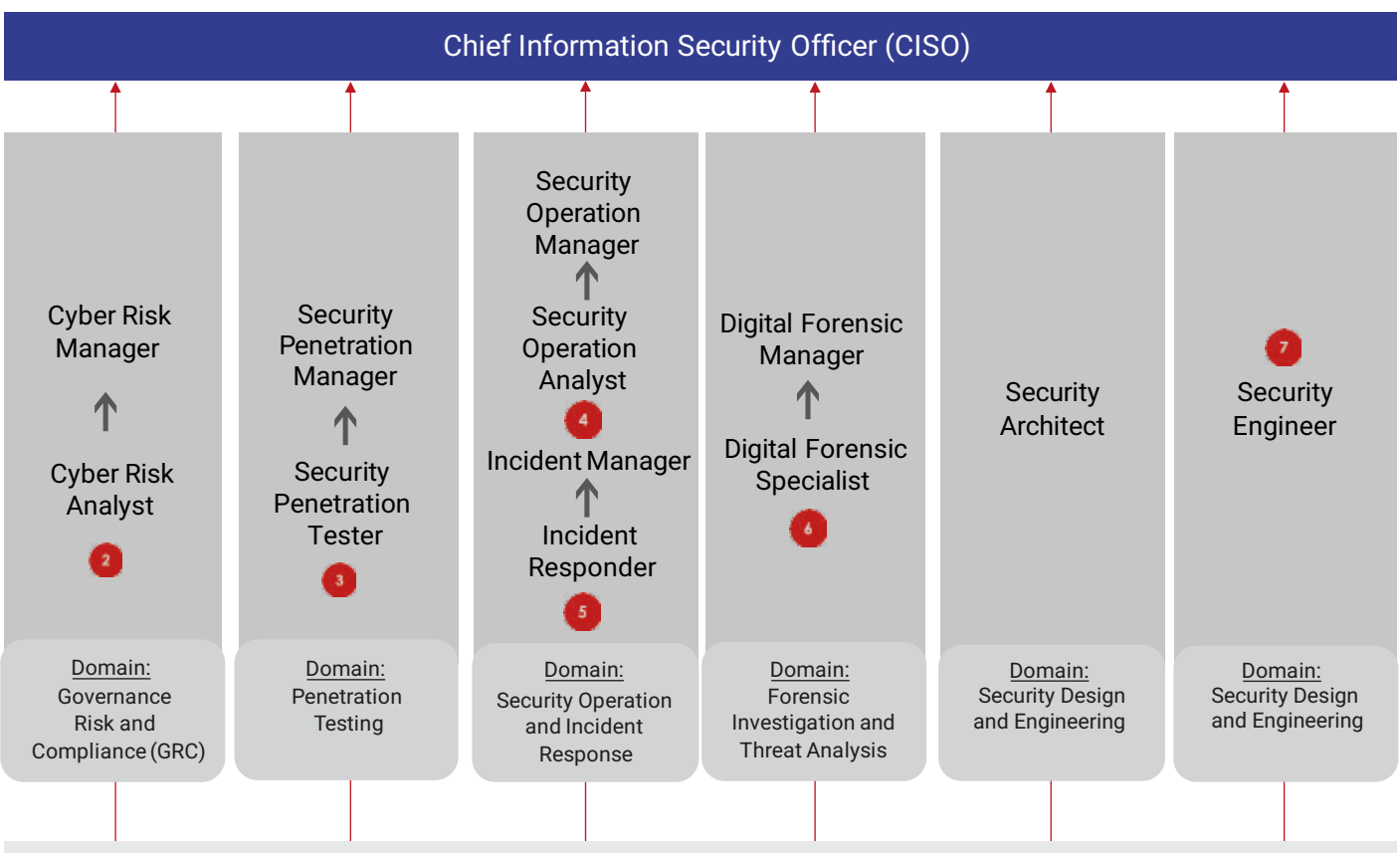
CYBERSECURITY



SECURITY EXECUTIVE/ ASSOCIATE SECURITY ANALYST

Job Description

- Supports security systems and operations administration, monitoring and maintenance
- Monitors security alerts and events
- Collects and documents contextual information based on established practices and supports the preparation and publishing of security advisories
- Assists with the analysis of security-related information and events, escalation of incidents for validation and remediation
- Required to be on standby with on-call availability with varied shifts including nights, weekends and holidays

Competencies

- Cyber Incident Management & Problem Management
- Cyber Forensics
- Infrastructure Support
- Security Administration
- Security Assessment & Testing
- Security Education & Awareness
- Project Management
- Threat Intelligence & Detection

Common Certifications*

- ISACA CSX Fundamental Certificate (For Beginner)
- CompTIA A+ (For Beginner)
- EC-Council Certified Network Defender (CND) (For Beginner)
- Cisco Certified Entry Networking Technician (CCENT) (For Beginner)
- GIAC Security Essentials Certification (GSEC) (Level 1)
- Cisco Certified Network Professional Security (CCNP Security)
- CompTIA Security+
- Rocheston Certifications
- EC-Council Certified Ethical Hacker (CEH)
- (ISC)² Systems Security Certified Practitioner (SSCP)
- EC-Council Certified Incident Handler (E|CIH)
- ITIL V4 Foundation for IT Service Management
- ISO/IEC 27001:2013 Information Security Management System Requirements

Career Pathway

Chief Information Security Officer (CISO)

↑

Branch into any 6 specific Cybersecurity domain

↑

Security Executive / Associate Security Analyst

Essential / Core Skills

- Linux
- Active Directory
- Firewalls
- Network Security
- Windows Server
- Security Information and Event Management (SIEM)

Commonly Used Tools / New Technologies

- Splunk
- Python
- Wireshark
- Vulnerability scanner

Soft Skills

- Communication
- Creative Thinking
- Problem Solving
- Sense Making
- Teamwork
- Stakeholder Management

***This list is not exhaustive and serves only as a guide**

	SFIA Level[1]	NOSS[2]
Chief Information Security Officer (CISO)	5	
Security Executive/Assoc Security Analyst	3	

[1] SFIA Level:
SFIA stands for Skills Framework for the Information Age. It is a model for describing and managing skills and competencies for professionals working in the field of Information and Communication Technologies (ICT), software engineering and digital transformation. Published in 2000 by the British Computer Society (BCS).

[2] NOSS:
The acronym NOSS stands for National Occupational Skills Standards. NOSS is a document that outlines the dexterity required of an employee working in Malaysia at a certain level of employment to achieve specific skills.

PEMBANGUNAN SUMBER MANUSIA BERHAD
Wisma HRDF, Jalan Beringin, Damansara Heights
50490 Kuala Lumpur

Email: support@hrdf.com.my **Tel: 1800-88-4800**

CONNECT WITH

CYBER RISK ANALYST

Job Description

- Conducts independent comprehensive assessments of the management, operational, and technical security controls and control enhancements employed within or inherited by an information technology (IT) system to determine the overall effectiveness of the controls and ensure an acceptable level of risk to organisational operations (including mission, functions, image, or reputation), organisational assets and individuals based on enterprise needs.

Competencies

- Audit & Compliance
- Business Needs Analysis
- Cyber Incident Management
- Cyber Risk Management
- Security Governance
- Security Program Management
- Security Strategy
- Cyber Crisis Management
- Business continuity planning (BCP) / Change Control Management / Asset Management
- Relevant law and regulation (Legal regulation and compliance)
- Emerging Tech (Cloud security, IoT, ICS, OT)
- Troubleshooting and Risk Analysis

Common Certifications*

- (ISC)² Certified Information Systems Security Professional (CISSP)
- GIAC Certified Incident Handler (GCIH)
- ISACA Certified Information Systems Auditor (CISA)
- ISACA Certified Information Security Manager (CISM)
- GIAC Critical Controls Certification (GCCC)
- ISACA Certified in Risk and Information Systems Control (CRISC)
- ISO/IEC 27001:2013 Lead Auditor

Career Pathway

Chief Information Security Officer (CISO)

↑

Cyber Risk Manager

↑

Cyber Risk Analyst

Essential / Core Skills

- Network Security
- Linux
- Firewalls

Commonly Used Tools / New Technologies

- SQL
- LogRadar
- Security Information and Event Management (SIEM)
- Python
- Cascading Style Sheets (CSS)

Soft Skills

- Communication
- Computational Thinking
- Problem Solving
- Sense Making
- Teamwork
- Stakeholder Management

***This list is not exhaustive and serves only as a guide**

Domain: Governance Risk and Compliance (GRC)

	SFIA Level[1]	NOSS[2]
Chief Information Security Officer (CISO)	5	
Cyber Risk Manager	4 & 5	
Cyber Risk Analyst	3	

[1] SFIA Level:
SFIA stands for Skills Framework for the Information Age. It is a model for describing and managing skills and competencies for professionals working in the field of Information and Communication Technologies (ICT), software engineering and digital transformation. Published in 2000 by the British Computer Society (BCS).

[2] NOSS:
The acronym NOSS stands for National Occupational Skills Standards. NOSS is a document that outlines the dexterity required of an employee working in Malaysia at a certain level of employment to achieve specific skills.

PEMBANGUNAN SUMBER MANUSIA BERHAD
Wisma HRDF, Jalan Beringin, Damansara Heights
50490 Kuala Lumpur

Email: support@hrdf.com.my **Tel: 1800-88-4800**

CONNECT WITH

SECURITY PENETRATION TESTER

Job Description

- Performs assessments of systems, networks, application and technology (eg. IOT, cloud) within the network environment or enclave and identifies where those systems/networks deviate from acceptable configurations, enclave policy, or local policy
- Measures effectiveness of defense-in-depth architecture against known vulnerabilities

Competencies

- Audit & Compliance
- Cyber Risk Management
- Emerging Technology Synthesis
- Security Assessment & Testing
- Test Planning
- Threat Analysis & Defense
- Security Architecture Understanding
- Project Management
- Emerging Tech (Cloud security, IoT, ICS, OT)

Common Certifications*

- Offensive Security (OffSec) Certified Professional (OSCP)
- GIAC Penetration Tester Certification (GPEN)
- EC-Council Certified Security Analyst (ECSA)
- CompTIA Pentest+

Essential / Core Skills

- Penetration Testing
- Network Security
- Linux
- Python
- Ethical Hacking
- Kali Linux

Career Pathway

Chief Information Security Officer (CISO)

↑

Security Penetration Manager

↑

Security Penetration Tester

Commonly Used Tools / New Technologies

- Java
- Red Teaming
- Burp Suite
- Powershell

Soft Skills

- Communication
- Creative Thinking
- Problem Solving
- Sense Making
- Teamwork
- Stakeholder Management
- Report Writing

***This list is not exhaustive and serves only as a guide**

Domain: Penetration Testing

	SFIA Level [1]	NOSS [2]
Chief Information Security Officer (CISO)	5	
Security Penetration Manager	4 & 5	
Security Penetration Tester	3	Level 5, J620 Cyber Security Penetration Testing & Assessment -Cyber Security

[1] SFIA Level:
SFIA stands for Skills Framework for the Information Age. It is a model for describing and managing skills and competencies for professionals working in the field of Information and Communication Technologies (ICT), software engineering and digital transformation. Published in 2000 by the British Computer Society (BCS).

[2] NOSS:
The acronym NOSS stands for National Occupational Skills Standards. NOSS is a document that outlines the dexterity required of an employee working in Malaysia at a certain level of employment to achieve specific skills.

PEMBANGUNAN SUMBER MANUSIA BERHAD
Wisma HRDF, Jalan Beringin, Damansara Heights
50490 Kuala Lumpur

Email: support@hrdf.com.my **Tel: 1800-88-4800**

CONNECT WITH

SECURITY OPERATION ANALYST

Job Description

- Develops cyber indicators to maintain awareness of the status of the highly dynamic operating environment
- Collects, processes, analysis, and disseminates cyber threat/warning assessments

Competencies

- Cyber Incident Management
- Cyber Risk Management and Assessment
- Disaster Recovery Management
- Threat Analysis & Defense
- Threat Intelligence & Detection
- Enterprise Architecture
- Cyber Crisis Management
- Cyber Forensic
- Surveillance and Incident Response
- Operations Management

Common Certifications*

- GIAC Cyber Threat Intelligence (GCTI)
- (ISC)² Certified Information Systems Security Professional (CISSP)
- CompTIA Cybersecurity Analyst (CySA+)
- EC-Council Certificed SOC Analyst (CSA)
- EC-Council Certified Threat Intelligence Analyst (C|TIA)

Career Pathway

Chief Information Security Officer (CISO)

↑

Security Operation Manager

↑

Security Operation Analyst

Essential / Core Skills

- Security Information and Event Management (SIEM)
- Linux

Commonly Used Tools / New Technologies

- SQL
- Vulnerability Management
- LogRadar
- Wireshark

Soft Skills

- Communication
- Creative Thinking
- Problem Solving
- Sense Making
- Teamwork
- Stakeholder Management

***This list is not exhaustive and serves only as a guide**

Domain: Security Operation and Incident Response

	SFIA Level[1]	NOSS[2]
Chief Information Security Officer (CISO)	5	
Security Operation Manager	4	
Security Operation Analyst	3	

[1] SFIA Level:
SFIA stands for Skills Framework for the Information Age. It is a model for describing and managing skills and competencies for professionals working in the field of Information and Communication Technologies (ICT), software engineering and digital transformation. Published in 2000 by the British Computer Society (BCS).

[2] NOSS:
The acronym NOSS stands for National Occupational Skills Standards. NOSS is a document that outlines the dexterity required of an employee working in Malaysia at a certain level of employment to achieve specific skills.

PEMBANGUNAN SUMBER MANUSIA BERHAD
Wisma HRDF, Jalan Beringin, Damansara Heights
50490 Kuala Lumpur

Email: support@hrdf.com.my **Tel: 1800-88-4800**

CONNECT WITH

INCIDENT RESPONDER

Job Description

- Investigates, analyzes, and responds to cyber incidents within the network environment or enclave
- Identifies, collects, examines, and preserves evidence using controlled and documented analytical and investigative techniques
- Conducts detailed investigations on computer-based crimes establishing documentary or physical evidence, to include digital media and logs associated with cyber intrusion incidents

Competencies

- Cyber Forensic
- Cyber Risk Management
- Cyber Incident Management
- Threat Analysis & Defense
- Threat Intelligence & Detection
- Disaster Recovery Management
- Enterprise Architecture
- Cyber Crisis Management

Common Certifications*

- GIAC Certified Incident Handler (GCIH)
- PGI GCHQ Certified Security Operations Centre (SOC) Incident Responder
- EC-Council Computer Hacking Forensic Investigator (CHFI)
- GIAC Certified Forensic Analyst (GCFA)
- GIAC Certified Intrusion Analyst (GCIA)
- Certified Reverse Engineering Analyst (CREA)

Essential / Core Skills

- Incident Management
- ITIL
- Troubleshooting

Career Pathway

Chief Information Security Officer (CISO)

↑

Incident Manager

↑

Incident Responder

Commonly Used Tools / New Technologies

- Active Directory
- Incident Response
- Root Cause Analysis
- Incident Handling
- Agile Methodologies
- LogRadar

Soft Skills

- Communication
- Creative Thinking
- Problem Solving
- Sense Making
- Analytical
- Teamwork
- Stakeholder Management

Domain: Security Operation and Incident Response

***This list is not exhaustive and serves only as a guide**

	SFIA Level [1]	NOSS [2]
Chief Information Security Officer (CISO)	5	
Incident Manager	4 & 5	
Incident Responder	3	

[1] SFIA Level:
SFIA stands for Skills Framework for the Information Age. It is a model for describing and managing skills and competencies for professionals working in the field of Information and Communication Technologies (ICT), software engineering and digital transformation. Published in 2000 by the British Computer Society (BCS).

[2] NOSS:
The acronym NOSS stands for National Occupational Skills Standards. NOSS is a document that outlines the dexterity required of an employee working in Malaysia at a certain level of employment to achieve specific skills.

PEMBANGUNAN SUMBER MANUSIA BERHAD
Wisma HRDF, Jalan Beringin, Damansara Heights
50490 Kuala Lumpur

Email: support@hrdf.com.my **Tel: 1800-88-4800**

CONNECT WITH

DIGITAL FORENSIC SPECIALIST

Job Description

- Conducts detailed investigations on computer-based crimes establishing documentary or physical evidence, to include digital media and logs associated with cyber intrusion incidents
- Analyses digital evidence and investigates computer security incidents to derive useful information in support of system/network vulnerability mitigation
- Expert witness in court / Ability to testify in court

Competencies

- Cyber Forensic
- Cyber Risk Management
- Cyber Incident Management
- Security Assessment & Testing
- Threat Analysis & Defense
- Threat Intelligence & Detection
- Enterprise and Device Architecture
- Chain of custody. Relevant law and regulation (Legal / Statutory regulation and compliance)

Common Certifications*

- AccessData Certified Examiner (ACE)
- IACIS Certified Forensic Computer Examiner (CFCE)
- GIAC Certified Forensic Analyst (GCFA)
- EnCase™ Certified Examiner (EnCE)
- EC-Council Computer Hacking Forensic Investigator (CHFI)

Core Skills

- Network Security
- Linux
- Computer Forensics
- Python
- Forensic Analysis

Career Pathway

Chief Information Security Officer (CISO)

↑

Digital Forensic Manager

↑

Digital Forensic Specialist

Emerging Skills

- Malware Analysis
- Penetration Testing
- C++
- Cyber Threat Intelligence (CTI)
- Wireshark
- Analytics
- Machine Learning

Soft Skills

- Communication
- Creative Thinking
- Problem Solving
- Sense Making
- Teamwork
- Stakeholder Management
- Report Writing
- Analytical

***This list is not exhaustive and serves only as a guide**

Domain: Forensic Investigation and Threat Analysis

	SFIA Level[1]	NOSS[2]
Chief Information Security Officer (CISO)	5	
Digital Forensic Manager	4 & 5	
Digital Forensic Specialist	4	

[1] SFIA Level:
SFIA stands for Skills Framework for the Information Age. It is a model for describing and managing skills and competencies for professionals working in the field of Information and Communication Technologies (ICT), software engineering and digital transformation. Published in 2000 by the British Computer Society (BCS).

[2] NOSS:
The acronym NOSS stands for National Occupational Skills Standards. NOSS is a document that outlines the dexterity required of an employee working in Malaysia at a certain level of employment to achieve specific skills.

PEMBANGUNAN SUMBER MANUSIA BERHAD
Wisma HRDF, Jalan Beringin, Damansara Heights
50490 Kuala Lumpur

Email: support@hrdf.com.my **Tel: 1800-88-4800**

CONNECT WITH

SECURITY ENGINEER

Job Description

- Develops and implements secure system architecture
- Embeds security principles into the design of system architectures to mitigate the risks posed by new technologies and business practices.
- Performs routine activities related to the periodic review and audit activities of infrastructure security systems and maintains documentation of security standards and procedures

Competencies

- Business Needs Analysis
- Cyber Risk, Governance and Compliance Emerging Technology Synthesis
- Infrastructure Design / Enterprise Design
- Security Administration
- Security Architecture
- Security Solution Architecture
- Security Programme Management
- Security Strategy
- Business continuity planning (BCP) / Change Control Management
- Relevant law and regulation (Legal, statutory regulation and compliance)
- Emerging Tech (Cloud security, IoT, ICS, OT)
- Identify access control
- Information Security
- Troubleshooting

Common Certifications*

- (ISC)² Certified Information Systems Security Professional (CISSP)
- (ISC)² Certified Cloud Security Professional (CCSP)
- CSA Certified Cloud Security Knowledge (CCSK)
- General Data Protection Regulation (GDPR) certifications
- Personal Data Protection Act (PDPA) certifications
- Technology/Domain specific

Career Pathway

Chief Information Security Officer (CISO)

↑

Security Engineer

Core Skills

- Network Security
- Firewalls
- Linux
- Active Directory

Emerging Skills

- Amazon Web Services (AWS)
- Security Information and Event Management (SIEM)
- LogRadar
- Python
- Cisco products
- Cascading Style Sheets (CSS)
- Public Key Infrastructure (PKI) security

Soft Skills

- Communication
- Computational Thinking
- Problem Solving
- Sense Making
- Teamwork
- Stakeholder Management

***This list is not exhaustive and serves only as a guide**

Domain: Security Design and Engineering

	SFIA Level[1]	NOSS[2]
Chief Information Security Officer (CISO)	5	
Security Engineer	4	

[1] SFIA Level:
SFIA stands for Skills Framework for the Information Age. It is a model for describing and managing skills and competencies for professionals working in the field of Information and Communication Technologies (ICT), software engineering and digital transformation. Published in 2000 by the British Computer Society (BCS).

[2] NOSS:
The acronym NOSS stands for National Occupational Skills Standards. NOSS is a document that outlines the dexterity required of an employee working in Malaysia at a certain level of employment to achieve specific skills.

PEMBANGUNAN SUMBER MANUSIA BERHAD
Wisma HRDF, Jalan Beringin, Damansara Heights
50490 Kuala Lumpur

Email: support@hrdf.com.my **Tel: 1800-88-4800**

CONNECT WITH