Configuration verification and audit process
Overview

A variety of things can go wrong with the CM (configuration management) process. Brown et al. [1999] list a set of "antipatterns" — commonly repeated flawed practices:

- Reliance on a software configuration tool to implement an SCM program.
- The CM manager becomes a controlling force beyond his or her planned role. This leads to the CM manager dictating the delivery sequence and dominating all other processes.
- Delegating CM functions to whoever happens to be available. Project managers, often strapped for resources, frequently parcel out the CM function to developers.
– Use of decentralized repositories. The key behind CM is shared information. This requires a shared repository.

– Object-oriented development poses granularity problems. CM must happen at a detailed level of the interaction of a few objects and at a higher level where component interfaces are deployed.
Configuration verification and audit process

• The configuration verification and audit process includes:
  
  – **Configuration verification** of the initial configuration of a CI, and the incorporation of approved engineering changes, to assure that the CI meets its required performance and documented configuration requirements.

  – **Configuration audit** of configuration verification records and physical product to validate that a development program has achieved its performance requirements and configuration documentation.
Inputs to the configuration verification and audit activity

Inputs to the configuration verification and audit activity include:

- Configuration, status, and schedule information from status accounting
- Approved configuration documentation (which is a product of the configuration identification process)
- The results of testing and verification
- The physical hardware CI
- Build instructions and engineering tools, including the software engineering environment, used to develop, produce, test, and verify the product.
• Configuration verification

Is a process that is common to configuration management, systems engineering, design engineering and quality assurance. It is the means by which a developer verifies his or her design solution.

– The functional aspect of configuration verification encompasses all of the test and demonstrations performed to meet the quality assurance.
The tests include:

- Verification/qualification tests performed on a selected unit or units of the CI,
- Repetitive acceptance testing performed on each deliverable CI, or on a sampling from each CIs.

The physical aspect of configuration verification establishes that the as-built configuration conforms to the as-designed configuration.

The developer accomplishes this verification by physical inspection, process control, or a combination of the two.
Configuration audit activity concepts and principles

• Configuration audits

Provide the framework, and the detailed requirements, for verifying that the development effort has successfully achieved all the requirements specified in the configuration baselines.

If there are any problems, it is the auditing activity's responsibility to ensure that all action items are identified, addressed, and closed out before the design activity fulfilled the requirements.
Configuration audit phases

- There are three phases to the audit process, and each is very important.
  - **The pre-audit** part of the process sets the schedule, agenda, facilities, and rules of conduct and identifies the participants for the audit.
  - **The actual audit** itself is the second phase;
  - **The post-audit phase**, in which follow-up of the audit action items must take place.

For complex products, the configuration audit process may be a series of sequential/parallel audits of various CIs conducted over a period of time to verify all relevant elements in the system product structure.
Functional Configuration Audit

The functional configuration audit (FCA) is used to

- Verify that the actual performance of the CI meets the requirements stated in its performance specification
- To certify that the CI has met those requirements. For systems, the FCA is used to verify that the actual performance of the system meets the requirements stated in the system performance specification.

In some cases, especially for very large, complex CIs and systems, the audits can be accomplished in increments.

Each increment can address a specific functional area of the system/CI.
• **Physical Configuration Audit**

The physical configuration audit (PCA) is used to examine the actual configuration of the CI that is representative of the product configuration in order to verify that the related design documentation matches the design of the deliverable CI.

It is used to validate many of the supporting processes that were used in the production of the CI.

To verify that any elements of the CI that were redesigned after the completion of the FCA also meet the requirements of the CI's performance specification.
As discussed, configuration audits address two major concerns:

- The ability of the developed design to meet the specified performance requirements (the FCA addresses this concern)

- The accuracy of the documentation reflecting the production design (the PCA addresses this concern)
Application of Audits During Life Cycle

• It is during the Engineering and Manufacturing Development (EMD) phase that the final, production, operationally ready design is developed.

• Thus, this phase is normally the focus for the auditing activity. A PCA will be performed for each HW CI that has completed the FCA process to "lock down" the detail design by establishing a product baseline.

• Hardware CIs built during this phase are sometimes "pre-production prototypes" and are not necessarily representative of the production hardware. Therefore, it is very common for the PCAs to be delayed until early in the Production phase of the program.
Audit Checklists

• Audit Planning Checklist
  – Global plan and schedule for all FCAs/PCAs expanding on CM PLAN
  – CIs to be audited; specific units to be audited
  – Scope: contract requirements, specification, approved plans
  – Location and dates for each audit
  – Composition of audit team and their functions in the audit
  – Documentation to be audited and reference material
  – Administrative requirements; security requirements