



**The Institute of Cost Accountants of India**

# **INFORMATION SYSTEM SECURITY AUDIT**

**BATCH: 5**



*Elocutionist: Dr. Saurabh Maheshwari*

# Chapter – 5

**BUSINESS APPLICATION-  
ACQUISITION, DEVELOPMENT  
& IMPLEMENTATION**



# NEEDS AND BENEFITS OF SDLC

- Relevance of SDLC for Business Process Automation
- Need for SDLC
- Benefits of SDLC



# SDLC & PHASES OF SDLC

Software Development Life Cycle (SDLC) is a process used in the software industry to design, develop and test high-quality software packages. It consists of a detailed plan describing how to develop, maintain, replace and alter or enhance specific software that meets or exceeds customer expectations, reaches completion within times, and cost estimates.

- Phase 1: Preliminary Investigation
- Phase 2: Requirement Analysis
- Phase 3: System Analysis & System Design
- Phase 4: Acquisition of System Resources
- Phase 5: System Development
- Phase 6: System Testing & User Training
- Phase 7: System Implementation
- Phase 8: Post-Implementation Review & System Maintenance

... cont.

- Phase 1: Preliminary Investigation
- Phase 2: Requirement Analysis
- Phase 3: System Analysis & System Design
- Phase 4: Acquisition of System Resources
- Phase 5: System Development
- Phase 6: System Testing & User Training
- Phase 7: System Implementation
- Phase 8: Post-Implementation Review & System Maintenance

- Problem Identification & Setting Objectives
- Feasibility Study
  - Technical
  - Financial
  - Economical
  - Scheduled
  - Resources
  - Compliance / Legal
  - Behavioural / Social
  - Operational
- Business Case
- Auditor's Role

... cont.

- Phase 1: Preliminary Investigation
- Phase 2: Requirement Analysis
- Phase 3: System Analysis & System Design
- Phase 4: Acquisition of System Resources
- Phase 5: System Development
- Phase 6: System Testing & User Training
- Phase 7: System Implementation
- Phase 8: Post-Implementation Review & System Maintenance

- Requirement collection [Document Review, Questionnaire, Interviews, and Observations]
- Analysing current system of working
  - Source Document Review
  - Input Review
  - Processing Review
  - Output Review
  - Storage Review
  - Security Review
- Preparation of SRS [System Requirement Specifications]
- Auditor's Role

... cont.

- Phase 1: Preliminary Investigation
- Phase 2: Requirement Analysis
- Phase 3: System Analysis & System Design
- Phase 4: Acquisition of System Resources
- Phase 5: System Development
- Phase 6: System Testing & User Training
- Phase 7: System Implementation
- Phase 8: Post-Implementation Review & System Maintenance

- System Analysis
- System Design
  - DFD
  - CASE Tools
  - Data Dictionary / Meta Data
  - System Component Matrix
  - Decision Table / Decision Trees
  - Screen Layouts [UI – UX]
  - Other
- Drafting SDR [System Design Report]
- Finalizing System Development Approach / Strategy
  
- Auditor's Role



# SYSTEM DEVELOPMENT APPROACHES / METHODOLOGIES

- Waterfall Approach
- Prototype Approach
- Incremental Approach
- Re-Engineering Methodology
- Reverse Engineering Approach
- Component-Based System Development Approach
- RAD Approach
- Agile Methodology
- Web-based Approach



... cont.

- Phase 1: Preliminary Investigation
- Phase 2: Requirement Analysis
- Phase 3: System Analysis & System Design
- Phase 4: Acquisition of System Resources
- Phase 5: System Development
- Phase 6: System Testing & User Training
- Phase 7: System Implementation
- Phase 8: Post-Implementation Review & System Maintenance

- Finalizing Specification
- Releasing ITT & RFP for inviting bids
- Vendor validation
- Documentations with Vendor
  
- Auditor's Role

... cont.

- Phase 1: Preliminary Investigation
- Phase 2: Requirement Analysis
- Phase 3: System Analysis & System Design
- Phase 4: Acquisition of System Resources
- Phase 5: System Development
- Phase 6: System Testing & User Training
- Phase 7: System Implementation
- Phase 8: Post-Implementation Review & System Maintenance

No direct involvement

- Auditor's Role
  - Debugging
  - Adhering of standards and compliance
  - Documentation

... cont.

- Phase 1: Preliminary Investigation
- Phase 2: Requirement Analysis
- Phase 3: System Analysis & System Design
- Phase 4: Acquisition of System Resources
- Phase 5: System Development
- Phase 6: System Testing & User Training
- Phase 7: System Implementation
- Phase 8: Post-Implementation Review & System Maintenance


- System Testing
  - Black Box – White Box – Gray Box
  - Alpha – Beta
  - Unit – Integration – System & Regression
    - ✓ Security – Recovery
    - ✓ Stress / Volume / Load
    - ✓ Quality – Functional – Structural – Legal
    - ✓ Performance Testing
    - ✓ Portability Testing
  - UAT
- User Training
- Documentation ?
- Auditor's Role

... cont.

- Phase 1: Preliminary Investigation
- Phase 2: Requirement Analysis
- Phase 3: System Analysis & System Design
- Phase 4: Acquisition of System Resources
- Phase 5: System Development
- Phase 6: System Testing & User Training
- Phase 7: System Implementation
- Phase 8: Post-Implementation Review & System Maintenance

- Pre-Requisites of Implementation
  - Site Preparation
  - Hardware & Networking Equipment Testing & Installation
  - Testing Completed Satisfactorily
  - Training & Job Scheduling
  - Data Conversion
- Implementation/ Conversion Strategies
  - Direct / Abrupt
  - Phased
  - Pilot
  - Parallel
- Documentation ?
- Auditor's Role

... cont.

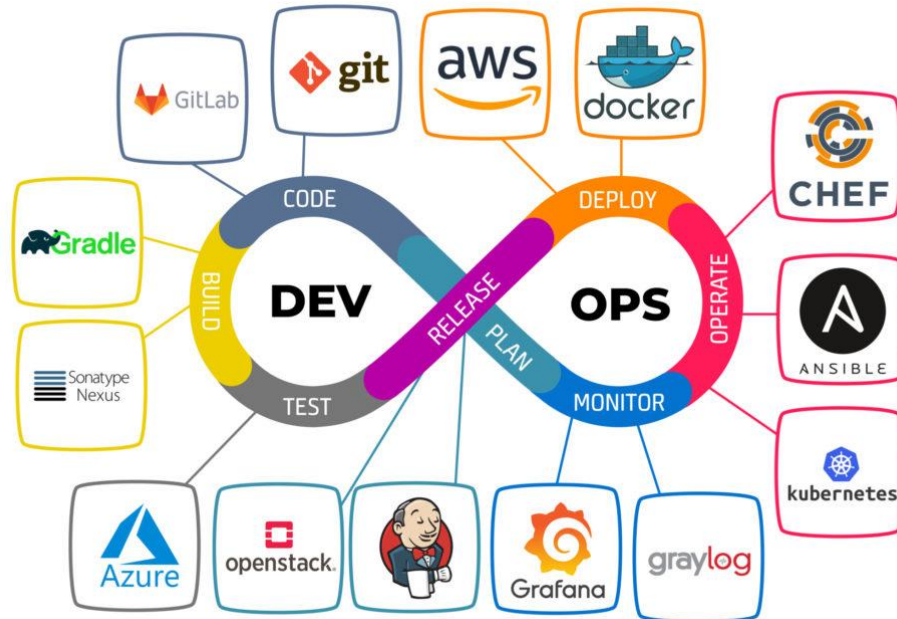
- Phase 1: Preliminary Investigation
  - Phase 2: Requirement Analysis
  - Phase 3: System Analysis & System Design
  - Phase 4: Acquisition of System Resources
  - Phase 5: System Development
  - Phase 6: System Testing & User Training
  - Phase 7: System Implementation
  - Phase 8: Post-Implementation Review & System Maintenance
- 

- System Evaluation / Post Implementation Review
  - Development Evaluation
  - Operation Evaluation
  - Information Evaluation
  - Evaluation on the basis of Objectives
- Maintenance
  - Scheduled
  - Corrective
  - Adaptive
  - Perfective
  - Preventive
  - Rescue / Fire Fighting
- Documentation ?
- Auditor's Role



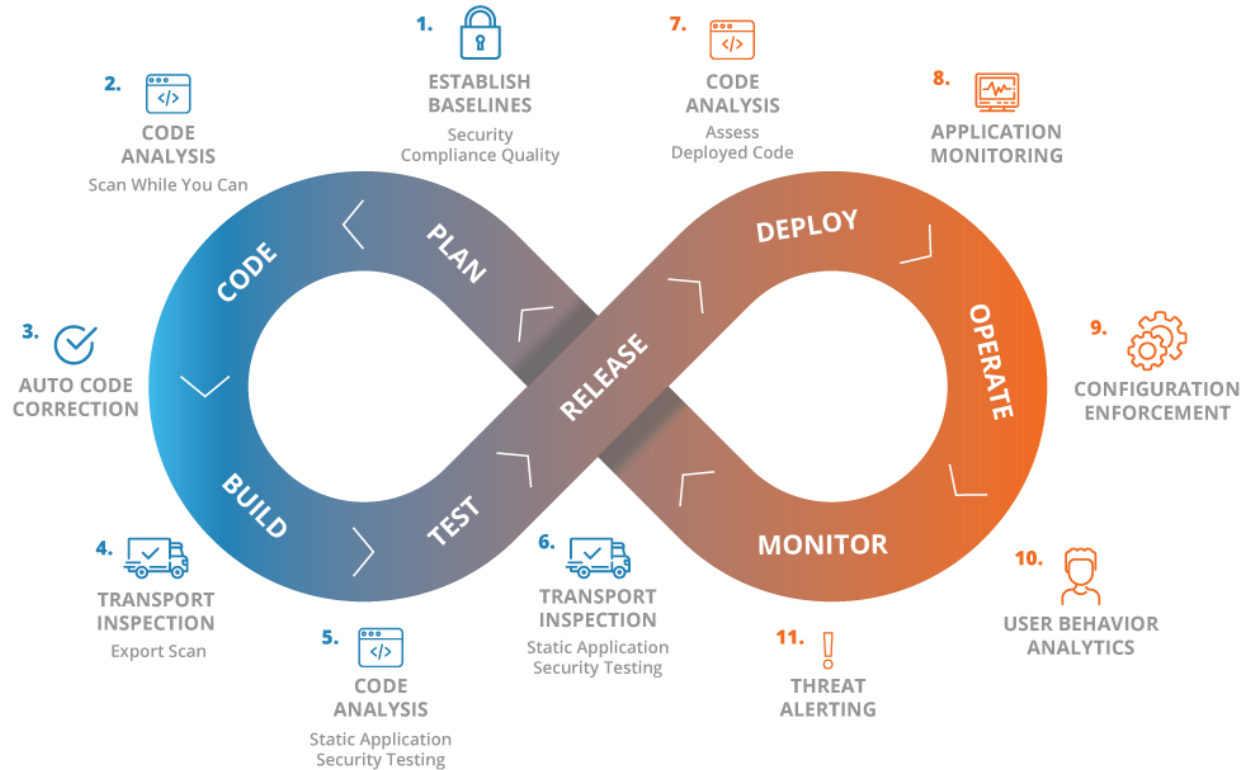
# DEVOPS

## ■ DevOps

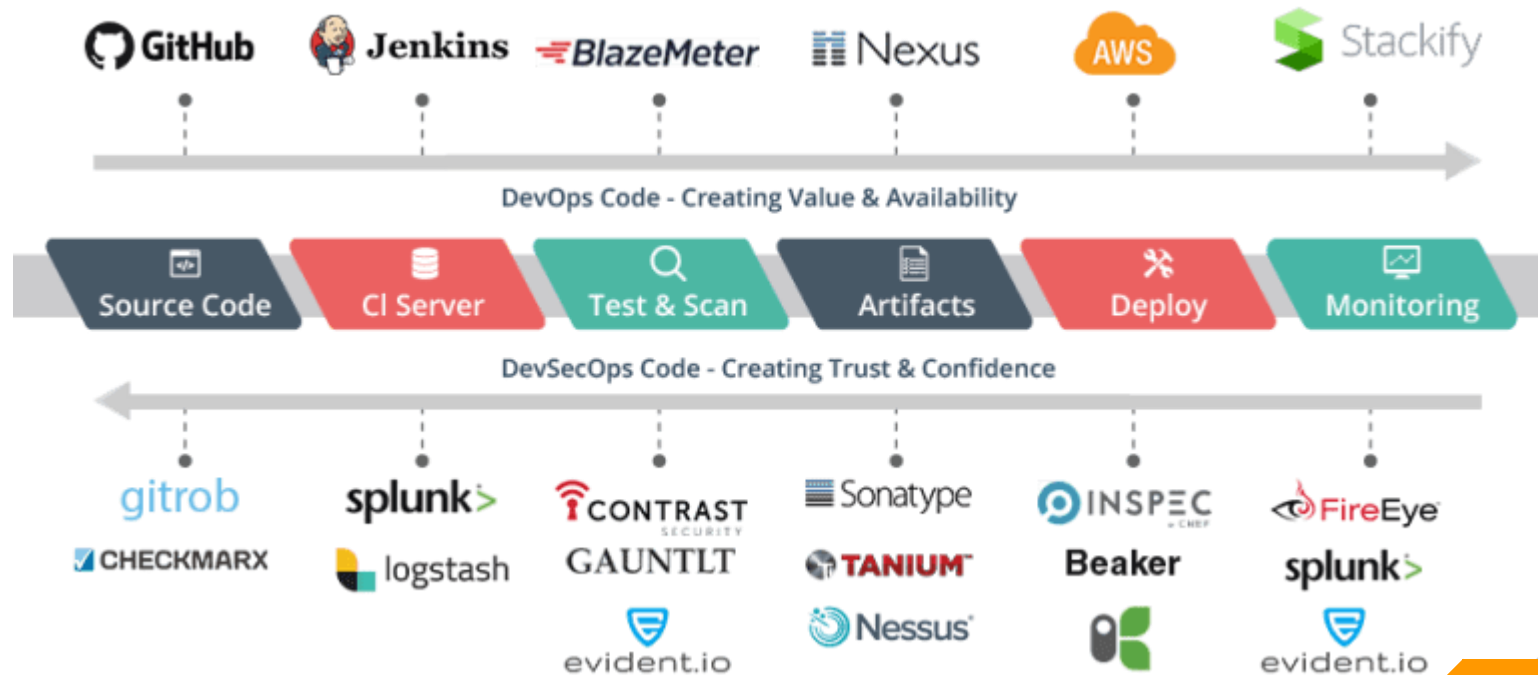


## DEVSECOPS / SECURE SDLC

- DevSecOps is a software development approach that emphasizes the integration of security practices and principles into the software development process, as well as collaboration and communication among development, security, and operations teams. It combines the principles of DevOps, which emphasizes collaboration and communication among development, operations, and other teams involved in the software development process, with security practices and principles.
- In a DevSecOps approach, security is not viewed as a separate or isolated process, but rather an integral part of the entire software development lifecycle. The goal of DevSecOps is to ensure that security is integrated throughout the development process and not added as an afterthought, which can lead to delays, higher costs, and increased risks.
- DevSecOps teams work to automate security processes and integrate security controls into the continuous integration and continuous delivery (CI/CD) pipeline. This approach allows security teams to identify and address security issues earlier in the development process, resulting in faster and more secure software delivery.









## APPLICATION CONTROLS & AUDIT



“

*Two-thirds of the Earth is covered with Water and the rest one-third is covered with Auditors from different verticals evaluating the business operations from different angles.*

*- Dr. Saurabh Maheshwari*



# THANKS!

**Any questions?**