами
- Інфраструктура
- Інформаційна безпека

Об'єкти аудиту в IT-управлінні

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

Більшість ризиків у IT мають місце на 1 і 2 рівні!

Більшість проблем на 3 і 4 рівні.

IT-аудитор оцінює один чи більше аспектів якості IT-аудиту.

Найбільш поширеними аспектами якості в IT-аудиті є:

Надійність - у загальному надійність можна визначити, як вірогідність того, що інформаційна система на задовільному рівні виконає завдання, для якого її було розроблено або задумано, за певний період часу у визначеному середовищі.

Безпека – означає захист інформації та інформаційних систем від неавторизованого доступу або зміни інформації, яка зберігається, обробляється або передається, а також відмови у послузі не авторизованим користувачам. Безпека інформації передбачає заходи, необхідні для виявлення, документування і боротьби з такими загрозами.

Результативність - це здатність досягнути бажаного результату

Ефективність - означає виконання або здатність виконати завдання у співвідношенні із затратами часу і ресурсів.

Типові для державних установ види IT-аудиту

IT-аудит безпеки (конфіденційність, цілісність і доступність): Ідеться не тільки про безпеку інформації у системі чи прикладній програмі, а й також про те, як організована безпека інформації, цілісність систем та розподіл відповідальності в державній установі.

IT-аудит якості (результативність, ефективність): У цьому IT-аудиті розглядається якість інформаційної системи, прикладної програми або/і бізнес процесів.

Аудит IT-проекту, під час якого внутрішній аудитор перевіряє управління та організацію IT-проекту, наприклад, запровадження інформаційної системи.

Аналіз даних: не зовсім IT-аудит, але часто це частина фінансового аудиту. IT-аудитор може виконувати функцію підтримки в аналізі фінансових даних. Завдання IT-аудитора полягає у виокремленні та зборі фінансової інформації з бази даних інформаційної системи, у запитах та звітах, необхідних для аналізу фінансових даних

Увага!!! Окремі IT-аудити проводиться дуже рідко.
Як правило, вони є елементами аудиту ефективності.

Приклади IT-аудитів, що проводила Центральна служба внутрішнього аудиту в Нідерландах

- Тестування системи онлайн аукціону, що був застосований урядом для аукціонера Telecom.
- Поради в частині автоматизації документальних процесів Міністерств.
- Тестування безпеки Blackberries, які застосовують службовці
- Тестування системи автоматизованих систем подачі заяв громадянами, у яких зберігаються дані про повернені податки.
- Аудит безпеки хмаринкових та віртуальних технологій.
- Аудит інформаційних центрів
- Тестування програмних модулів у великих фінансових системах.

Критерії IT-аудиту

Для проведення IT-аудиту, IT-аудитору необхідний належний набір критеріїв аудиту, які можна застосувати до об’єкта IT-аудиту.

Критерії аудиту – це принципи (або норми), які використовуються для оцінки

Набір критеріїв аудиту може бути поєднаним, наприклад:

- COBIT (як правило витяг);
- вимога з внутрішнього положення або законодавства;
- процес/правила/процедури організації IT процесу або їх частина.

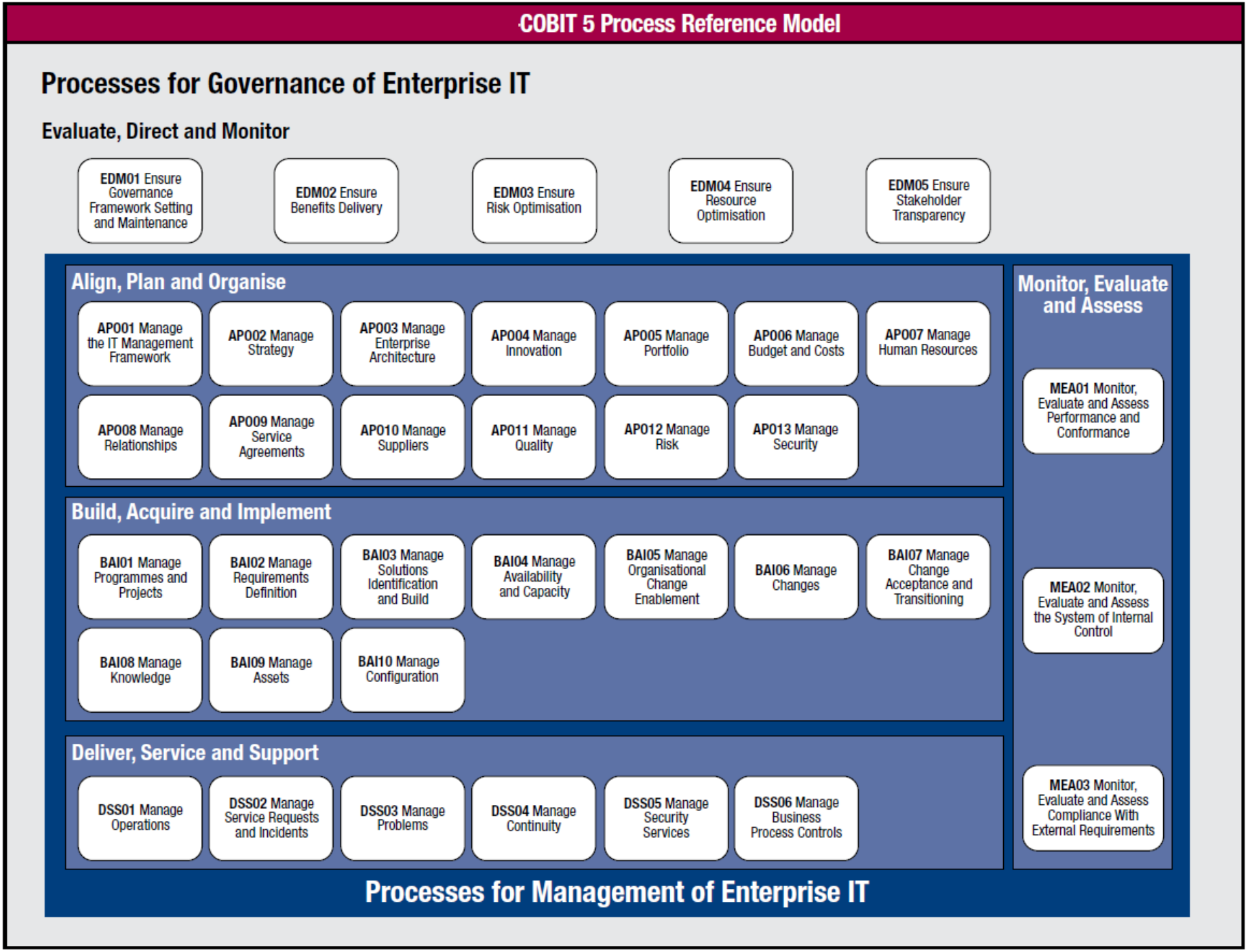
Основи (стандарти, норми), які використовуються під час проведення IT-аудиту

- COBIT 5
- ITIL V3
- PRINCE 2
- ASL
- BiSL
- ISO/IEC 27001 і 27002
- Керівництво з аудиту глобальних технологій 8
- Загальна програма аудиту/гарантії прикладних програм

Для обрання правильної основи IT-аудитор має вирішувати, яка основа найбільш підходить по відношенню до IT-об’єкта

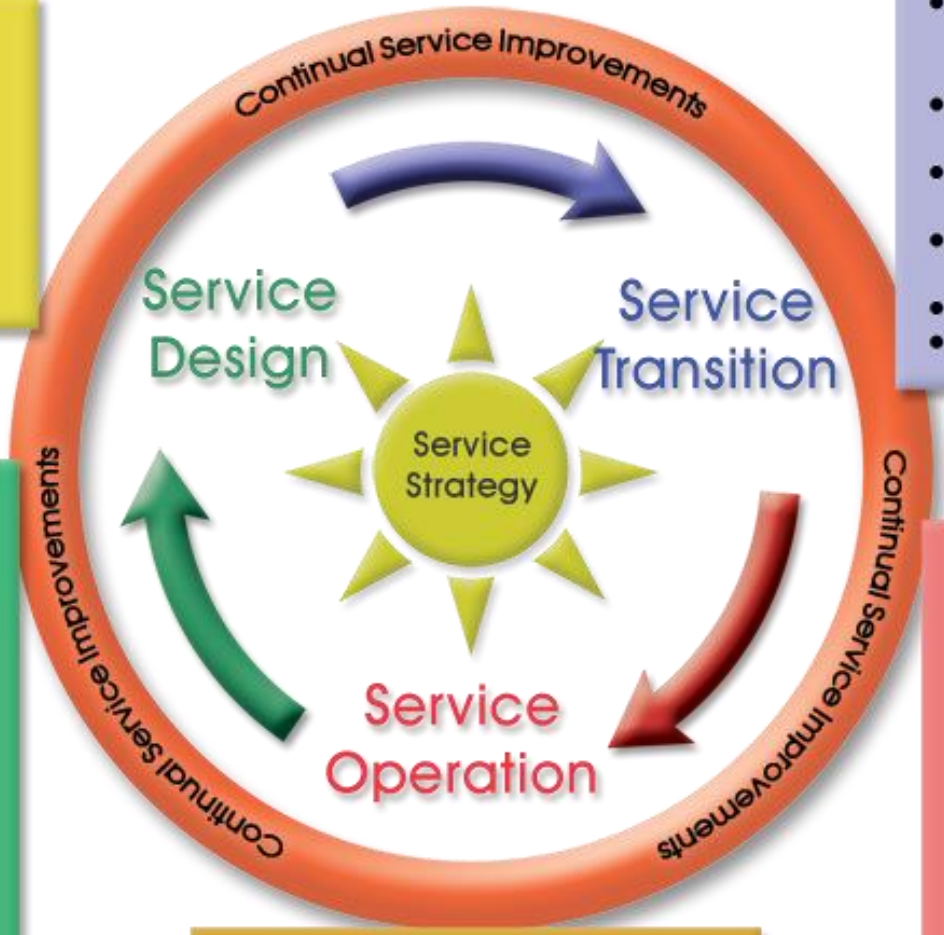
- Якщо IT-об’єкт – це Безпека, то найкращий вибір – ISO/IEC 27001.
- Якщо IT-об’єкт – це Проект, то найкращий вибір – PRINCE 2.
- Якщо IT-об’єкт – це Заходи контролю за прикладними програмами, то найкращий вибір – це GTAG-8 або Загальна програма аудиту/гарантії прикладних програм.
- Якщо IT-об’єкт – це якість процесів IT-департаменту, тоді, найкраща основа ITIL

CobiT (Control Objectives for Information and Related Technologies) "Завдання управління для інформаційних та суміжних технологій" - являє собою пакет документів, близько 40 міжнародних і національних стандартів і керівництв в галузі управління IT , аудиту та IT-безпеки


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
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 – (Infrastructure Library) “Бібліотека інфраструктури інформаційних технологій” - бібліотека, що описує найкращу практику застосування способів організації роботи підрозділів або компаній, що займаються наданням послуг у галузі інформаційних технологій

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