

AUDITING AND GOVERNANCE RISK AND COMPLIANCE | COURSE BROCHURE

Cyber GRC: Governance, Risk, and Compliance for Cybersecurity

5 days | Classroom training | English

SMART HORIZON

info@smarthorizon.uk
2 Kingdom Street, Paddington
London W2 6BD, United Kingdom

Explore current programmes

https://smarthorizon.uk



Course content

Why attend

This course provides a comprehensive understanding of Cyber Governance, Risk, and Compliance (GRC) frameworks, focusing on their application in cybersecurity. Participants will develop practical skills to assess risks, implement governance structures, and ensure compliance with relevant regulations and standards.

Cybersecurity professionals face increasing pressure to manage risks and ensure compliance with various regulations. This course addresses the complexities of integrating governance, risk management, and compliance into cybersecurity strategies, which are critical for protecting organisational assets and maintaining stakeholder trust. Participants will learn to navigate the evolving regulatory landscape, understand the implications of non-compliance, and develop frameworks that align with organisational objectives. By mastering these principles, they will be better equipped to safeguard sensitive information, enhance their organisation's resilience against cyber threats, and effectively communicate GRC strategies to stakeholders across the organisation.
Participants will engage in practical exercises that simulate real-world scenarios, enabling them to develop actionable strategies for identifying and mitigating risks. This hands-on approach will cover essential tasks such as conducting risk assessments, designing governance structures, and evaluating compliance requirements. By practising these capabilities, attendees will enhance their decision-making skills and contribute effectively to their organisation's cybersecurity posture. The course will also emphasise the importance of stakeholder communication and collaboration, ensuring that participants can effectively advocate for Cyber GRC initiatives within their organisations. Ultimately, this course prepares professionals to implement robust GRC frameworks that support long-term cybersecurity objectives.

Professional Problems This Course Is Designed to Solve

- Difficulty translating subject knowledge into practical workplace decisions.
- Inconsistent approaches to the activities covered in the course outline.
- Lack of a structured plan for applying and reviewing new skills.

Course methodology

The course employs a blend of case studies, interactive workshops, and simulations to deepen understanding of Cyber GRC principles. Participants will analyse real-world scenarios, engage in group discussions, and complete practical exercises that require them to apply GRC frameworks. Specific exercises will include developing risk assessment matrices, creating compliance checklists, and designing governance frameworks. Outputs include risk assessment reports, compliance documentation, and governance structure proposals, providing tangible evidence of learning and practical skills that can be directly applied in the workplace. This methodology ensures that participants not only learn theoretical concepts but also gain hands-on experience in implementing Cyber GRC practices effectively.



Course content

Course objectives

By the end of this course, participants will be able to:
• Analyse key Cyber GRC frameworks and their relevance to organisational cybersecurity.
• Assess organisational risks using established methodologies and tools to inform decision-making.
• Design a governance structure that aligns with Cyber GRC best practices and organisational needs.
• Evaluate compliance requirements based on relevant regulations and standards to ensure adherence.
• Prioritise risks to develop effective mitigation strategies that protect organisational assets.
• Construct a Cyber GRC implementation plan tailored to organisational needs and regulatory requirements.

Target audience

This course is suitable for:
• Cybersecurity Managers responsible for risk management and compliance oversight.
• IT Auditors tasked with evaluating cybersecurity controls and governance frameworks.
• Compliance Officers ensuring adherence to regulatory requirements in cybersecurity.
• Risk Analysts focused on identifying and mitigating cybersecurity risks.

Target competencies

Participants will develop competencies in:
• Evaluate and apply Cyber GRC frameworks effectively in organisational contexts.
• Conduct thorough risk assessments in cybersecurity scenarios to identify vulnerabilities.
• Develop governance structures that support cybersecurity initiatives and compliance.
• Implement compliance measures aligned with industry standards and regulations.
• Prioritise and manage cybersecurity risks strategically to enhance resilience.
• Create actionable Cyber GRC plans for organisational implementation and monitoring.

Course outline

Day 1: Introduction to Cyber GRC Frameworks

Applied activity: Participants will analyse a case study of a company facing compliance issues. They will identify the GRC frameworks applicable to the case and discuss their relevance, considering the company's specific context and challenges, including stakeholder impacts and potential risks.
Output: A summary report outlining the identified frameworks and their implications for the case study, including recommendations for improvement.

09:00–09:54	Overview of Cyber GRC concepts and their importance in cybersecurity management.



Course content

09:54–10:48	Key frameworks: NIST, ISO 27001, and COBIT and their applications in practice.
10:48–11:00	Roles and responsibilities in Cyber GRC within organisations and their impact on security.
11:00–11:30	**Coffee break**
11:30–12:12	Roles and responsibilities in Cyber GRC within organisations and their impact on security. (continued)
12:12–13:06	Understanding the regulatory landscape affecting cybersecurity practices and compliance.
13:06–14:00	Introduction to risk management principles and their relevance to GRC in cybersecurity.

Day 2: Risk Assessment Methodologies

Applied activity: In groups, participants will conduct a risk assessment on a fictional organisation, identifying potential threats and vulnerabilities, categorising risks, and proposing mitigation strategies based on their findings, while considering organisational priorities and resource constraints.
Output: A detailed risk assessment report including identified risks, prioritisation, and proposed mitigation strategies.

09:00–09:54	Identifying and categorising cybersecurity risks using industry-standard techniques and tools.
09:54–10:48	Quantitative vs qualitative risk assessment techniques and their applications in practice.
10:48–11:00	Utilising tools for risk assessment: FAIR, OCTAVE, and others for effective analysis.
11:00–11:30	**Coffee break**
11:30–12:12	Utilising tools for risk assessment: FAIR, OCTAVE, and others for effective analysis. (continued)
12:12–13:06	Developing risk assessment matrices and heat maps for visualisation of risk levels.
13:06–14:00	Communicating risk assessment results effectively to stakeholders and decision-makers.

Day 3: Governance Structures for Cyber GRC

Applied activity: Participants will create a governance structure for a fictional organisation, defining roles, responsibilities, and reporting lines, while ensuring alignment with Cyber GRC best practices and organisational goals, and addressing potential challenges in implementation.
Output: A governance framework document outlining the proposed structure, roles, and responsibilities.

09:00–09:54	Designing effective governance frameworks for cybersecurity initiatives and compliance.
09:54–10:48	Roles of cybersecurity committees and boards in governance and oversight.
10:48–11:00	Integrating Cyber GRC into organisational culture and practices for sustainability.



Course content

11:00–11:30	**Coffee break**
11:30–12:12	Integrating Cyber GRC into organisational culture and practices for sustainability. (continued)
12:12–13:06	Best practices for governance documentation and policy development in cybersecurity.
13:06–14:00	Measuring governance effectiveness in cybersecurity through metrics and KPIs.

Day 4: Compliance and Regulatory Requirements

Applied activity: Participants will review a compliance scenario involving a data breach and assess the organisation's adherence to relevant regulations, proposing corrective actions and improvements to prevent future breaches while considering stakeholder communication.
Output: A compliance assessment report with recommendations for improvement and a plan for corrective actions.

09:00–09:54	Understanding key cybersecurity regulations: GDPR, HIPAA, PCI-DSS and their implications for organisations.
09:54–10:48	Conducting compliance assessments and audits to evaluate adherence to regulations.
10:48–11:00	Developing compliance checklists and documentation for organisational policies and procedures.
11:00–11:30	**Coffee break**
11:30–12:12	Developing compliance checklists and documentation for organisational policies and procedures. (continued)
12:12–13:06	Aligning organisational policies with regulatory requirements and best practices for compliance.
13:06–14:00	Strategies for maintaining ongoing compliance and preparing for audits effectively.

Day 5: Integrated Cyber GRC Implementation

Applied activity: In teams, participants will develop a full Cyber GRC implementation plan for a fictional organisation, integrating governance, risk, and compliance strategies, and preparing for potential audits and evaluations while addressing resource allocation and stakeholder engagement.
Output: A comprehensive Cyber GRC implementation plan document that outlines strategies, roles, and metrics for success.

09:00–09:54	Developing a comprehensive Cyber GRC implementation plan for organisations based on best practices.
09:54–10:48	Aligning governance, risk, and compliance efforts to enhance overall cybersecurity posture.
10:48–11:00	Utilising metrics and KPIs to measure GRC effectiveness and inform strategic decisions.



Course content

11:00–11:30	**Coffee break**
11:30–12:12	Utilising metrics and KPIs to measure GRC effectiveness and inform strategic decisions. (continued)
12:12–13:06	Creating a communication strategy for stakeholders to promote GRC initiatives and ensure buy-in.
13:06–14:00	Preparing for audits and continuous improvement in Cyber GRC practices and policies.

The timings provided are estimates and may vary depending on the number of participants and the discussions taking place during the sessions. They are indicative only and do not constitute a binding commitment.

Dates, venues and fees

Current published course plans. Fees are per participant in GBP, excluding unconfirmed taxes.

Venue	Start date	End date	Fee (GBP)
Dubai Confirmed dates	9 Nov 2026	13 Nov 2026	**£3,150.-**
Online Confirmed dates	9 Nov 2026	13 Nov 2026	**£1,250.-**
Frankfurt Confirmed dates	23 Nov 2026	27 Nov 2026	**£2,650.-**
Online Confirmed dates	23 Nov 2026	27 Nov 2026	**£1,250.-**
Kuala Lumpur Confirmed dates	7 Dec 2026	11 Dec 2026	**£1,450.-**
Online Confirmed dates	7 Dec 2026	11 Dec 2026	**£1,250.-**



Course content

Dates, venues and fees (continued)

Venue	Start date	End date	Fee (GBP)
Paris Confirmed dates	14 Dec 2026	18 Dec 2026	**£2,860.–**
Online Confirmed dates	14 Dec 2026	18 Dec 2026	**£1,250.–**
Cape Town Confirmed dates	4 Jan 2027	8 Jan 2027	**£1,890.–**
Online Confirmed dates	4 Jan 2027	8 Jan 2027	**£1,250.–**
Istanbul Confirmed dates	11 Jan 2027	15 Jan 2027	**£2,650.–**
Online Confirmed dates	11 Jan 2027	15 Jan 2027	**£1,250.–**
Amsterdam Confirmed dates	25 Jan 2027	29 Jan 2027	**£2,540.–**
Online Confirmed dates	25 Jan 2027	29 Jan 2027	**£1,250.–**
Singapore Confirmed dates	8 Feb 2027	12 Feb 2027	**£2,820.–**



Course content

Dates, venues and fees (continued)

Venue	Start date	End date	Fee (GBP)
Online Confirmed dates	8 Feb 2027	12 Feb 2027	**£1,250.–**
London Confirmed dates	22 Feb 2027	26 Feb 2027	**£2,450.–**
Online Confirmed dates	22 Feb 2027	26 Feb 2027	**£1,250.–**
Dubai Confirmed dates	8 Mar 2027	12 Mar 2027	**£3,150.–**
Online Confirmed dates	8 Mar 2027	12 Mar 2027	**£1,250.–**
Rome Confirmed dates	15 Mar 2027	19 Mar 2027	**£2,450.–**
Online Confirmed dates	15 Mar 2027	19 Mar 2027	**£1,250.–**
Frankfurt Confirmed dates	22 Mar 2027	26 Mar 2027	**£2,650.–**
Online Confirmed dates	22 Mar 2027	26 Mar 2027	**£1,250.–**



Course content

Dates, venues and fees (continued)

Venue	Start date	End date	Fee (GBP)
Kuala Lumpur Confirmed dates	12 Apr 2027	16 Apr 2027	**£1,450.-**
Online Confirmed dates	12 Apr 2027	16 Apr 2027	**£1,250.-**
Paris Confirmed dates	26 Apr 2027	30 Apr 2027	**£2,860.-**
Online Confirmed dates	26 Apr 2027	30 Apr 2027	**£1,250.-**
Barcelona Confirmed dates	3 May 2027	7 May 2027	**£2,840.-**
Online Confirmed dates	3 May 2027	7 May 2027	**£1,250.-**
Istanbul Confirmed dates	10 May 2027	14 May 2027	**£2,650.-**
Online Confirmed dates	10 May 2027	14 May 2027	**£1,250.-**
Amsterdam Confirmed dates	24 May 2027	28 May 2027	**£2,540.-**



Course content

Dates, venues and fees (continued)

Venue	Start date	End date	Fee (GBP)
Online Confirmed dates	24 May 2027	28 May 2027	**£1,250.–**
Singapore Confirmed dates	14 Jun 2027	18 Jun 2027	**£2,820.–**
Online Confirmed dates	14 Jun 2027	18 Jun 2027	**£1,250.–**
London Confirmed dates	21 Jun 2027	25 Jun 2027	**£2,450.–**
Online Confirmed dates	21 Jun 2027	25 Jun 2027	**£1,250.–**
Rome Confirmed dates	5 Jul 2027	9 Jul 2027	**£2,450.–**
Online Confirmed dates	5 Jul 2027	9 Jul 2027	**£1,250.–**
Dubai Confirmed dates	12 Jul 2027	16 Jul 2027	**£3,150.–**
Online Confirmed dates	12 Jul 2027	16 Jul 2027	**£1,250.–**



Course content

Dates, venues and fees (continued)

Venue	Start date	End date	Fee (GBP)
Frankfurt Confirmed dates	26 Jul 2027	30 Jul 2027	**£2,650.-**
Online Confirmed dates	26 Jul 2027	30 Jul 2027	**£1,250.-**
Kuala Lumpur Confirmed dates	9 Aug 2027	13 Aug 2027	**£1,450.-**
Online Confirmed dates	9 Aug 2027	13 Aug 2027	**£1,250.-**
Paris Confirmed dates	23 Aug 2027	27 Aug 2027	**£2,860.-**
Online Confirmed dates	23 Aug 2027	27 Aug 2027	**£1,250.-**
Vienna Confirmed dates	6 Sept 2027	10 Sept 2027	**£2,940.-**
Online Confirmed dates	6 Sept 2027	10 Sept 2027	**£1,250.-**
Istanbul Confirmed dates	13 Sept 2027	17 Sept 2027	**£2,650.-**



Course content

Dates, venues and fees (continued)

Venue	Start date	End date	Fee (GBP)
Online Confirmed dates	13 Sept 2027	17 Sept 2027	**£1,250.–**
Amsterdam Confirmed dates	20 Sept 2027	24 Sept 2027	**£2,540.–**
Online Confirmed dates	20 Sept 2027	24 Sept 2027	**£1,250.–**
Singapore Confirmed dates	11 Oct 2027	15 Oct 2027	**£2,820.–**
Online Confirmed dates	11 Oct 2027	15 Oct 2027	**£1,250.–**
London Confirmed dates	25 Oct 2027	29 Oct 2027	**£2,450.–**
Online Confirmed dates	25 Oct 2027	29 Oct 2027	**£1,250.–**
Cape Town Confirmed dates	1 Nov 2027	5 Nov 2027	**£1,890.–**
Online Confirmed dates	1 Nov 2027	5 Nov 2027	**£1,250.–**



Course content

Dates, venues and fees (continued)

Venue	Start date	End date	Fee (GBP)
Dubai Confirmed dates	8 Nov 2027	12 Nov 2027	**£3,150.–**
Online Confirmed dates	8 Nov 2027	12 Nov 2027	**£1,250.–**
Frankfurt Confirmed dates	22 Nov 2027	26 Nov 2027	**£2,650.–**
Online Confirmed dates	22 Nov 2027	26 Nov 2027	**£1,250.–**
Kuala Lumpur Confirmed dates	6 Dec 2027	10 Dec 2027	**£1,450.–**
Online Confirmed dates	6 Dec 2027	10 Dec 2027	**£1,250.–**
Paris Confirmed dates	13 Dec 2027	17 Dec 2027	**£2,860.–**
Online Confirmed dates	13 Dec 2027	17 Dec 2027	**£1,250.–**



Course content

Plan your next step

Dates, availability, exact venue, taxes, inclusions and payment terms require written confirmation. This brochure is not a quotation, registration, booking confirmation or visa invitation. Participants receive a Smart Horizon UK certificate of attendance; programmes are not externally accredited and do not award a professional qualification or designation. Confirm arrangements before booking travel.

For group or in-house training, contact our learning team to discuss your objectives and delivery arrangements.

Contact Smart Horizon

info@smarthorizon.uk
2 Kingdom Street, Paddington
London W2 6BD, United Kingdom

View the latest course details online