Chapter 1 – Types of Audits

Introduction

Here we are at the start of the Certified Quality Auditor exam day guide and we obviously need to start with one of the most foundational topics!

So, what exactly is an audit?

An audit is a formal, systematic, independent, and documented process of collecting objective evidence to assess the extent to which an organization is in compliance with defined audit criteria.

These criteria could be regulations, international standards, contractual requirements, or internal procedures.

In other words, an audit compares *what is happening* with *what should be happening*.

Auditing is not just a "check-the-box" exercise. It is one of the most effective tools in the quality profession, because it provides insight into whether processes, systems, and products are operating as intended and whether they are delivering value.

Why Do We Audit?

At first glance, it may seem that we audit only because standards such as **ISO 9001** require it.

Indeed, clause 9.2 of ISO 9001 states that organizations "shall conduct internal audits at planned intervals" to ensure their management systems are both conforming and effective.

But the true value of auditing goes much deeper. Auditing is a proven method for both **quality control** and **quality improvement**. By collecting evidence about how systems and processes perform, auditors can uncover problems that exist today, as well as risks that could cause problems in the future.

This allows management to take corrective actions, implement preventive measures, and continuously improve.

Some of the tangible benefits of auditing include:

- Verifying that products and services conform to customer requirements.
- Providing evidence needed for certification or registration (such as ISO 9001 or ISO 13485).
- Driving accountability in suppliers and ensuring supply chain reliability.

- Supplying management with data for decision-making, resource allocation, and risk prioritization.
- Identifying areas for efficiency gains, performance improvement, or cost reduction.

Bottom line: we don't audit just because "the standard says so." We audit because it adds value and strengthens the organization.

ISO 19011 – Guidelines for Auditing Management Systems

Alongside ISO 9001 and other system-specific standards, there is a guidance document every auditor should know: **ISO 19011:2018**.

Unlike ISO 9001, this document does not impose requirements. Instead, it provides practical guidelines on how to plan, conduct, and report audits. It also emphasizes **risk-based thinking**, auditor competence, and the use of audit programs to manage resources effectively.

For CQAs, ISO 19011 is a "go-to reference" for the methodology and principles of auditing.

Types of Audits

Audits can be classified in multiple ways, and it is important to remember that these classifications are not mutually exclusive. For instance, you might perform a **third-party compliance audit** or a **first-party process audit**.

The three most common classification methods are:

1. By the **relationship** of the parties involved.
2. By the **scope** of the audit.
3. By the **purpose** of the audit.

Other ways to distinguish audits include **timing** (planned, surveillance, follow-up), **method** (on-site vs. remote/desk), and **integration** (joint audits across multiple systems).

Audits by Relationship

First-Party Audits (Internal Audits): Conducted by an organization on itself to verify compliance, effectiveness, and readiness. Independence must be preserved by ensuring that auditors do not audit their own work.

Second-Party Audits (Supplier Audits): Conducted by a customer on a supplier. These audits verify that suppliers are capable of meeting requirements, and they are often part of qualification or ongoing evaluation.

Third-Party Audits (Independent Audits): Conducted by registrars, certification bodies, or regulators. These impartial audits may result in certification, accreditation, or regulatory approval, and therefore carry significant weight.

Audits by Scope

System Audits: Broad in scope, covering the entire quality management system (QMS). For example, an ISO 9001 system audit looks across all processes to confirm that the QMS is fully implemented.

This type of audit generally has a large, broad scope.

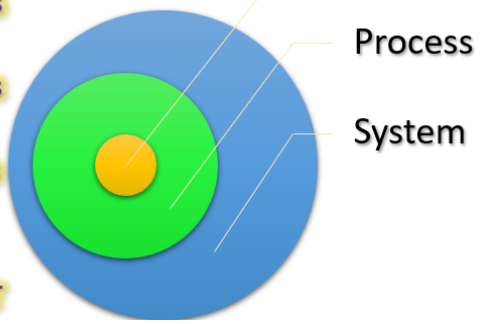
Process Audits: Narrower in focus, examining one or more specific processes. A process audit might evaluate calibration, document control, or complaint handling.

Remember, your quality system is a collection of all of the processes that we use to ensure quality. So a process audit is always a smaller scope than a system audit.

Product Audits: Focused on finished products or services to ensure "fitness for use" (form, fit, and function). Unlike inspections, product audits are performed after release to catch issues missed during production.

A system is a collection of process that each produce a product:

- Material Identification and Traceability
- Handling of Non-conforming Material
- CAPA ----------> CAPA Records
- Supplier Management
- Customer Complaints --------> Complaint Records
- Document Control
- Internal Auditing ----------> Audit Records
- Process Validation
- Process Control and Monitoring
- Production Processes ----------> The PRODUCT



Audits by Purpose

Registration Audits: Conducted by third parties to certify an organization to a standard (e.g., ISO 9001, ISO 13485, IATF 16949).

Supplier Audits: Performed to evaluate, approve, and monitor suppliers, often as second-party audits.

Compliance Audits: Confirm adherence to laws, regulations, contracts, or internal procedures. These may be first-, second-, or third-party.

Performance Audits: Go beyond compliance, focusing on efficiency, effectiveness, and results (e.g., auditing a Lean Six Sigma process for waste reduction).

Follow-Up Audits: Conducted after a previous audit to verify the completion and effectiveness of corrective actions.

Integrated or Joint Audits: Cover multiple management systems (e.g., quality + environmental) or involve multiple parties. These save time and reduce audit fatigue.

Desk Audit (Document Review) - An audit performed "at your desk" of the documents associated with a product, process or system. No interviews or observational activities.

Auditing is more than a compliance exercise — it is a key driver of assurance, accountability, and continual improvement. For Certified Quality Auditors, mastering these principles ensures not only exam success but also professional credibility in the workplace.

Chapter 2 – Purpose and Scope of Audits

In this chapter, we'll explore how the purpose of an audit drives its scope, and how audits serve as an independent assessment of a system's effectiveness, efficiency, and risk control.

Audits are much more than compliance checks—they're diagnostic tools that help organizations understand whether their quality systems are working as intended.

The relationship between Leadership, Business and Audits

Deming once said – If you can't describe what you're doing as a process, you don't know what you're doing!

Every activity within every business can and should be viewed as a process.

From the way material is received, inspected, handled, assembled, manufactured, packaged and shipped.

To our engineering processes such as Designing products, validating processes, calibrating equipment and doing root cause analysis through CAPA.

It should also be understood that our results (good or bad) are a reflection of our processes.

Leaders within organizations are responsible for managing their business processes, and leadership plays a key role in the health of those processes.

That leadership includes making decisions, ensuring compliance, allocating resources, managing risk and solving problems.

Leaders can only be effective in those tasks (managing risk, solving problems, ensuring compliance) if they have clear, unbiased facts and data about their processes.

This is where Audits come in. As auditors we provide leaders with a clear, unbiased evaluation of their processes so that they can manage risks, solve problems and make improvements to those processes!

The Purpose of an Audit

Every audit begins with a purpose—the 'why' behind the activity.

The purpose establishes the intent and expected outcomes of the audit. In many organizations, this purpose is defined by the client (the person or group requesting the audit) and refined by the lead auditor.

Typical audit purposes include:

- Assessing compliance to regulatory or internal requirements
- Verifying system or process effectiveness

• Measuring efficiency and resource utilization
• Identifying risks or potential nonconformities
• Supporting continual improvement and management decisions

In essence, the purpose gives direction and value to the audit. A well-defined purpose ensures the audit adds insight rather than simply generating findings.

Audit Type	Purpose	Example Scope
1st Party Audit	Verify compliance with internal procedures and identify opportunities for improvement	One department, process, or site within the organization
2nd Party Audit	Evaluate a supplier or contractor's ability to meet contract or regulatory requirements	Supplier's quality system, production line, or specific deliverable
3rd Party Audit	Obtain independent certification or registration	Entire quality management system vs. external standard (ISO 9001, ISO 13485)
Supplier Audit	Ensure supplier's processes and systems meet purchasing company's requirements	Supplier facilities, incoming materials, or critical processes
Compliance Audit	Verify adherence to regulations, standards, or policies	Specific regulations (FDA QSR, OSHA, EPA) or clauses in ISO standards
Performance Audit	Assess effectiveness, efficiency, and outcomes of processes	Process performance metrics, resource utilization, achievement of objectives
Registration/ Certification	Gain or maintain formal certification to a standard	Whole organization quality management system against ISO or industry standard
Desk Audit	Review documented evidence without on-site presence	Policies, procedures, records, certifications (submitted electronically)
Follow-Up Audit	Verify corrective actions taken after previous findings	Previously nonconforming process, department, or requirement

How Purpose Influences Scope

Once the purpose is clear, it determines the scope—the 'what, where, and how much' of the audit.

The scope defines the physical locations, departments, timeframes, standards, and processes that will be examined. In ISO 19011 terms, the scope is the 'extent and boundaries' of the audit.

For example, if the purpose is to verify compliance with ISO 13485 in the production area, the scope might include manufacturing, equipment maintenance, and calibration processes—but exclude design control or post-market activities.

In contrast, a broader purpose such as assessing overall system effectiveness would naturally lead to a larger scope that touches multiple departments.

Purpose and scope must always be aligned. A narrow purpose with a broad scope can waste time and resources, while a broad purpose with a narrow scope risks missing important findings.

Audits as Independent Assessments

An essential value of auditing is its independence. Auditors provide an unbiased, fact-based assessment of a system's effectiveness, efficiency, and risk management performance. This independent perspective allows management to make decisions with confidence.

Effectiveness answers the question: Are processes achieving their intended results? Efficiency asks: Are we achieving those results with minimal waste and optimal use of resources?

Audits also serve as an early-warning system for risks. By evaluating how well controls are working, auditors can identify gaps before they become nonconformances or compliance issues.

Risk-Based Thinking in Purpose and Scope Definition

Modern auditing practices, aligned with ISO 19011:2018, emphasize risk-based thinking when defining audit purpose and scope.

This means that auditors and clients should consider the level of risk and the impact of potential failures when deciding what areas to audit and how much evidence to collect.

High-risk processes—those with significant safety, regulatory, or customer impact—deserve more attention and deeper sampling.

Lower-risk processes may require lighter coverage. This approach ensures that audit resources are used effectively and that the audit provides the greatest possible value.

This will be discussed in more detail later on in the course!

Chapter 3 – Criteria to Audit Against

In the previous chapter, we explored how the purpose and scope of an audit set the direction and boundaries for what will be examined.

In this chapter, we take the next step—understanding the 'yardstick' auditors use to measure conformance. This yardstick is known as the **audit criteria**.

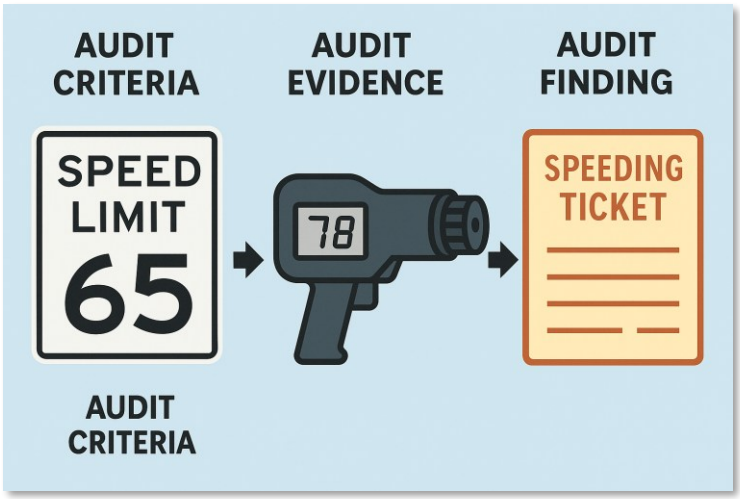
Defining Audit Criteria

Audit criteria are the policies, procedures, or requirements used as a reference against which audit evidence is compared.

They define what **'good'** looks like in measurable, objective terms. According to ISO 19011, audit criteria can include requirements from standards, contracts, or other established documents.

The goal of an audit is not to check personal preferences or opinions, but to **verify conformance** against these defined benchmarks.

Audit Criteria becomes the **reference** against which we compare **audit evidence** and create **audit findings**. The are known as the **Audit Basis**.



Audit criteria can be either documented (such as ISO standards or internal SOPs) or implied (such as cultural or industry expectations for safety, cleanliness, or ethical behavior).

Both are valid when recognized and accepted by the organization or its customers.

Types of Audit Criteria

Audit criteria can be grouped into two broad categories: external and internal. Understanding the difference helps auditors select the right reference for each audit objective.

External Criteria

External criteria are requirements that originate outside the organization. They often represent expectations from customers, regulators, or international bodies. Examples include:

- **National and International Standards**: These include ISO 9001, ISO 13485 (Medical Devices), IATF 16949 (Automotive), and other globally recognized frameworks. These standards define the minimum system requirements for quality management.
- **Regulations and Laws**: Government-issued requirements such as FDA 21 CFR Part 820, EPA regulations, or OSHA standards are mandatory compliance criteria.
- **Contracts**: A contract is an agreement between two parties, typically including the terms and conditions for an exchange of goods. These often specify quality, delivery, or documentation expectations that suppliers must meet.
- **Purchase Order (Purchase Agreement)**: A purchase order is another tool that can be used to dictate an agreement and terms and conditions between two parties. These might include specific requirements (Conformance to ASME Y14.5 or ASME D4169)
- **Customer Specifications**: These may define dimensional tolerances, material requirements, or special inspection criteria.
- **Industry Codes and Guidelines:** Examples include ANSI, ASTM, or SAE standards, which define performance or testing criteria.

Below are a list of some commonly used international / national standards within Auditing:

- ISO 13485 – Quality management for **medical devices**
- IATF 16949 – **Automotive** sector (formerly ISO/TS 16949)
- ISO 27001 – **Information security** management
- AS 9100 – **Aerospace** quality management
- TL 9000 – The **Telecommunication** Industries
- ISO 14001 – **Environmental** Management Systems
- ISO 22000 – **Food Safety** Management

Internal Criteria

Internal criteria are developed within the organization itself and represent how the business intends to operate. These may or may not align perfectly with external criteria, but they must still be followed consistently. Common examples include:

- **Company Policies and Objectives**: High-level statements of intent, such as commitments to quality, safety, or sustainability.
- **Quality Manuals:** These describe the structure of the organization's quality management system and its major elements.
- **Standard Operating Procedures (SOPs**): Step-by-step instructions on how specific processes are performed.
- **Work Instructions and Forms:** Detailed process-level documents that define how to execute tasks, inspect components, or record data.

Audit Criteria versus Performance Standards

We've discussed the concept of a performance audit, and so I wanted to quickly distinguish between our audit criteria and the performance standards that might be included in a performance audit.

	Audit Criteria	Performance Standards
Definition	The policies, procedures, and requirements used as a reference in an audit	The specific expectations for how a process, product, or system should perform
Example	ISO 9001:2015 clause 8.5.1 as the audit criterion for control of production	"95% on-time delivery" as a performance standard for a shipping department
Purpose	To determine conformance during an audit	To set the desired level of performance for operations or processes
Focus	Are we doing what we said we would do? (conformance to documented requirements)	How well are we doing it? (effectiveness or efficiency of performance)
Source	Various (Previous Slide)	Typically, internal and defined by management to support strategic goals
Application in Audits	Used by auditors to guide the evaluation process	May be referenced during audits, especially when assessing effectiveness, but not always a formal part of audit criteria.

Quality Awards and Social Responsibility as Criteria

Beyond compliance and internal controls, some organizations adopt additional frameworks to assess performance and reputation. Two common examples include quality award models and social responsibility standards.

• **Quality Award Models:** Frameworks like the Malcolm Baldrige National Quality Award or EFQM Excellence Model provide holistic criteria for organizational excellence.

• **Social Responsibility Standards:** ISO 26000 and related sustainability frameworks establish ethical, environmental, and community-focused expectations.

While these criteria are voluntary, they're becoming increasingly important as organizations integrate social responsibility into their core business practices.

Selecting the Right Audit Criteria

Choosing the correct audit criteria is one of the most important responsibilities of the audit planner or lead auditor. The criteria must align with the audit's purpose and scope and must be clearly communicated to all parties before the audit begins.

To select the right criteria, auditors should:

- Review the audit purpose to identify relevant requirements.
- Determine whether the audit is compliance-based, performance-based, or both.
- Identify applicable external and internal standards.
- Verify that the auditee is aware of and agrees with the criteria.
- Document the chosen criteria in the audit plan or checklist.

Auditors must avoid introducing personal interpretations or expectations. Findings should always tie back to documented requirements, ensuring objectivity and consistency across audits.

Examples of Audit Criteria in Practice

Here are several examples showing how audit criteria are applied in real-world scenarios:

• **External Compliance Audit:** Auditing a supplier's quality management system against ISO 9001:2015.

• **Product Audit:** Comparing finished medical device packaging to customer specifications and FDA requirements.

•**Process Audit:** Verifying that an assembly process follows approved work instructions and calibration standards.

•**Corporate Responsibility Audit:** Assessing sustainability practices against ISO 26000 and company environmental policies.

Chapter 4 – Roles and Responsibilities

An effective audit relies on the cooperation and competency of several key participants.

Each party involved—**client, lead auditor, audit team members, and auditee**—has unique responsibilities that contribute to the credibility, efficiency, and objectivity of the audit process.

The Client

The client is the individual or organization that requests or sponsors the audit.

They define the purpose, scope, and objectives of the audit and determine the standards or requirements against which performance will be evaluated.

The client also selects or approves the auditing organization and ensures the necessary resources—such as access, personnel, and documentation—are made available.

In addition to commissioning the audit, the client plays a critical role after the audit concludes.

They receive the final audit report, determine which corrective or preventive actions are required, and monitor follow-up activities to ensure issues are resolved.

In regulated industries, the client may also be responsible for reporting results to external authorities or certification bodies.

The Lead Auditor

The lead auditor, often called the audit team leader, is responsible for managing the entire audit from start to finish.

This person acts as the central point of communication between the client, the audit team, and the auditee.

Their duties include developing the audit plan, coordinating the activities of the team, ensuring adequate coverage of the audit scope, and resolving any conflicts or uncertainties that arise during the process.

A strong lead auditor must balance technical expertise with interpersonal skills. They ensure that each audit team member is competent and objective, assign responsibilities based on expertise, and uphold ethical standards throughout the audit.

The lead auditor also facilitates the opening and closing meetings, delivers clear findings, and prepares the final audit report. In accordance with ISO 19011, the lead auditor must ensure that all evidence is verifiable, traceable, and presented accurately.

The Audit Team Members

Audit team members support the lead auditor in collecting, analyzing, and verifying audit evidence.

They are responsible for maintaining objectivity and confidentiality, staying within the defined audit scope, and documenting findings clearly.

Each team member must understand the audit plan, criteria, and objectives, and contribute constructively to discussions and data collection.

Auditors are expected to use professional judgment when interpreting criteria and evidence. They should be skilled in observation, interviewing, and analysis.

When multiple auditors are used, the team must coordinate effectively to ensure consistency and avoid duplication of effort.

The Auditee

The auditee is the organization, department, or process being audited. Their primary responsibility is to cooperate with the auditors and provide access to all relevant personnel, facilities, and documentation.

The auditee should assign a coordinator or guide to accompany the auditors during on-site activities, answer questions, and help the audit team navigate the organization.

After the audit, the auditee reviews the findings, determines appropriate corrective actions, and ensures timely implementation.

The Audit Program and Program Manager

In organizations that manage multiple audits, an **audit program manager** or coordinator oversees the overall **audit program.**

An **audit program** is a **structured plan** that outlines the **scope, objectives, responsibilities**, and procedures for conducting one or more audits within a defined timeframe.

The **program manager role** includes:

- **Selects** and **qualifies auditors**, and **monitors** auditor **performance**
- Determines **audit program schedule**, scope and objectives
- Creates **procedures** and **policies** to **control the audit** program
- **Assigns auditors** to the schedule to ensure objective and **impartial audits**
- Ensures **ethical behavior** from auditors within the program

Communication and Ethics

Effective communication and professional ethics are essential across all audit roles. Auditors must act with integrity, fairness, and respect for confidentiality.

Open, factual communication fosters trust and reduces defensiveness during the audit process.

The lead auditor should ensure that findings are expressed objectively and that both positive observations and opportunities for improvement are discussed.

Team members should also model professionalism—arriving prepared, adhering to schedules, and avoiding arguments or subjective language.

The auditee, in turn, should view the audit as a collaborative opportunity to identify risks and enhance system performance rather than as a punitive inspection.

Example – Coordinated Roles in Action

Imagine a supplier quality audit at a medical device manufacturer.

The client (purchasing organization) defines the audit's purpose—to verify supplier compliance with ISO 13485 and internal quality requirements.

The lead auditor develops an audit plan and assigns specific areas to each team member.

During the audit, the auditee's quality manager provides access to process records and facilitates interviews.

Afterward, the lead auditor compiles findings into a report, and the client determines the necessary follow-up actions.

Each participant contributes uniquely to ensure that the audit is thorough, objective, and value-added.