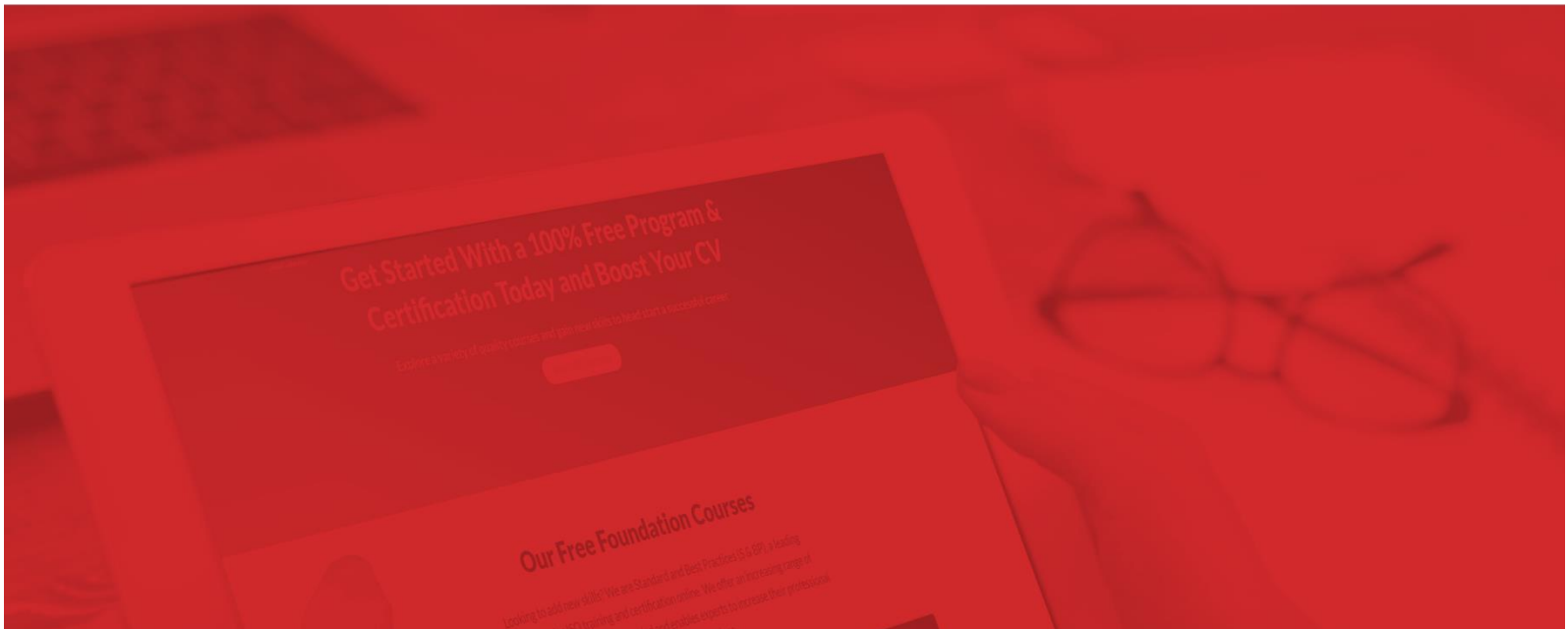
...global validation

SBP ISO 37301:2021 (CMS) LEAD AUDITOR COURSE- CASE STUDIES



CASE STUDY #1

Case Study: Compliance Management System Audit at TechCom Solutions Ltd.

1. Organization Overview

TechCom Solutions Ltd. is a mid-sized multinational IT services provider, headquartered in Germany, with operations in the United Kingdom, Poland, and the United States. The company offers cloud infrastructure services, cybersecurity solutions, and custom software development. With over 1,200 employees and numerous clients in finance, healthcare, and government sectors, the organization faces diverse compliance obligations related to data protection, anti-bribery, export control, and labor laws.

To reinforce its corporate integrity, regulatory adherence, and ethical conduct, TechCom implemented a **Compliance Management System (CMS)** aligned with **ISO 37301:2021 – Compliance Management Systems – Requirements with Guidance for Use**.

2. Background to the Audit

Following the initial implementation of the CMS, TechCom engaged in several internal initiatives:

- Conducted a **comprehensive internal audit**.
- Delivered **compliance training** to all business units.
- Integrated compliance-related performance metrics into their internal dashboards.
- Appointed a **Compliance Officer** with direct access to top management.
- Established an **anonymous whistleblower mechanism**.
- Developed a structured **compliance risk assessment** process.

Now, the company is preparing for a **third-party certification audit** and has engaged a recognized certification body. As a member of the lead audit team, your role is to assess the conformity and effectiveness of the CMS, following the ISO 37301 standard.

3. Audit Objectives

The audit was initiated with clearly defined objectives:

- **Evaluate the CMS** for conformity with ISO 37301 requirements.
- **Assess the effectiveness** of compliance controls in meeting legal, regulatory, and contractual obligations.
- **Verify the implementation** of corrective actions from the most recent internal audit.
- **Examine leadership commitment** and the role of governance in compliance efforts.
- **Evaluate employee awareness** and the operationalization of compliance procedures across different departments.

4. Audit Terms and Definitions in Context

The audit team encountered and applied several audit terms and definitions in practice:

- **Audit criteria**: ISO 37301 standard, internal policies, applicable legal requirements.
- **Audit evidence**: Compliance reports, interview records, training logs, risk assessments.
- **Audit findings**: Conformities, opportunities for improvement, and nonconformities.
- **Nonconformity**: One finding involved incomplete documentation of third-party due diligence.
- **Corrective action**: Implemented in response to a previously identified issue in vendor compliance monitoring.

5. Audit Categories Observed

In this engagement, multiple categories of audits were observed or referenced:

- **First-party audit**: Internal audit conducted by TechCom's own compliance team.
- **Second-party audit**: Supplier audits conducted by TechCom on outsourced data processors.
- **Third-party audit**: Certification audit conducted by your audit team as part of an accredited body.

6. Types of Audit Referenced

The audit encompassed several **types of audits** by focus:

- **Compliance audit**: Focused on adherence to legal and regulatory obligations.
- **Process audit**: Evaluated how well the whistleblower process and compliance training were managed.
- **System audit**: Reviewed the overall CMS framework, from leadership and planning to monitoring and improvement.
- **Risk-based audit**: Targeted areas identified through the compliance risk assessment matrix.

7. Stages of Audit Conducted

The audit followed a structured approach, moving through the typical **stages of an audit**:

1. **Audit Initiation**: Audit plan developed, scope confirmed, auditees notified.
2. **Audit Preparation**: Document review conducted (policies, procedures, risk assessments, training materials).
3. **Audit Execution**: On-site and remote interviews with compliance team, IT, HR, legal, and selected employees.
4. **Audit Reporting**: Draft report shared with TechCom including findings, positive observations, and recommendations.
5. **Follow-up**: Schedule agreed upon for submission of corrective action plans where nonconformities were found.

8. Surveillance Audits

TechCom was in the second year of their certification cycle, making them eligible for their first **surveillance audit** within six months. As part of this audit, the certification body reviewed:

- Progress on implementation of improvement actions.
- Operational compliance in new regional offices added in the past year.
- Continuous monitoring mechanisms and how TechCom uses KPIs to track compliance.

Surveillance audits were explained to the client as mandatory follow-ups to ensure ongoing conformity and effectiveness of the CMS between the initial certification and the final **recertification audit** at the end of the 3-year cycle.

9. Recertification Audit (Future Considerations)

Although not currently in scope, the **recertification audit** was discussed during the closing meeting. It was highlighted that:

- The recertification audit will be more comprehensive.
- All significant changes in business operations or compliance risks over the 3-year period will be reviewed.
- Evidence of continual improvement will be key to successful recertification.
- The organization should maintain records of periodic internal audits, surveillance feedback, and management reviews.

10. Outcome and Key Learnings

The audit team found TechCom's CMS to be **generally conforming** with ISO 37301 requirements, with:

- **Two minor nonconformities** requiring corrective actions.
- **Three opportunities for improvement** related to internal awareness, supplier compliance tracking, and automation of compliance risk metrics.
- **Several positive practices** acknowledged, including top management commitment, use of compliance dashboards, and an inclusive training program.

The audit concluded with a **recommendation for initial certification**, subject to closure of the minor nonconformities within 30 days.

CASE STUDY #2

Case Study: Global Compliance Audit Programme at MediPharm International Ltd.

1. Organization Overview

MediPharm International Ltd. is a global pharmaceutical manufacturing and distribution company, headquartered in Switzerland, with regional offices and production facilities across Europe, Asia, North America, and Africa. With over 15,000 employees, the company must comply with a wide array of legal, regulatory, and ethical obligations related to pharmaceutical development, marketing, and distribution, including data privacy laws, anti-bribery regulations, export controls, and good manufacturing practices (GMP).

To ensure effective compliance oversight across its operations, the Group Compliance Office at MediPharm decided to develop and implement a structured **Compliance Audit Programme** based on **ISO 37301:2021 – Compliance Management Systems**.

2. Initiation of the Audit Programme

The **Global Chief Compliance Officer (GCCO)** initiated a multi-year **Compliance Audit Programme** with the following strategic drivers:

- Increasing regulatory scrutiny in key jurisdictions.
- Integration of newly acquired companies in Asia-Pacific.
- Operational expansion into Latin America.
- Implementation of a centralized compliance monitoring system.
- Board-level focus on ethical culture and legal adherence.

The GCCO appointed an **Audit Programme Manager** to oversee the design, execution, monitoring, and improvement of the compliance audit programme across the organization.

3. Establishing Audit Programme Objectives

The following **audit programme objectives** were established and approved by top management:

- Verify compliance with internal policies, external legal obligations, and ethical standards.
- Assess the maturity and effectiveness of compliance management systems in all subsidiaries.
- Detect and prevent noncompliance before it escalates to legal or reputational risk.
- Promote a culture of compliance and continuous improvement.
- Provide data-driven input to strategic compliance risk management.
- Support integration of acquired entities into MediPharm's compliance framework.

4. Audit Programme Scope and Extent

The Audit Programme Manager defined the **extent of the audit programme**:

- **Geographic scope**: All regions—Europe, North America, Asia-Pacific, Africa, and Latin America.
- **Business units**: Manufacturing, supply chain, R&D, marketing, sales, procurement, and HR.
- **Compliance domains**: Anti-bribery, data privacy, product labelling, regulatory submissions, third-party due diligence.
- **Audit methods**: On-site audits, remote audits, document reviews, and stakeholder interviews.
- **Frequency**: High-risk sites audited annually; medium-risk sites every two years; low-risk sites on a three-year cycle.

5. Audit Duration and Time Allocation

Each audit was planned with a **risk-based duration and time allocation** model:

- **Small regional site**: 2 auditors for 2 days.
- **Medium-sized manufacturing site**: 3 auditors for 3 days.
- **Headquarters and global functions**: 5 auditors for 5 days.
- Time allocated per audit phase:

- Preparation and planning: 15%
- Fieldwork and interviews: 60%
- Documentation review: 15%
- Reporting and follow-up: 10%

6. Audit Programme Risks and Opportunities

The Audit Programme Manager identified and evaluated several **risks and opportunities**:

Risks:

- Unavailability of key compliance staff during audits.
- Language and cultural barriers in local audits.
- Cybersecurity restrictions during remote access reviews.
- Misalignment between regional policies and global CMS.

Opportunities:

- Use of data analytics to detect anomalies in compliance behavior.
- Leveraging technology to perform hybrid audits.
- Training local auditors to reduce travel costs.
- Enhancing stakeholder awareness of compliance obligations.

Mitigation strategies and action plans were developed to address these risks and maximize opportunities.

7. Establishing the Audit Programme

The Audit Programme Manager led the creation of the audit programme using the following steps:

- Defined clear audit scope, frequency, methods, and responsibilities.
- Created a **three-year rolling audit plan** aligned with business risks and compliance priorities.

- Assigned qualified internal auditors and established an external auditor pool for specialized topics.
- Secured audit resources including access to systems, travel budgets, and translation support.
- Coordinated with regional compliance officers to ensure local alignment.

8. Implementation of the Audit Programme

During the **implementation phase**, the following actions were taken:

- Issued a formal audit schedule to all business units.
- Developed standard audit checklists and reporting templates.
- Conducted auditor training on ISO 37301, legal updates, and audit techniques.
- Executed 24 audits in Year 1, including:
    - A bribery prevention audit in Brazil.
    - A data privacy compliance audit in Germany.
    - A marketing and promotion practices audit in India.
- Utilized an audit management system to track findings, corrective actions, and status updates.

9. Monitoring the Audit Programme

The programme's progress was continuously monitored through:

- Monthly reports to the Compliance Committee summarizing completed audits, nonconformities, and corrective actions.
- Use of dashboards to track:
    - Audit schedule adherence.
    - Audit result trends by region and function.
    - Timeliness of corrective action implementation.
- Periodic engagement with regional compliance leaders for performance feedback.

10. Reviewing and Improving the Audit Programme

At the end of Year 1, a **comprehensive programme review** was conducted. The review process included:

- Evaluating feedback from auditees and auditors.
- Comparing actual outcomes against planned objectives.
- Analyzing audit trends, such as recurrence of findings in third-party management.
- Identifying systemic issues such as policy translation gaps and training inconsistencies.

Based on the review:

- The audit plan for Year 2 was updated to increase frequency of audits in high-risk regions.
- Additional training modules were developed for compliance officers.
- Digital compliance monitoring tools were proposed to supplement audit activities.

11. Conclusion

MediPharm's structured and well-managed compliance audit programme allowed it to:

- Proactively identify and address risks.
- Improve global CMS integration and consistency.
- Enhance organizational culture of compliance.
- Support sustainable and ethical business growth.

CASE STUDY #3

Case Study: Evaluating and Enhancing Auditor Competence at VeritasLogix Corporation

1. Organization Overview

VeritasLogix Corporation is a multinational logistics and supply chain company operating across 30 countries with a workforce of 22,000 employees. The company manages sensitive data related to client operations, border controls, customs regulations, and ethical labor practices. Due to regulatory pressure and stakeholder demands, the organization has adopted **ISO 37301:2021** to enhance its **Compliance Management System (CMS)**.

To ensure the effective implementation and oversight of the CMS, VeritasLogix launched an internal **Compliance Audit Function** supported by a team of internal auditors. A strategic focus was placed on building and maintaining a **competent team of auditors** to perform robust audits that ensure both conformity and effectiveness of the CMS.

2. Initial Competency Requirements and Gap Analysis

The **Head of Compliance Audit**, in coordination with HR, initiated a structured process to define and assess auditor competence across regional offices. The following baseline **knowledge and skills requirements** were identified for ISO 37301 auditors:

- Understanding of compliance obligations (laws, regulations, internal policies).
- Familiarity with ISO 37301 and ISO 19011 guidelines.
- Knowledge of risk-based thinking and compliance risk assessment.
- Effective communication, interviewing, and report-writing skills.
- Analytical thinking and objectivity.
- Fluency in local and English languages.

An initial **competency gap analysis** was performed on the existing 18 auditors across global regions. Results revealed:

- 8 auditors lacked knowledge of ISO 37301 requirements.

- 5 auditors had limited experience conducting compliance audits.
- 6 auditors had strong technical knowledge but weak communication and reporting skills.

3. Achieving Auditor Competence

To address identified gaps and ensure auditor capability, the company implemented a **three-phase competency development plan**:

Phase 1: Training

- Mandatory training in ISO 37301:2021, compliance audit techniques, and risk assessment principles.
- Scenario-based workshops and mock audits.
- Legal update sessions relevant to regional operations.

Phase 2: Supervised Audit Participation

- Each junior or partially competent auditor participated in at least three audits under the supervision of a lead auditor.
- Evaluations were conducted using observation checklists focusing on planning, execution, documentation, and communication.

Phase 3: Competence Confirmation

- After observed audits, auditors underwent a knowledge test and an interview with the Compliance Audit Panel to assess readiness for independent audits.

4. Establishing Auditor Evaluation Criteria

To formalize competence assessment, VeritasLogix established standardized **auditor evaluation criteria**, based on:

- Conformity to ISO 19011:2018 guidelines on auditor attributes and behaviors.
- Demonstrated knowledge of ISO 37301, legal context, and compliance controls.
- Consistency in audit planning and execution.
- Ability to write objective, clear, and evidence-based audit reports.

- Feedback from auditees and audit team members.
- Continuous professional development (CPD) activity logs.

These criteria were embedded into the company's HR performance appraisal system for all compliance auditors.

5. Ongoing Evaluation and Monitoring

Auditor competence was monitored through a structured **annual performance evaluation** process, which included:

- A 360-degree feedback loop from audit team leaders, peers, and business unit auditees.
- Review of completed audit reports for technical accuracy, language clarity, and alignment with ISO 37301 principles.
- Assessment of corrective actions initiated based on audit findings.
- Attendance records from compliance seminars, webinars, and workshops.
- Self-assessments and updated CVs submitted annually.

Auditors who did not meet expectations in specific competencies were required to complete additional training or co-audit assignments before continuing independently.

6. Maintaining and Improving Auditor Competence

VeritasLogix took proactive measures to **maintain and improve auditor competence** through:

- Subscription to industry compliance and audit newsletters.
- Enrollment in e-learning platforms offering ISO-based training.
- Regular coaching and mentoring sessions for junior auditors.
- Cross-functional audit exchanges with the cybersecurity and quality audit teams.
- Annual internal auditor conference to share best practices and lessons learned.

A CPD log was required for each auditor, tracking formal training hours, articles read, audit experience, and certifications obtained.

7. Audit Team Rotation and Specialization

To ensure continuous growth and specialization, auditors were encouraged to:

- Rotate among audit domains such as third-party risk, data privacy, anti-bribery, and environmental compliance.
- Pursue professional certifications (e.g., Certified Compliance & Ethics Professional – CCEP).
- Lead specialized audits requiring domain knowledge in trade compliance or labor law.

This rotation and upskilling strategy allowed the audit program to remain dynamic and responsive to emerging compliance risks.

8. Outcomes After 24 Months

Two years into the program:

- 100% of compliance auditors had demonstrated full competence against all evaluation criteria.
- Average audit report quality score (based on internal review) improved by 42%.
- Audit findings became more actionable and risk-prioritized.
- Employee satisfaction with the audit process rose by 30%, based on post-audit surveys.
- Regulatory inquiries saw faster resolution due to improved evidence and documentation from audits.

9. Terms and Definitions Used in the Programme

To support consistency and clarity, the audit function maintained a **glossary of key terms** aligned with ISO 37301 and ISO 19011, including:

- **Compliance obligation**
- **Compliance risk**
- **Competence**
- **Audit criteria**
- **Auditor attributes**

- **Objective evidence**
- **Corrective action**

This glossary was integrated into training materials, audit procedures, and the internal audit management system.