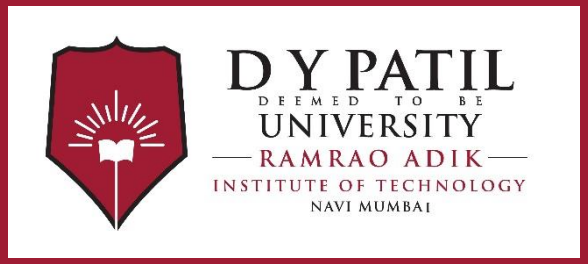


Information Security

Module: 6

•Faculty: Mrs. Bhavana Alte
• Mr. Prathmesh Gunjgur

Contents

Module 6:

Lecture 34: Operating System Security

Enterprise Security Architecture

- An enterprise security architecture is an integrated and comprehensive strategy for protecting the organization against cyber threats. To achieve comprehensive protection, an organization needs to ensure that there are no visibility or protection gaps that an attack could slip through.

- An enterprise license agreement (ELA) provides a means for an organization to simply and efficiently deploy security solutions across its entire environment. With an ELA, an organization has access to all of a vendor's cyber security solutions to achieve comprehensive and integrated security across networks, endpoints, mobile devices, cloud infrastructure, and IoT devices.

Enterprise Security Architecture

- An enterprise security architecture is a strategy for providing comprehensive protection for an organization against cyber threats. The three core principles are consolidation, zero trust, and threat prevention.
- Consolidation: A consolidated security architecture is essential to effectively and scalably managing an organization's security risk. Security integration enables security visibility and threat management via a centralized, user-friendly interface, eliminating inefficient context switching and improving the performance of the corporate SOC.
- Zero trust: A zero-trust security strategy tailors the permissions assigned to a user, application, or system to what is necessary for their role. This limits the probability and impact of security incidents by limiting what an attacker can access within an organization's environment.
- Threat Prevention: Prevention is a strategic approach to threat management. An enterprise security architecture should proactively take steps to block the access vectors used by cyberattackers and identify and block threats before they reach corporate systems. With prevention, an attacker has no opportunity to access or damage corporate systems, minimizing the cost and impact of an attack on the organization.

Enterprise Security Architecture

- Benefits of an Enterprise Security Architecture: By deploying an enterprise cyber security architecture with an ELA, an organization can achieve significant benefits, including:
- Lower TCO: An integrated security architecture with an ELA eliminates overlapping and underutilized security tools. Additionally, with an ELA, an organization may have access to competitive pricing and discounts.
- Operational Efficiency: An enterprise security architecture is composed of solutions that are designed to work together to provide the organization with comprehensive protection against threats. By eliminating security gaps and overlapping solutions and simplifying security monitoring and management, an enterprise security architecture increases the efficiency of the corporate security architecture and SOC.
- Interoperability with IT Infrastructure and Existing Integrations: An enterprise cyber security architecture is built out of solutions designed for integration. This enables an organization to integrate solutions with its existing infrastructure.
- Enterprise Security Solution for All Company Sizes: With an ELA, an organization purchases credits that provide access to various security solutions. This enables an organization to tailor its security architecture to its unique needs and budget.

Enterprise Security Architecture

- SABSA is an Enterprise Security Architecture Framework. It stands for “Sherwood Applied Business Security Architecture” as it was first developed by John Sherwood.
- The concept of architecture as the means by which we integrate different solutions and approaches to differing and complex needs, and provides a mechanism to manage such complexity.
- Layers, from the most general to the most specific under SABSA, are as follows:
  - Conceptual Security Architecture
  - Contextual Security Architecture
  - Logical Security Architecture
  - Physical Security Architecture
  - Component Security Architecture
- Step-by-step you extend the chain of traceability through the entire security architecture.The basic questions are answered
  - what is being considered
  - when is the activity performed
  - how is the activity performed
  - who performs the activity
  - where is the activity performed

Enterprise Security Architecture

Table 2: SABSA Architecture Matrix™ 2018

	ASSETS (What)	MOTIVATION (Why)	PROCESS (How)	PEOPLE (Who)	LOCATION (Where)	TIME (When)
CONTEXTUAL ARCHITECTURE	Business Goals & Decisions	Business Risk	Business Meta-Processes	Business Governance	Business Geography	Business Time Dependence
	Business Value; Taxonomy of Business Assets, including Goals & Objectives , Success Factors, Targets	Opportunities & Threats Inventory	Business Value Chain; Business Capabilities	Organisational Structure & the Extended Enterprise	Inventory of Buildings, Sites, Territories, Jurisdictions, etc.	Time dependencies of Business Goals and Value Creation
CONCEPTUAL ARCHITECTURE	Business Value & Knowledge Strategy	Risk Management Strategy & Objectives	Strategies for Process Assurance	Security & Risk Governance; Trust Framework	Domain Framework	Time Management Framework
	Business Attributes Taxonomy & Profile (with integrated performance targets)	Enablement & Control Objectives; Policy Architecture; Risk Categories; Risk Management Strategies; Risk Architecture; Risk Modelling Framework; Assurance Framework.	Inventory of all Operational Processes (IT, industrial, & manual); Process Mapping Framework; Architectural Strategies for IT used in process support.	Owners, Custodians and Users; Service Providers & Customers; Trust Modelling Framework	Security Domain Concepts & Framework	Through-Life Risk Management Framework; Attribute Performance Targets
LOGICAL ARCHITECTURE	Information Assets	Risk Management Policies	Process Maps & Services	Trust Relationships	Domain Maps	Calendar & Timetable
	Inventory of Information Assets; Information Model of the Business	Risk Models; Domain Policies; Assurance Criteria (populated Assurance Framework).	Information Flows; Functional Transformations; Service Oriented Architecture; Services Catalogue; Application Functionality and Services	Domain Authorities; Entity Schema; Privilege Profiles; Trust Relationship Models	Domain Definitions; Inter-domain Associations & Interactions	Start Times, Lifetimes & Deadlines
PHYSICAL ARCHITECTURE	Data Assets	Risk Management Practices	Process Mechanisms	Human Interface	Infrastructure	Processing Schedule
	Data Dictionary & Data Storage Devices Inventory	Risk Management Rules & Procedures; Risk Metadata	Working Procedures; Application Software; Middleware; Systems; Security Mechanisms; Process Control Points	User Interface to Business Systems; Identity & Access Control Systems	Workspaces; Host Platforms, Layout of Devices & Networks	Timing & Sequencing of Processes and Sessions
COMPONENT ARCHITECTURE	Component Assets	Risk Management Components & Standards	Process Components & Standards	Human Entities: Components & Standards	Locator Components & Standards	Step Timing & Sequencing Components and Standards
	Products and Tools, including Data Repositories and Processors	Risk Analysis Tools; Risk Registers; Risk Monitoring and Reporting Tools	Tools and Protocols for Process Delivery; Application Products	Identities; Job Descriptions; Roles; Functions; Actions & Access Control Lists	Nodes, Addresses and other Locators; Component Configuration	Time Schedules; Clocks, Timers & Interrupts
MANAGEMENT ARCHITECTURE	Delivery and Continuity Management	Operational Risk Management	Process Delivery Management	Governance, Relationship & Personnel Management	Environment Management	Time & Performance Management
	Assurance of Operational Excellence & Continuity	Risk Assessment; Risk Monitoring & Reporting; Risk Treatment	Management & Support of Systems, Applications & Services	Management & Support of Enterprise-wide and Extended Enterprise Relationships	Management of Buildings, Sites, Platforms & Networks	Management of Calendar and Timetable

Module 6:

Lecture 38: Enterprise Security

Enterprise Security Architecture

- COBIT 5 framework or Control Objectives for Information and Related Technologies 5 framework was developed to guide IT governance and management. The COBIT 5 framework was first released by ISACA in April 2012 and is essential to developing, controlling, and maintaining risk and security for organizations worldwide.
- COBIT 5 includes
  - Strategic Alignment
  - Value Delivery
  - Resource Management
  - Risk Management
  - Performance Management
- Governance objectives are Evaluate, Direct, and Monitor (EDM)
  - Evaluate-It involves agreeing and identifying objectives that need to be achieved
  - Direct- This includes decision-making and prioritization
  - Monitor- Compliance, and performance against objectives

Enterprise Security Architecture

Components of COBIT 5 Framework

- Framework – It organizes IT governance objectives and links them to business requirements by ensuring good practices of IT domains and processes are implemented simultaneously.

- Process Description – A reference process model that is followed during the implementation, which is available for everyone working in the enterprise. It maps the responsibility areas of Plan, Build, Run, and Monitor (PBRM).

- Control Objectives – Provide a complete set of high-level requirements to be considered by the management for effective control of each IT process.

- Management Guidelines – These help to assign responsibility to agree on objectives and measure performance to illustrate the relationship between each individual process.

- Maturity Models – Access maturity and capability for each process and help to address gaps in the implementation of the processes.

Enterprise Security Architecture

COBIT 5 is based on five principles that are essential for the effective management and governance of enterprise IT:
Principle 1: Meeting stakeholder needs
Principle 2: Covering the enterprise end to end
Principle 3: Applying a single integrated framework
Principle 4: Enabling a holistic approach
Principle 5: Separating governance from management

Benefits of COBIT
The COBIT 5 framework can help organizations of all sizes:

- Improve and maintain high-quality information to support business decisions.
- Use IT effectively to achieve business goals.
- Use technology to promote operational excellence.
- Ensure IT risk is managed effectively.
- Ensure organizations realize the value of their investments in IT; and
- Achieve compliance with laws, regulations and contractual agreements.

Enterprise Security Architecture

- TOGAF stands for The Open Group Architecture Framework. It is an enterprise architecture methodology. The Open Group developed it in 1995.

- TOGAF aims to help the organization address their needs through four main goals:

  - Getting a provable return on investment (ROI).
  - Utilizing more cost and money-effective resources.
  - Avoiding being “locked in.”
  - Making sure that the stakeholders and team members are speaking the same language.

Enterprise Security Architecture

TOGAF works on three main pillars that make it possible to achieve the goals listed above. These pillars demonstrate an organized process that helps utilize technology in a way that meets the business objectives.

The three key pillars of TOGAF are:

Enterprise Continuum: It is a classification system that tracks customized enterprise solutions from generic to industry standards.

Architecture Development Model (ADM): Its goal is to develop enterprise architecture with the help of performance engineering.

Domains of enterprise architecture: They are divided into four main parts:

- Business architecture: It outlines business strategies and the organization of processes.
- Data architecture: It records how the data assets and management resources are structured.
- Applications architecture: It defines a blueprint for the deployment of individual systems.
- Technical architecture: It includes the hardware, software, and network infrastructure.

Enterprise Security Architecture

ADM stands for Architecture Development Method. It is the core of TOGAF that is responsible for developing Enterprise Architecture that aligns with the business requirements.

The ADM consists of 4 steps:

Adjusting TOGAF to meet the system and business requirements.
Defining the scope of work and preparing for rollout.
Managing the development and implementation of the architecture.
Handling the changes after implementation.

Enterprise Security Architecture

ADM stands for Architecture Development Method. It is the core of TOGAF that is responsible for developing Enterprise Architecture that aligns with the business requirements.

The ADM consists of 4 steps:

Adjusting TOGAF to meet the system and business requirements.
Defining the scope of work and preparing for rollout.
Managing the development and implementation of the architecture.
Handling the changes after implementation.

Enterprise Security Architecture

Phases within the ADM are as follows:

The Preliminary Phase describes the preparation and initiation activities required to prepare to meet the business directive for new enterprise architecture, including the definition of an Organization-Specific Architecture framework and the definition of principles.

Phase A: Architecture Vision describes the initial phase of an architecture development cycle. It includes information about defining the scope, identifying the stakeholders, creating the Architecture Vision, and obtaining approvals.

Phase B: Business Architecture describes the development of a Business Architecture to support an agreed Architecture Vision.

Phase C: Information Systems Architectures describes the development of Information Systems Architectures for an architecture project, including the development of Data and Application Architectures.

Enterprise Security Architecture

Phases within the ADM are as follows:
Phase D: Technology Architecture describes the development of the Technology Architecture for an architecture project.

Phase E: Opportunities & Solutions conducts initial implementation planning and the identification of delivery vehicles for the architecture defined in the previous phases.

Phase F: Migration Planning addresses the formulation of a set of detailed sequence of transition architectures with a supporting Implementation and Migration Plan.

Phase G: Implementation Governance provides architectural oversight of the implementation.

Phase H: Architecture Change Management establishes procedures for managing change to the new architecture.

Requirements Management examines the process of managing architecture requirements throughout the ADM.

Module 6:

Lecture 39: Database Auditing

Database Auditing

- Database auditing involves observing a database so as to be aware of the actions of database users. Database administrators and consultants often set up auditing for security purposes, for example, to ensure that those without the permission to access information do not access it.
- Areas that should audited to lessen the risk of a database getting hacked:

  - User Access and Authentication: Anyone from inside or outside an organization can get in through this door. In some cases, privileged users may be able to update or extract financial information from client data, or they may try to access the system at a time when they are not allowed to for nefarious motives.
  - Database Objects: People with access to database items, such as users' or companies' data, processes, or logic that define a system's functionality, can alter the structure, resulting in regular data corruption or theft. And if auditing is not enabled, you won't be able to account for any of it. Tables, views, procedures, database linkages, and run-time logical flows that manage business applications should get audited to ensure their integrity.

Database Auditing

- Areas that should audited to lessen the risk of a database getting hacked:
  - Data Access: A company's data is its most crucial component. All confidential and restricted data should not get accessed by anybody other than the intended recipients granted access to it.
  - Network: Huge amounts of data are also available on a variety of devices. You may need a lot of bandwidth for both on-premises and cloud-based applications. With the help of an audit of a network, you may better understand the massive amounts of data generated and determine where additional network resources are needed.

Database Auditing

Types of Auditing:

- Schema object auditing: It allows us to specify schema objects to be audited.
- SQL statement auditing: It allows us to specify SQL statements to be audited.
- SQL privilege auditing: It allows us to specify system privileges to be audited.

The audit facility allows you to specify the scope of audit actions as follows:

- By user: This allows us to audit a certain user, by default it is all users.
- Whenever Successful/Whenever unsuccessful: This allows us to specify whether we want auditing to always occur or only whether the specific action was successful or unsuccessful. By default, it is BOTH.
- By Session/ By Access: This allows us to assign how frequently audit files are to be created. By default, it is by access. A stream pool is utilized to build a buffer for the data pump.

Limits of Auditing: Database auditing service works on the statement level only. It will record a scenario in case a specific user has run a select query against a particular table, but it is incapable of telling you which rows have been retrieved. This enables auditing to the database.

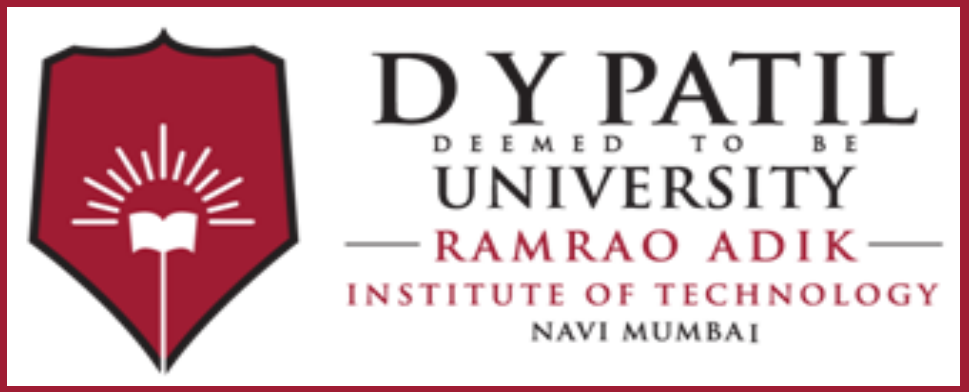
Database Auditing

Database auditing is essential for the following reasons:

- Maintain Data Quality It doesn't matter if you run a tiny business or a giant corporation when it comes to your database. You have complete control over where your customers' advertising appears online. The more precise audience targeting you can provide advertisers, the more they will trust you and remain loyal consumers. Here, success depends on having accurate and up-to-date information about your customers.

- Compliance with Data Privacy & Protection Regulations: Publishers and advertisers must keep data privacy compliance in mind in today's digital world. As a result of database audits, you'll be able to take advantage of new business prospects with the knowledge that your organization is adhering to regulations.

- Reducing Security Risks: It is impossible to exaggerate the importance of security to user trust and customer relationships. Regular database audits mean you're less likely to be attacked or caught off guard by a security breach.


D Y PATIL
DEEMED TO BE
UNIVERSITY
RAMRAO ADIK
INSTITUTE OF TECHNOLOGY
NAVI MUMBAI

Thank You