CYBERSECURITY
NON-TECHNICAL (GRC)
CURRICULUM

CYBERSECURITY PROFESSIONAL NON-TECHNICAL (GRC)

Who is it for

Candidates with non-technical backgrounds who are interested in learning about the non-technical aspects of Cybersecurity (Technology Governance Risk and Compliance)
No previous knowledge or experience with projects is required.

Who is it for

Learning Outcome for Cybersecurity Professional Program - Technical

By the end of this course, you will be able to function in any of these Entry Level roles:

- Cybersecurity Governance Risk and Compliance Analyst
- Data Protection and Privacy Officer
- IT Auditor
- Information Security Analyst
- IT Risk Management Officer

MONTH 1: Introduction to Technology Governance, Risk, and Compliance

1. Overview of technology GRC

2. Importance and benefits of effective technology governance

3. Key concepts and terminology

4. Types and sources of technology risks

5. Risk assessment methodologies

6. Risk mitigation strategies and controls

7. Cybersecurity principles and best practices

MONTH 2: Regulatory Environment and Compliance

1. Understanding technology-related regulations and standards

2. Compliance frameworks and frameworks (e.g., GDPR, PCI, DSS, ISO27001)

3. Compliance monitoring and reporting

4. Auditing and assurance in technology GRC

MONTH 3: Technology Governance Frameworks

1. Establishing technology governance structures

2. Roles and Responsibilities in technology governance

3. Developing technology policies and procedures

4. Performance measurement and reporting

MONTH 4: Incident Response and Business Continuity

1. Incident response planning and execution

2. Business continuity management for technology disruptions

3. Crisis management and communication strategies

MONTH 5: Ethical and Legal Considerations

1. Ethical issues in technology governance

2. Intellectual property and data protection

3. Privacy and data security regulations

MONTH 6: Emerging Trends and Challenges in Technology GRC

1. Cloud computing and its impact on technology governance

2. Artificial intelligence and machine learning governance

3. Internet of Things (IoT) and connected devices in technology risk management

4. Big data governance and compliance challenges

THE CYBERSECURITY PROGRAM OVERVIEW

- 100% Online Learning

- Hands-on Practical sessions With Videos, Exercises and Projects

- Lifetime Access to Materials

- 24 Classes and 60 Hours

- 100,000 USD Average Salary of Cybersecurity Professional

- Add projects to your portfolio

- 100% Job prospect visibility

- Industry Relevant Certifications

- Cybersecurity Exams Coaching

- 6 Months Intensive Training with Internship Opportunities

- Access to our Global Network of Technical Recruiters

BONUS CAREER COACHING SERVICES

1. How to have a successful and amazing career in Cybersecurity

2. Tech Visa Coaching for Nigerian Cybersecurity Professionals to relocate and work in the UK, US, Canada, and other western countries.

3. Freelancing opportunities for Cybersecurity Consultants

4. CV Revamp and Linkedin Optimisation

5. Interview Prep and Coaching

6. How to get Remote Job Roles as a Cybersecurity Professional

7. Projects and Portfolio Building

8. How to gain Work Experience and Internships as a Cybersecurity Professional

9. Access to our Alumni Network of Students

10. Access to our Global Network of Technical Recruiters

THE PROGRAM

MODE: Online

PLATFORM: Zoom, whatsapp support group and google drive

TOTAL DURATION OF PROGRAM: 6 Months (PROJECT BASED LEARNING)

DAYS OF CLASSES: Saturday

TIME OF CLASSES: 6:00PM to 8:30PM

Classes are live and access to replay of live classes is available.

THE PROGRAM FEE

50,000 Naira
(PROMO PRICE BASED ON OUTRIGHT PAYMENT)
NORMAL PRICE:
100,000 Naira

Bank Account To Pay Into :
5410623379
THE HAGITAL CONSULTING
Providus Bank

THANK YOU FOR CHOOSING US

OFFICE ADDRESS
4A Akinwale Street Opposite nationwide filling station off Yaya Abatan Ogba,Lagos