Course: Software Configuration Management

Week 9: Software Configuration Control

Lecturer: Yimer Amedie (MSc.)
Addis Ababa Science and Technology University, Ethiopia

October, 2025

Contents

Figure 1: Concepts of SCM
(Source: OpenAI, 2025)

- Introduction to configuration control
- The Configuration Control Process
- Baseline Management
- Deviations, Waivers, and Automation
- Integration with Other SCM Functions
- Challenges and best practices
- Summary

Learning Outcomes

After completing this lesson, you will be able to:

- Define configuration control and its role in SCM
- Describe the configuration control process steps
- Explain baseline protection and modification rules
- Understand deviation, waiver, and automation concepts
- Relate configuration control to compliance and auditing

Introduction to Configuration Control

- The formal process for managing changes to baselined Configuration Items (Leon, 2015).
  - Operates after change approval
  - Ensures only authorized modifications
  - Maintains configuration integrity
  - Aligns implementation with approval records
  - Connects governance with technical discipline

Configuration Control (CC)

- How CC different from SCM?
  - **SCM covers**
    - Planning, identification, control, status accounting, and auditing.
  - **Configuration Control focuses mainly on**
    - Managing approved changes after baselines are established.

SCM = the whole system;

Configuration Control = one critical part of it.

Problems of Uncontrolled Change

- Change is inevitable in software projects and if not properly controlled:
  - Loss of configuration integrity
  - Conflicting versions of the same item
  - Missing or outdated documentation
  - Difficulty in reproducing configurations
  - Increased risk during maintenance or release

Why Configuration Control

- **Configuration control is required to:**
  - Prevents divergence from approved design
  - Ensures accountability and traceability
  - Protects baseline integrity
  - Supports compliance and audit
  - Reduces risk of unauthorized changes

Scope of Configuration Control

- Starts after change approval
- Covers all controlled items
- Extends across lifecycle phases
- Interacts with other SCM functions
- Supports software stability

Baselines and Control Mechanism

An agreed-upon, approved version of a CI

- Protect baselines from direct edits
- Archive previous versions
- Establish new baselines through formal steps
- Maintain history for traceability

Configuration Items Governance

- Assign ownership for each CI
- Record all modifications
- Maintain configuration index
- Ensure synchronization among artifacts
- Prevent accidental overwrites

Configuration Control Principles

The principles are

- ✓ Authorization before modification
- ✓ Verification after modification
- ✓ Traceability of every action
- ✓ Reproducibility of configurations
- ✓ Auditability of activities

Control Policies and Enforcement

- Control policies define what can and cannot be changed
  - Assign control rights to authorized personnel
  - Require approval signatures before updates
  - Implement role-based access controls
  - Maintain automated audit trails

Change management and Control Process

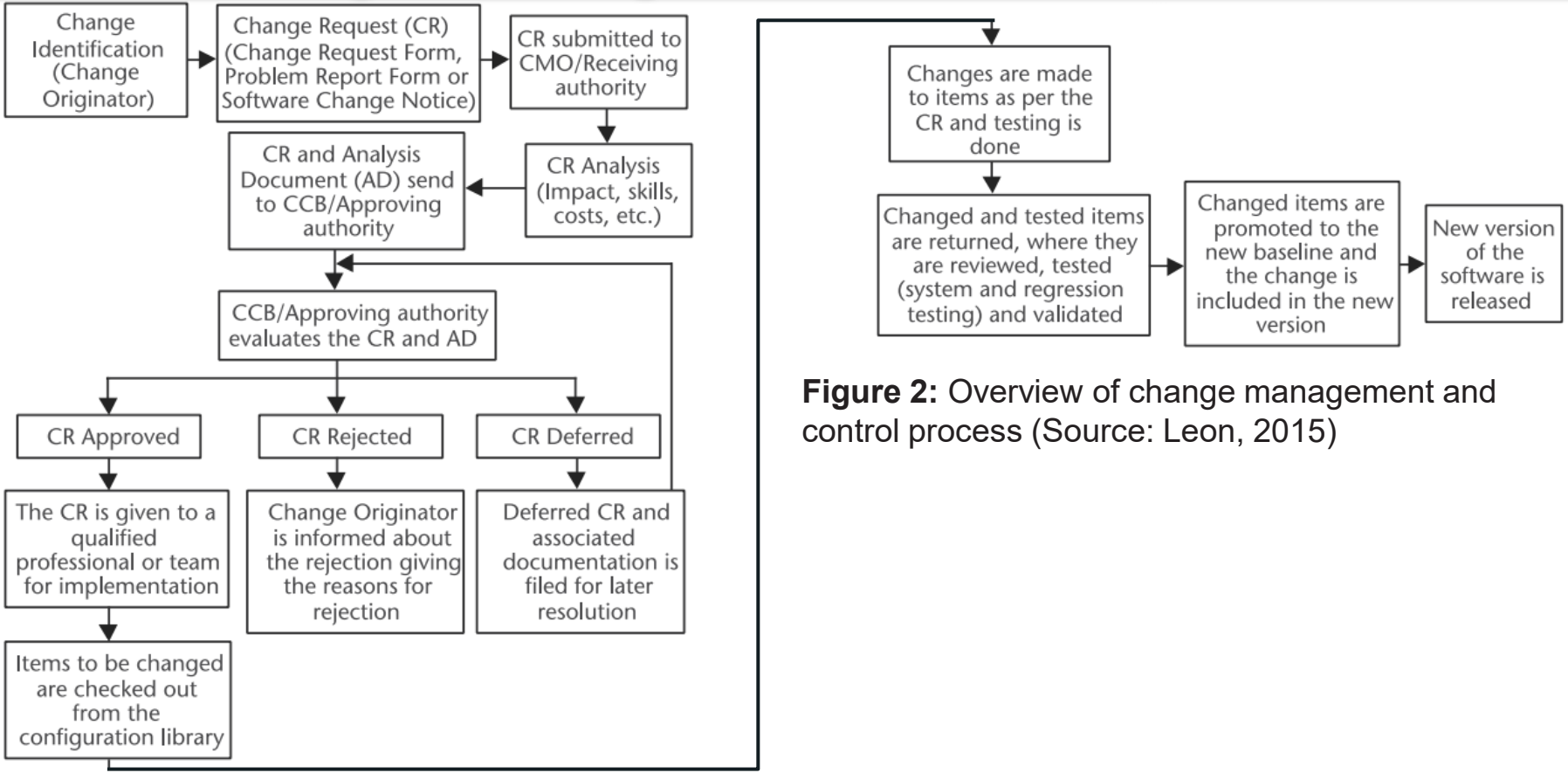
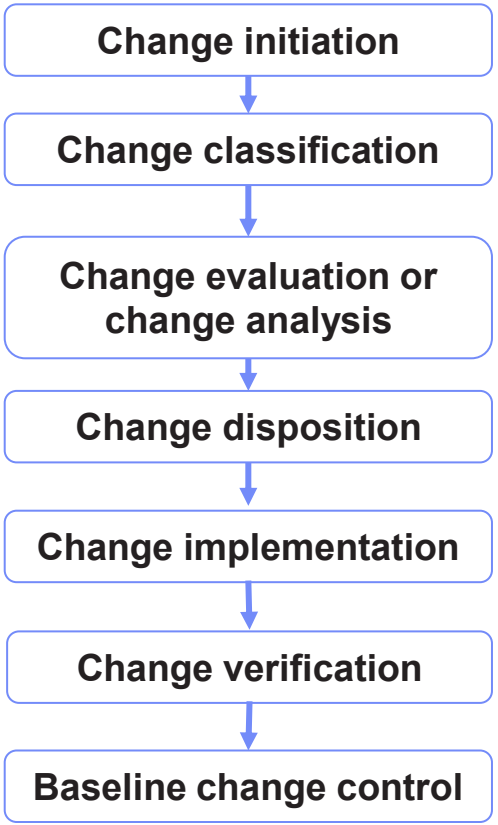


Figure 2: Overview of change management and control process (Source: Leon, 2015)

The Configuration Control Process



- Follows a structured multi-step workflow
- Applies to all baselined configuration items
- Involves multiple roles and authorities
- Emphasizes authorization, documentation, and verification
- Ends with updated baselines and records

Role of the Configuration Control Board

- CCB is a formal authority responsible for configuration decisions.
  - Enforces adherence to control policies
  - Reviews post-approval implementation
  - Validates version consistency
  - Oversees deviation and waiver tracking
  - Authorizes official releases

CCB Decision-Making Process

The responsibilities are:

- Review change requests and evaluation reports
- Approve, reject, or defer proposed changes
- Authorize baseline modifications and releases
- Ensure consistency across all configuration items
- Maintain official change control records

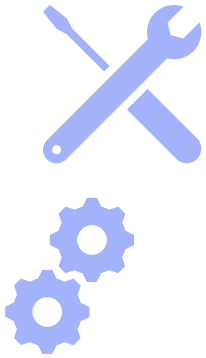
The decision-making process:

- Review documentation before meetings
- Discuss impact and technical feasibility
- Vote or reach consensus on disposition
- Record decisions with rationale
- Communicate outcomes to all stakeholders

Configuration Control Authority

- **The authority and delegation of configuration control is**
  - Defined in organizational SCM policy
  - Managed by SCM or control board
  - Independent from development teams
  - Accountable for compliance and reporting
  - Guided by international standards

Tool for Configuration Control



- Version control systems
- Continuous integration pipelines
- Configuration databases (CMDBs)
- Access management tools
- Audit and reporting utilities

Baseline Change Protection

The baseline Change Protection

- Lock approved baselines
- Use controlled branching
- Maintain historical archives
- Track all modifications
- Ensure audit traceability

Configuration Status Updates

- The status updates:
  - Provide regular status reports
  - Track modification progress
  - Record baseline health metrics
  - Identify open deviations
  - Communicate control findings

Configuration Control Records

- Document approvals and timestamps
- Record revision identifiers
- Maintain deviation and waiver logs
- Store audit outcomes
- Link to test and verification results

Managing Controlled Repositories

- Use strict access permissions
- Follow commit message standards
- Require review before integration
- Maintain backups and recovery plans
- Monitor repository activities regularly

Handling Deviations

Deviation in Configuration Control

- A temporary exception
- Authorized for specific scope and time
- It should be justified with valid reasons
- Document affected items and duration
- Obtain formal authorization before execution
- Close deviation after verification

Handling Waivers

Waiver in Configuration Control

- A permanent exception
- It should provide technical and business justification
- Evaluate associated risks and impacts
- Record approval and documentation changes
- Maintain visibility for future audits

Configuration Integrity Verification

- Verification involves comparison of approved and implemented states:
  - Validate version identifiers and dependencies
  - Detect unauthorized or missing components
  - Confirm alignment with documentation
  - Report verification outcomes to control authority

Auditing in Configuration Control

- During configuration control:
  - ✓ Conduct planned and surprise audits
  - ✓ Review documentation completeness
  - ✓ Verify authorization of changes
  - ✓ Evaluate deviation and waiver records
  - ✓ Recommend process improvements

Configuration Control Reports

The configuration control reports

- Summarize control activities
- Present compliance metrics
- Highlight deviations and waivers
- Include audit findings and corrective actions
- Support management decision-making

Configuration Control Metrics

The metrics for configuration control

- Count of unauthorized change attempts
- Average time to baseline update
- Number of open deviations or waivers
- Audit compliance rate
- Frequency of configuration reviews

Integration with Quality Assurance

Configuration control can be integrated with quality assurance to

- Coordinate QA with control activities
- Verify controlled builds in testing
- Use control data in defect analysis
- Maintain traceability between QA and SCM
- Report inconsistencies for corrective action

Configuration Control and Release Management

During release management, configuration control

- Verify all components before release
- Approve final build for deployment
- Tag and lock release versions
- Maintain rollback configurations
- Conduct post-release audits

Configuration Control Automation

- Automate baseline locking and notifications
- Integrate control with CI/CD pipelines
- Generate automated compliance reports
- Detect and alert policy violations
- Reduce manual intervention and errors

Documentation Standards

- During configuration control:
  - Record every control activity
  - Use standard templates and formats
  - Version-control all documentation
  - Ensure cross-referencing among records
  - Archive documents for audits

Challenges in Configuration Control

- ≠ Unauthorized access or editing
- ≠ Incomplete control documentation
- ≠ Tool integration issues
- ≠ Resistance to procedural discipline
- ≠ Limited automation capabilities

Best Practices for Effective Control

- → Enforce repository access policies
- → Conduct regular configuration audits
- → Automate logging and reporting
- → Integrate SCM tools with QA systems
- → Provide continuous training

Configuration Control Vs Change Management

- **Change Management** ➔ decision-making and evaluation
- **Configuration Control** ➔enforcement and documentation of approved changes
  - Change Management focuses on what to change
  - Configuration Control ensures how the change is applied

Both are complementary within SCM!

Case Example: Configuration Control in OLMS Project

- **Context:**
  - A university is developing a LMS that includes modules for user registration, course management, quizzes, and grade reports.
  - The system is managed under Software Configuration Management (SCM) with strict configuration control policies.

Case Example: Configuration Control in OLMS Project

- **Configuration control actions**
  - LMS baseline established for approved modules
  - New attendance feature approved by CCB
  - Controlled modification through authorized branch
  - Deviation issued for temporary API use
  - Configuration integrity verified before release

Case Example: Configuration Control in OLMS Project

- **Configuration control actions**
  - Waiver approved for minor UI nonconformance
  - Configuration audit conducted post-release
  - Audit confirms closure of deviations and waivers
  - Updated baseline tagged as Release 1.1
  - SCM documentation archived for traceability

Summary

- Software configuration control:
  - Enforces discipline post-approval
  - Maintains baseline and traceability
  - Manages deviations and waivers
  - Uses tools and audits for compliance
  - Ensures long-term quality and stability

References

1. Leon, A. (2015). Software Configuration Management Handbook (3rd ed.). Norwood: Artechhouse. Retrieved September 4, 2025.
2. OpenAI. (2025, September 4). SCM history and concepts [AI-generated image]. ChatGPT (Sora). https://chat.openai.com/

Thank You!

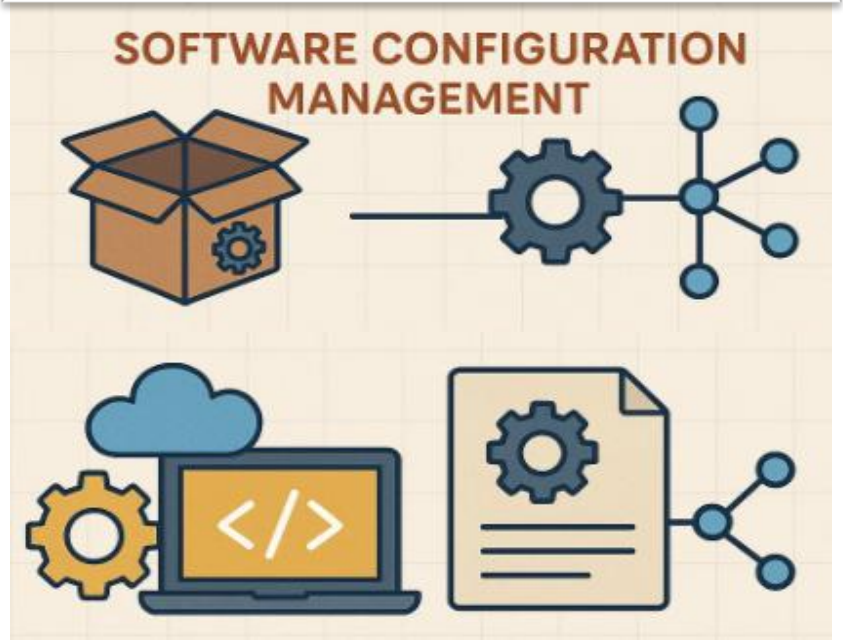


Figure 3: Concepts of SCM (Source: OpenAI, 2025)

NEXT LECTURE

Software Configuration Audit