# NCA and SAMA Cybersecurity Compliance Framework Training Course



16 - 20 Nov 2026

Vienna

5800 € (Per Person)

Ref: #CYB9002_89351

## Course Introduction / Overview:

This comprehensive training course provides an in-depth exploration of Saudi Arabia's key cybersecurity regulatory frameworks, specifically the National Cybersecurity Authority (NCA) Essential Cybersecurity Controls (ECC) and the Saudi Central Bank (SAMA) Cybersecurity Framework. In an era of escalating digital threats, achieving and maintaining compliance is not merely a legal obligation but a critical component of organizational resilience and trust. This program is meticulously designed to demystify the complexities of both frameworks, offering participants a clear and actionable roadmap for implementation. As discussed by security expert Ross J. Anderson in his seminal work, "Security Engineering: A Guide to Building Dependable Distributed Systems," the foundation of robust security lies in a principled and systematic approach, a philosophy that underpins our curriculum. BIG BEN Training Center has developed this course to move beyond theoretical understanding, focusing on the practical application of controls, risk management methodologies, and governance structures. Participants will gain the essential skills to navigate the regulatory landscape, conduct gap analyses, and build a sustainable compliance program that protects critical assets and ensures regulatory adherence.

## Target Audience / This training course is suitable for:

- Cybersecurity Managers and Directors.
- Information Security Officers and Analysts.
- IT Auditors and Internal Audit Staff.
- Compliance and Risk Management Professionals.
- IT Governance and Policy Managers.
- Legal and Regulatory Affairs Personnel.
- Consultants specializing in cybersecurity and regulatory compliance.
- IT and Operations Managers with security responsibilities.

## Target Sectors and Industries:

- Financial Services and Banking Sector.
- Government Agencies and Public Sector Entities.
- Telecommunications and Information Technology.
- Energy, Oil, Gas, and Utilities.
- Healthcare and Pharmaceutical Industries.
- Transportation and Logistics.
- Defense and National Security Sectors.
- Large Enterprises and Conglomerates operating in Saudi Arabia.

## Target Organizations Departments:

- Cybersecurity and Information Security.
- Information Technology (IT) and Operations.
- Internal Audit and Assurance.
- Legal and Compliance.
- Risk Management.
- Governance and Corporate Strategy.
- Procurement and Vendor Management.
- Human Resources (for security awareness programs).

## Course Offerings:

By the end of this course, the participants will have able to:

- Interpret the specific requirements and controls of the NCA ECC and SAMA Cybersecurity Framework.
- Develop a strategic roadmap for implementing and integrating both frameworks within their organization.
- Conduct thorough gap analyses to identify areas of non-compliance and prioritize remediation efforts.
- Establish effective cybersecurity governance structures as mandated by Saudi Arabian regulations.
- Master the process of risk assessment, management, and treatment aligned with NCA and SAMA guidelines.
- Design and implement robust security policies, standards, and procedures.
- Prepare for and confidently manage internal and external compliance audits.
- Develop comprehensive incident response and business continuity plans that meet regulatory expectations.
- Manage third-party and cloud security risks in accordance with framework requirements.
- Foster a culture of continuous compliance and cybersecurity improvement.

## Course Methodology:

The training methodology at BIG BEN Training Center is designed to be highly interactive, engaging, and practical, ensuring participants can apply their learning directly to their professional roles. We move beyond traditional lecture-based formats to create a dynamic learning environment. The course heavily utilizes real-world case studies drawn from scenarios within the Saudi Arabian regulatory landscape, allowing participants to analyze challenges and develop solutions for NCA and SAMA compliance. Interactive group discussions and workshops encourage peer-to-peer learning and the sharing of diverse industry perspectives. Practical, hands-on exercises will guide participants through key processes such as conducting a risk assessment, drafting a policy, and creating a compliance evidence portfolio. Our expert instructors facilitate sessions that are rich with practical examples, templates, and best-practice guidance. Continuous feedback is provided throughout the course, culminating in a final session focused on developing a personalized action plan for implementing the frameworks within each participant's organization, ensuring a tangible return on investment.

## Course Agenda (Course Units):

### Unit One: Foundations of Cybersecurity Regulation in Saudi Arabia

- Introduction to the National Cybersecurity Authority (NCA) and its mandate.
- Overview of the Saudi Central Bank (SAMA) and its role in financial sector cybersecurity.
- The legal and regulatory landscape for cybersecurity in the Kingdom.
- Understanding the scope, applicability, and objectives of the NCA ECC and SAMA Framework.
- Key definitions and terminologies used in both frameworks.
- The relationship between the frameworks and other international standards.
- Exploring the core principles of cybersecurity governance and risk management.

### Unit Two: A Deep Dive into the NCA Essential Cybersecurity Controls (ECC)

- Analyzing the five main domains of the NCA ECC.
- Cybersecurity Governance controls and implementation guidance.
- Cybersecurity Defense controls for protecting systems and data.
- Cybersecurity Resilience controls for response and recovery.
- Third-Party and Cloud Computing Cybersecurity controls.
- Industrial Control Systems (ICS) Cybersecurity controls.
- Mapping controls to organizational functions and responsibilities.

### Unit Three: Mastering the SAMA Cybersecurity Framework

- Deconstructing the four main domains of the SAMA Framework.
- Domain 1: Leadership and Governance requirements.
- Domain 2: Risk Management and Compliance processes.
- Domain 3: Operations and Technology controls.
- Domain 4: Third-Party Security considerations.
- Understanding maturity levels and their assessment.
- Specific requirements for financial institutions and FinTech companies.

## Unit Four: Practical Implementation and Integration Strategies

- Conducting a comprehensive gap analysis and readiness assessment.
- Developing a phased implementation roadmap and project plan.
- Strategies for integrating NCA and SAMA requirements into a unified control set.
- Writing effective cybersecurity policies, standards, and procedures.
- Techniques for evidence collection, documentation, and management.
- Implementing a Security Operations Center (SOC) aligned with regulatory needs.
- Change management and stakeholder communication for successful adoption.

## Unit Five: Auditing, Reporting, and Continuous Improvement

- Preparing for internal and external cybersecurity audits.
- Navigating the audit process and managing auditor interactions.
- Developing compliance reports for senior management and regulators.
- Managing and remediating findings of non-compliance.
- Building an effective incident response plan according to NCA and SAMA.
- Establishing metrics and Key Performance Indicators (KPIs) for compliance.
- Strategies for maintaining continuous compliance and ongoing monitoring.

# FAQ:

### Qualifications required for registering to this course?

There are no requirements.

### How long is each daily session, and what is the total number of training hours for the course?

This training course spans five days, with daily sessions ranging between 4 to 5 hours, including breaks and interactive activities, bringing the total duration to 20 - 25 training hours.

## Something to think about:

## What unique qualities does this course offer compared to other courses?

Beyond mere compliance, how can organizations leverage the NCA and SAMA frameworks as strategic enablers for business growth and digital trust in the Saudi Arabian market?

## What unique qualities does this course offer compared to other courses?

This course distinguishes itself by offering a unified and holistic perspective on both the NCA and SAMA frameworks, a crucial feature often missing in programs that focus on only one regulation. Rather than presenting the frameworks as separate, siloed requirements, our curriculum emphasizes an integrated compliance strategy, enabling organizations to build a single, efficient control environment that satisfies multiple regulatory bodies. The core focus is on practical, actionable implementation, moving participants beyond theoretical knowledge to the tangible skills required to build, manage, and sustain a compliance program. We utilize case studies and scenarios that are specifically contextualized for the Saudi Arabian market, addressing the unique challenges and opportunities within the region. The academic rigor of the course is grounded in real-world applicability, teaching participants not just what the controls are, but how to interpret, implement, and audit them effectively. It fosters a strategic mindset, encouraging professionals to view compliance not as a cost center, but as a strategic differentiator that enhances organizational resilience, builds customer trust, and supports secure digital transformation in alignment with Vision 2030.