



# Women Cyber Force

## CYBERSECURITY CAREER PATH













Guide

### Abstract

Planning a career in cybersecurity? This guide provides information on job titles, certifications and preparation resources from entry level to senior management.

[info@womencyberforce.lu](mailto:info@womencyberforce.lu)

# Contents

|   |    |
|---|----|
| INTRODUCTION.....   | 3  |
|  CYBERSECURITY IMPLEMENTER .....               | 4  |
|  Cyber INCIDENT RESPONDER.....                 | 6  |
|  CYBER LEGAL, POLICY & COMPLIANCE OFFICER..... | 8  |
|  CYBER THREAT INTELLIGENCE SPECIALIST .....    | 10 |
|  INFORMATION SECURITY OFFICER.....             | 12 |
|  Cybersecurity Auditor.....                   | 14 |
|  CYBERSECURITY ARCHITECT.....                | 16 |
|  Cybersecurity Researcher.....               | 18 |
|  CYBERSECURITY EDUCATOR.....                 | 20 |
|  Cybersecurity Risk OFFICER .....            | 22 |
|  Digital Forensics Investigator .....        | 24 |
|  PENETRATION TESTER.....                     | 26 |



EUROPEAN UNION AGENCY  
FOR CYBERSECURITY



---

<https://www.enisa.europa.eu/topics/cybersecurity-education/european-cybersecurity-skills-framework>

---

## INTRODUCTION

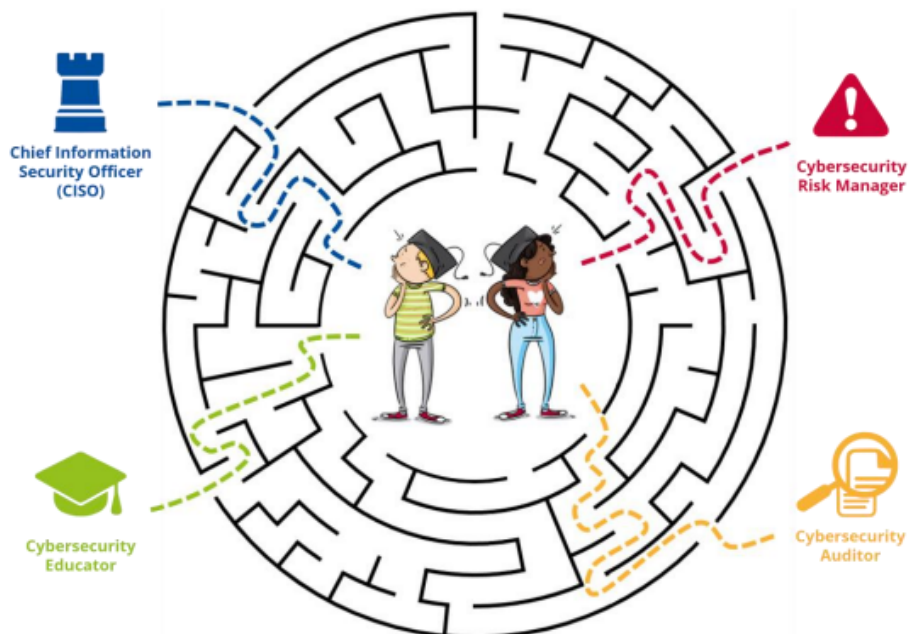
---

The cybersecurity industry remains a promising area of growth when it comes to career paths in tech and beyond. In recent years, while many industries saw decreases in opportunity due to the economic volatility and uncertainty that came with navigating an unprecedented global pandemic, the cybersecurity industry continued to grow. Remote work security risks, increasing ransomware attacks, and more all contributed to the increased need for cyber professionals.

However, there have been concerns that there just aren't enough people with the necessary skills to hire for all the available cybersecurity openings. This makes it a great time to consider one of the many different cybersecurity careers available for those with the right training.

This guide provides a non-exhaustive list of some of the cybersecurity careers with useful information. We took the European Cybersecurity Skills Framework from ENISA and we added more information about certifications, courses, and books everyone can use in that specific role.

---





# CYBERSECURITY IMPLEMENTER

## MISSION

Provides cybersecurity-related technical development, integration, testing, implementation, operation, maintenance, monitoring and support of cybersecurity solutions. Ensures adherence to specifications and conformance requirements, assures sound performance and resolves technical issues required in the organization’s cybersecurity-related solutions (systems, assets, software, controls and services), infrastructures and products.

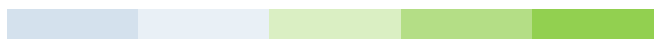
## RELATED FUNCTIONAL TITLES

- Information Security Implementer
- Cybersecurity Solutions Expert
- Cybersecurity Developer
- Cybersecurity Engineer
- Development, Security & Operations (DevSecOps) Engineer

## KNOWLEDGE

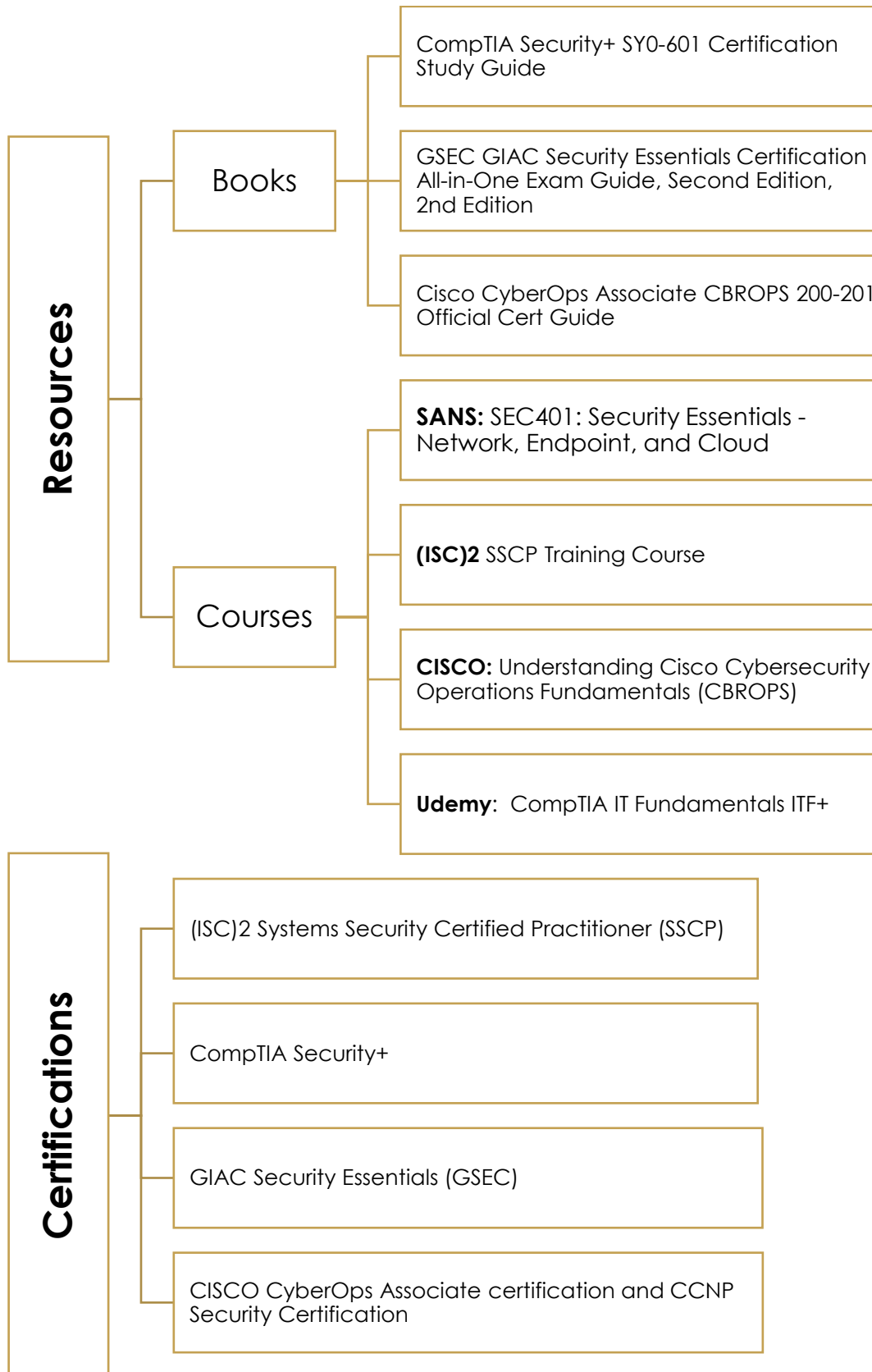
- Secure development lifecycle
- Computer programming
- Operating systems security
- Computer networks security
- Cybersecurity controls and solutions
- Offensive and defensive security practices
- Secure coding recommendations and best practices
- Cybersecurity recommendations and best practices
- Testing standards, methodologies and frameworks
- Testing procedures
- Cybersecurity-related technologies

## EFFORT LEVEL





# CYBERSECURITY IMPLEMENTER





## CYBER INCIDENT RESPONDER

### MISSION

Monitors and assesses systems' cybersecurity state. Analyses, evaluates and mitigates the impact of cybersecurity incidents. Identifies cyber incidents root causes and malicious actors. According to the organization's incident response plan, restores systems and processes' functionalities to an operational state, collecting evidences and documenting actions taken.

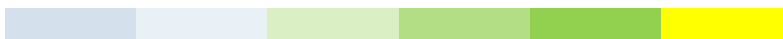
### RELATED FUNCTIONAL TITLES

- Cyber Incident Handler
- Cyber Crisis Expert
- Incident Response Engineer
- Security Operations Center (SOC) Analyst
- Cyber Fighter /Defender
- Security Operation Analyst (SOC Analyst)
- Cybersecurity SIEM Manager

### KNOWLEDGE

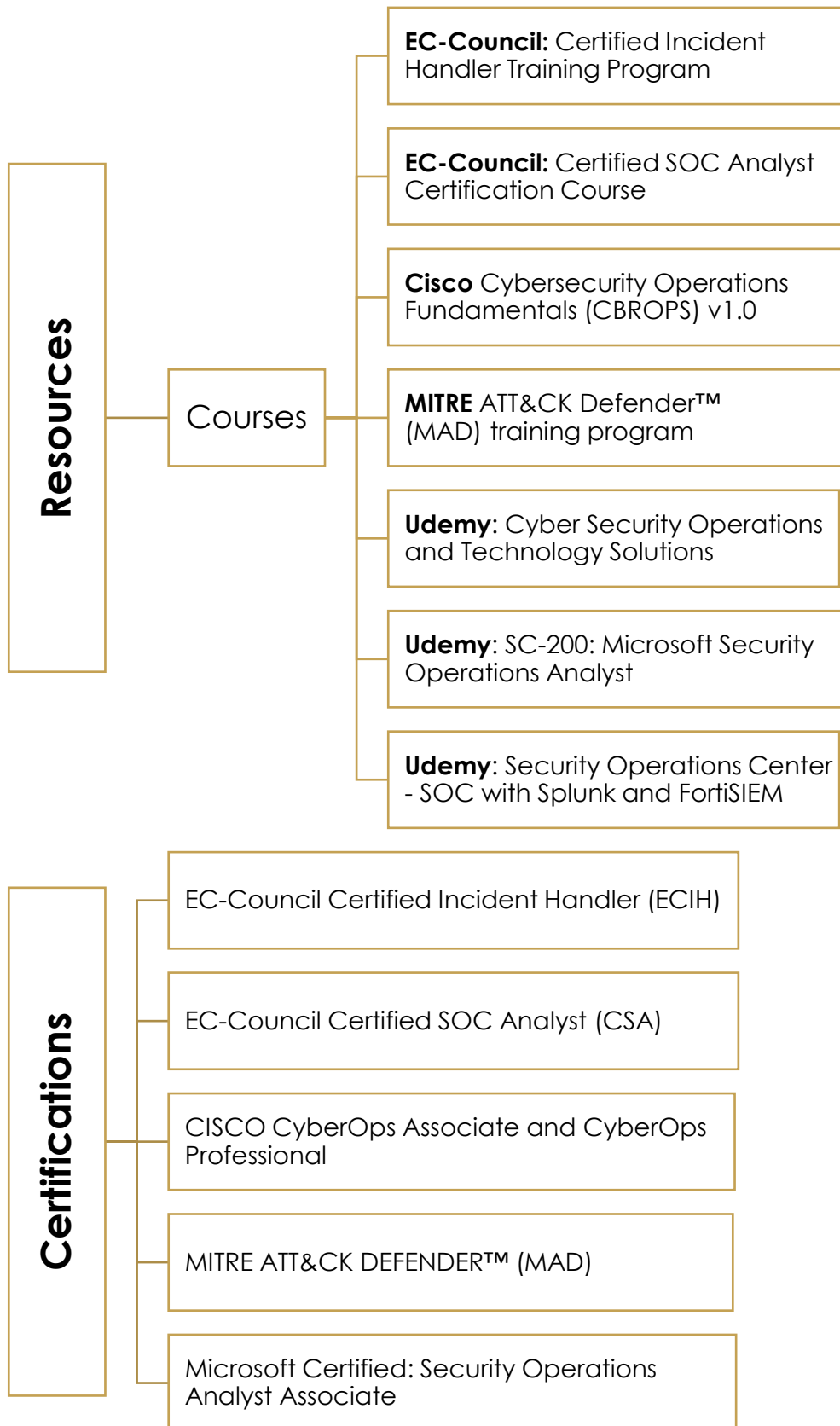
- Incident handling standards, methodologies and frameworks
- Incident handling recommendations and best practices
- Incident handling tools
- Incident handling communication procedures
- Operating systems security
- Computer networks security
- Cyber threats
- Cybersecurity attack procedures
- Computer systems vulnerabilities
- Cybersecurity-related certifications
- Cybersecurity related laws, regulations and legislations
- Secure operation centers (SOC) operation
- Computer security incident response teams (CSIRT) operation

### EFFORT LEVEL





# CYBER INCIDENT RESPONDER







## CYBER LEGAL, POLICY & COMPLIANCE OFFICER

### MISSION

Oversees and assures compliance with cybersecurity- and data-related legal, regulatory frameworks and policies in line with the organization’s strategy and legal requirements. Contributes to the organization’s data protection related actions. Provides legal advice in the development of the organization’s cybersecurity governance processes and recommended remediation strategies/solutions to ensure compliance.

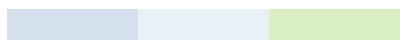
### RELATED FUNCTIONAL TITLES

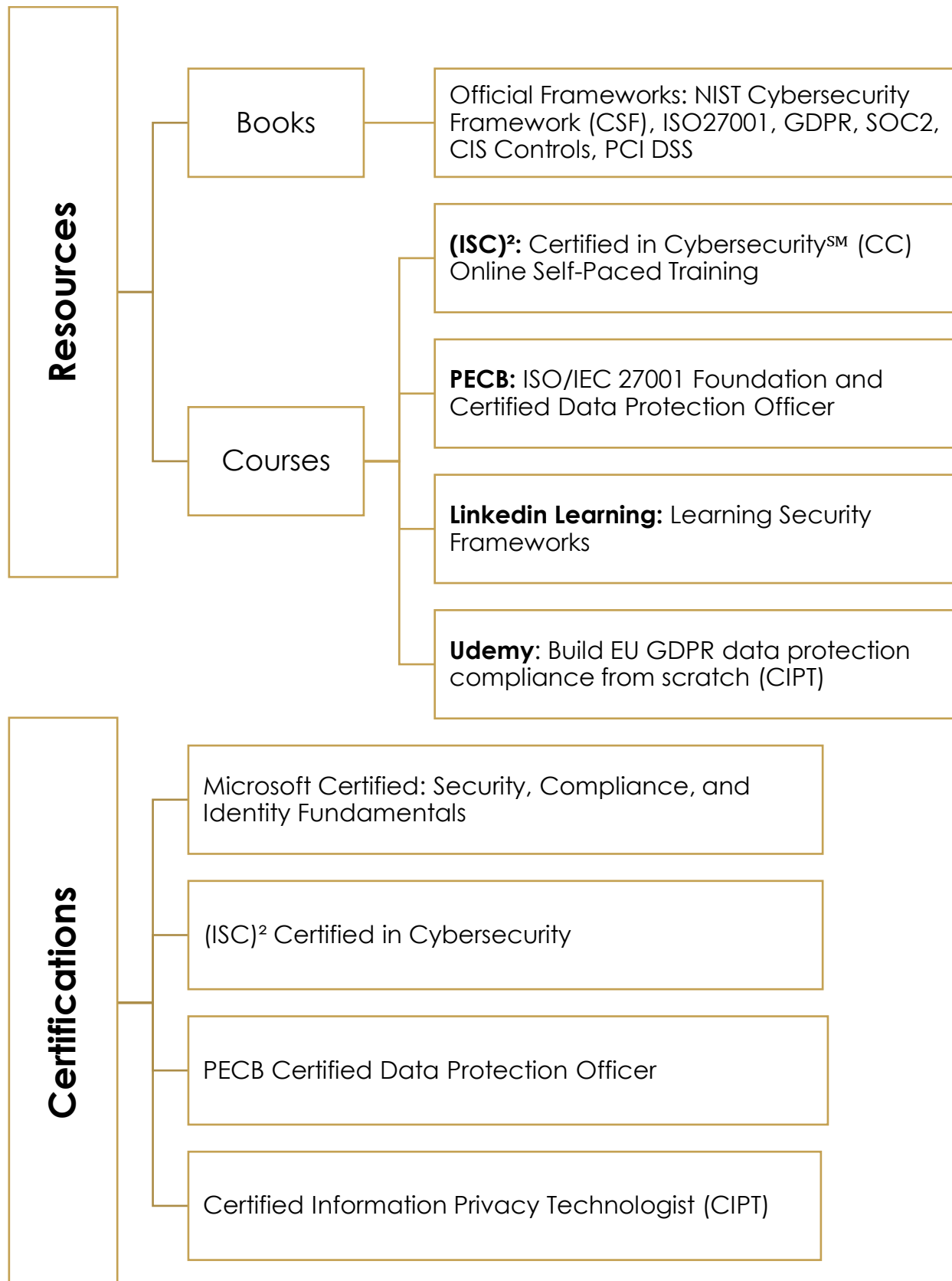
- Data Protection Officer (DPO)
- Privacy Protection Officer
- Cyber Law Consultant
- Cyber Legal Advisor
- Information Governance Officer
- Data Compliance Officer
- Cybersecurity Legal Officer
- IT/ICT Compliance Manager
- Governance Risk Compliance (GRC) Consultant

### KNOWLEDGE

- Cybersecurity related laws, regulations and legislations
- Cybersecurity standards, methodologies and frameworks
- Cybersecurity policies
- Legal, regulatory and legislative compliance requirements, recommendations and best practices
- Privacy impact assessment standards, methodologies and frameworks

### EFFORT LEVEL







# CYBER THREAT INTELLIGENCE SPECIALIST

## MISSION

Manages cyber threat intelligence life cycle including cyber threat information collection, analysis and production of actionable intelligence and dissemination to security stakeholders and the CTI community, at a tactical, operational and strategic level. Identifies and monitors the tactics, techniques and procedures (TTPs) used by cyber threat actors and their trends, track threat actors' activities and observe how non-cyber events can influence cyber-related actions.

## RELATED FUNCTIONAL TITLES

- Cyber Intelligence Analyst
- Cyber Threat Modeler

## KNOWLEDGE

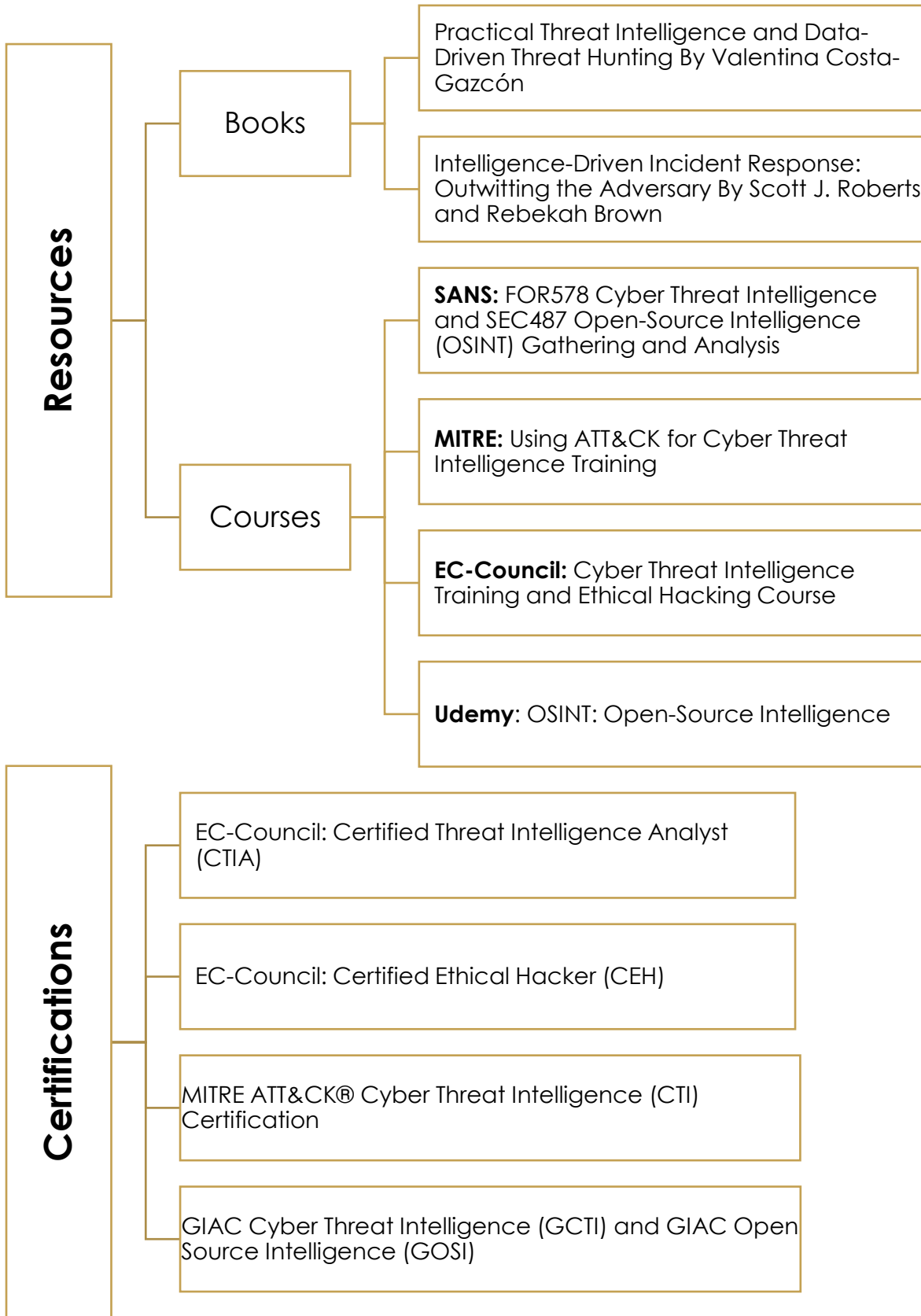
- Operating systems security
- Computer networks security
- Cybersecurity controls and solutions
- Computer programming
- Cyber Threat Intelligence (CTI) sharing standards, methodologies and frameworks
- Responsible information disclosure procedures
- Cross-domain and border-domain knowledge related to cybersecurity
- Cyber threats
- Cyber threat actors
- Cybersecurity attack procedures
- Advanced and persistent cyber threats (APT)
- Threat actors Tactics, Techniques and Procedures (TTPs)

## EFFORT LEVEL





# CYBER THREAT INTELLIGENCE SPECIALIST





## INFORMATION SECURITY OFFICER

### MISSION

Manages cyber threat intelligence life cycle including cyber threat information collection, analysis and production of actionable intelligence and dissemination to security stakeholders and the CTI community, at a tactical, operational and strategic level. Identifies and monitors the tactics, techniques and procedures used by cyber threat actors and their trends, track threat actors' activities and observe how non-cyber events can influence cyber-related actions.

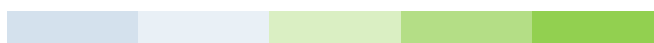
### RELATED FUNCTIONAL TITLES

- Cybersecurity Programme Director
- Chief Information Security Officer (CISO)
- Information Security Manager
- Head Of Information Security
- IT/ICT Security Officer

### KNOWLEDGE

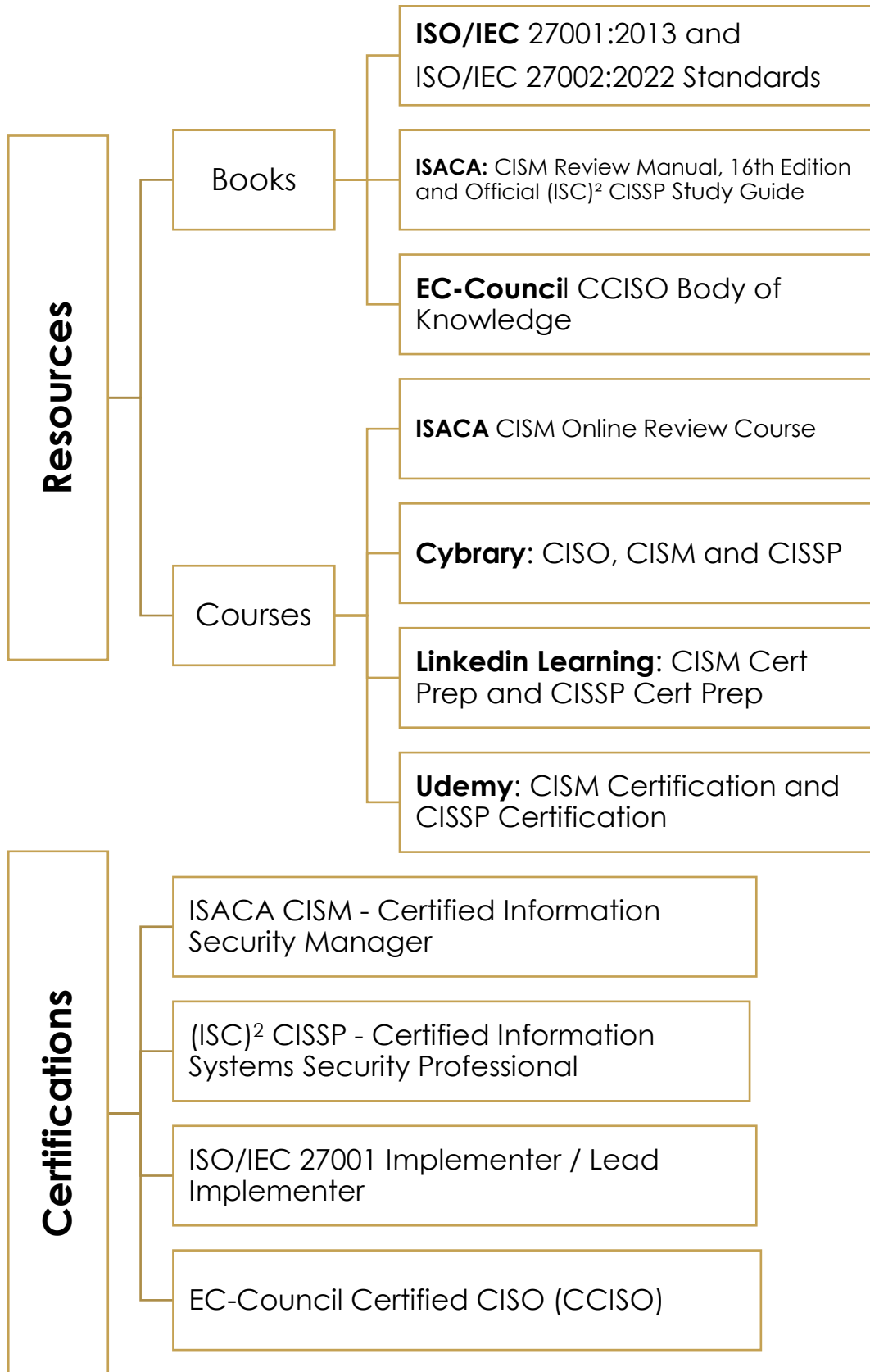
- Assess and enhance an organization's cybersecurity posture
- Analyze and implement cybersecurity policies, certifications, standards and frameworks
- Analyze and comply with cybersecurity-related laws, regulations and legislations
- Implement cybersecurity recommendations and best practices
- Develop, champion and lead the execution of a cybersecurity strategy
- Review and enhance security documents, reports, SLAs and ensure the security objectives
- Identify and solve cybersecurity-related issues
- Establish a cybersecurity plan
- Communicate, coordinate and cooperate with internal and external stakeholders
- Anticipate required changes to the organization's information security strategy and formulate new plans

### EFFORT LEVEL





# INFORMATION SECURITY OFFICER





# CYBERSECURITY AUDITOR

## MISSION

Conducts independent reviews to assess the effectiveness of processes and controls and the overall compliance with the organization’s legal and regulatory frameworks policies. Evaluates, tests and verifies cybersecurity-related products (systems, hardware, software and services), functions and policies ensuring, compliance with guidelines, standards and regulations.

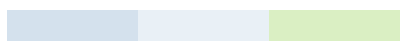
## RELATED FUNCTIONAL TITLES

- Information Security Auditor (IT or Legal Auditor)
- Governance Risk Compliance (GRC) Auditor
- Cybersecurity Audit Manager
- Cybersecurity Procedures and Processes Auditor
- Information Security Risk and Compliance Auditor
- Data Protection Assessment Analyst

## KNOWLEDGE

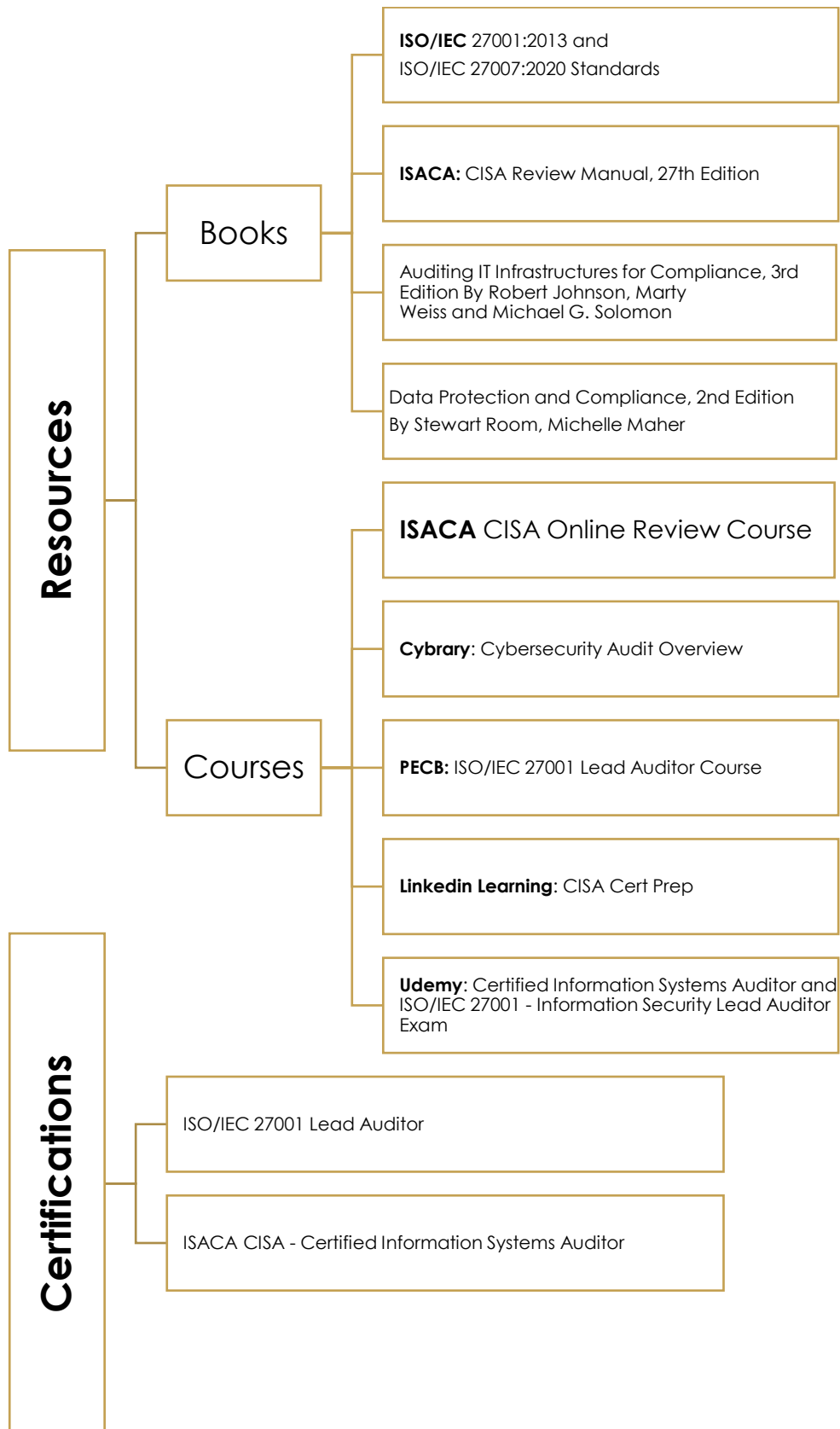
- Cybersecurity controls and solutions
- Legal, regulatory and legislative compliance requirements, recommendations and best practices
- Monitoring, testing and evaluating cybersecurity controls' effectiveness
- Conformity assessment standards, methodologies and frameworks
- Auditing standards, methodologies and frameworks
- Cybersecurity standards, methodologies and frameworks
- Auditing-related certification
- Cybersecurity-related certifications

LEVEL  
EFFORT





# CYBERSECURITY AUDITOR







# CYBERSECURITY ARCHITECT

## MISSION

Designs solutions based on security-by-design and privacy-by-design principles. Creates and continuously improves architectural models and develops appropriate architectural documentation and specifications. Coordinate secure development, integration and maintenance of cybersecurity components in line with standards and other related requirements.

## RELATED FUNCTIONAL TITLES

- Cybersecurity Solutions Architect
- Cybersecurity Designer
- Data Security Architect

## KNOWLEDGE

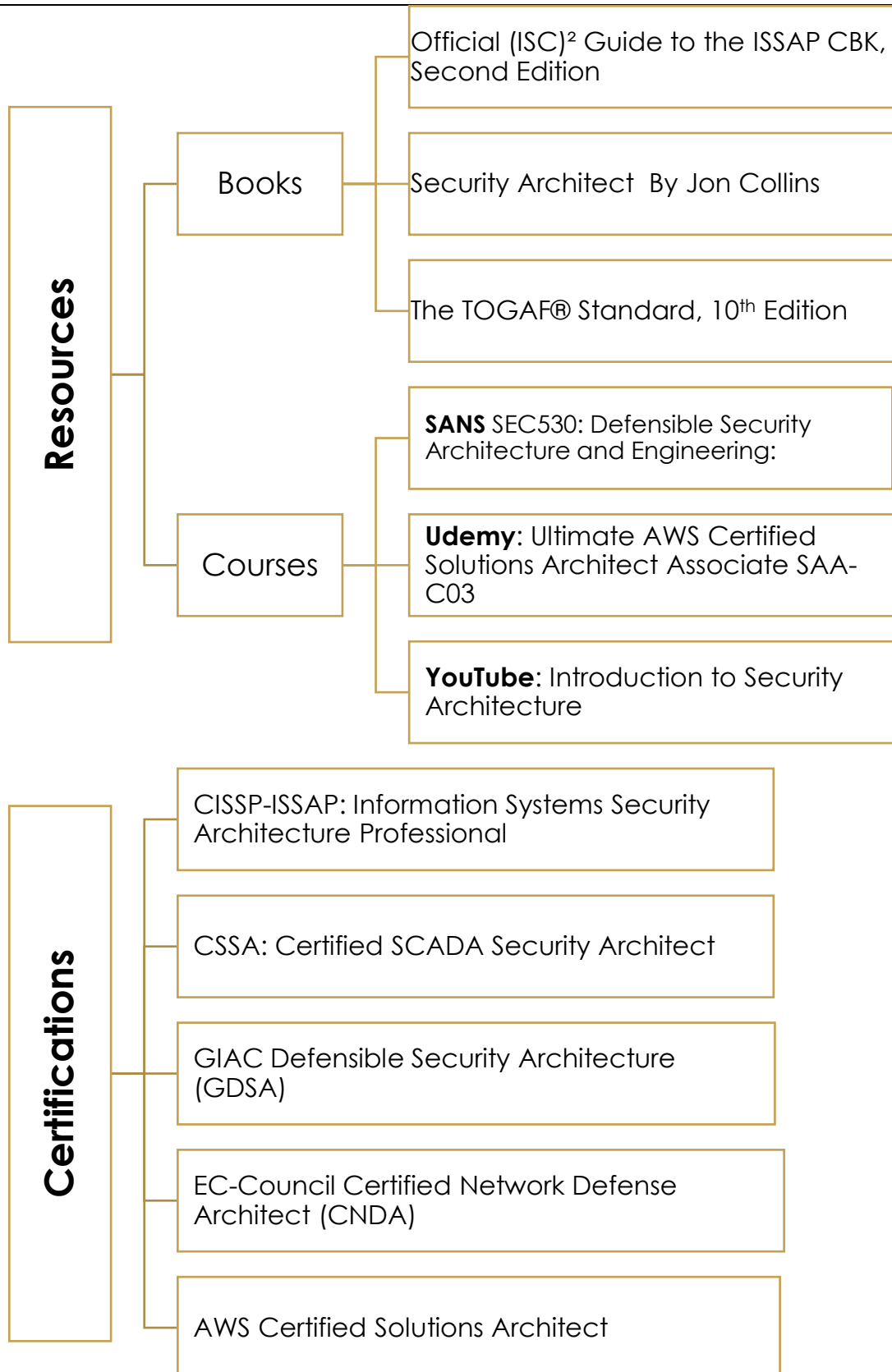
- Cybersecurity-related certifications
- Cybersecurity recommendations and best practices
- Cybersecurity standards, methodologies and frameworks
- Cybersecurity-related requirements analysis
- Secure development lifecycle
- Security architecture reference models
- Cybersecurity-related technologies
- Cybersecurity controls and solutions
- Cybersecurity risks & Cyber threats
- Cybersecurity trends
- Legal, regulatory and legislative compliance requirements, recommendations and best practices
- Legacy cybersecurity procedures
- Privacy-Enhancing Technologies (PET)
- Privacy-by-design standards, methodologies & frameworks

**EFFORT LEVEL**





# CYBERSECURITY ARCHITECT





## CYBERSECURITY RESEARCHER

### MISSION

Conducts fundamental/basic and applied research and facilitates innovation in the cybersecurity domain through cooperation with other stakeholders. Analyses trends and scientific findings in cybersecurity.

### RELATED FUNCTIONAL TITLES

- Cybersecurity Research Engineer
- Chief Research Officer (CRO) in cybersecurity
- Senior Research Officer in cybersecurity
- Research and Development (R&D) Officer in cybersecurity
- Scientific Staff in cybersecurity
- Research and Innovation Officer/Expert in cybersecurity
- Research Fellow in cybersecurity

### KNOWLEDGE

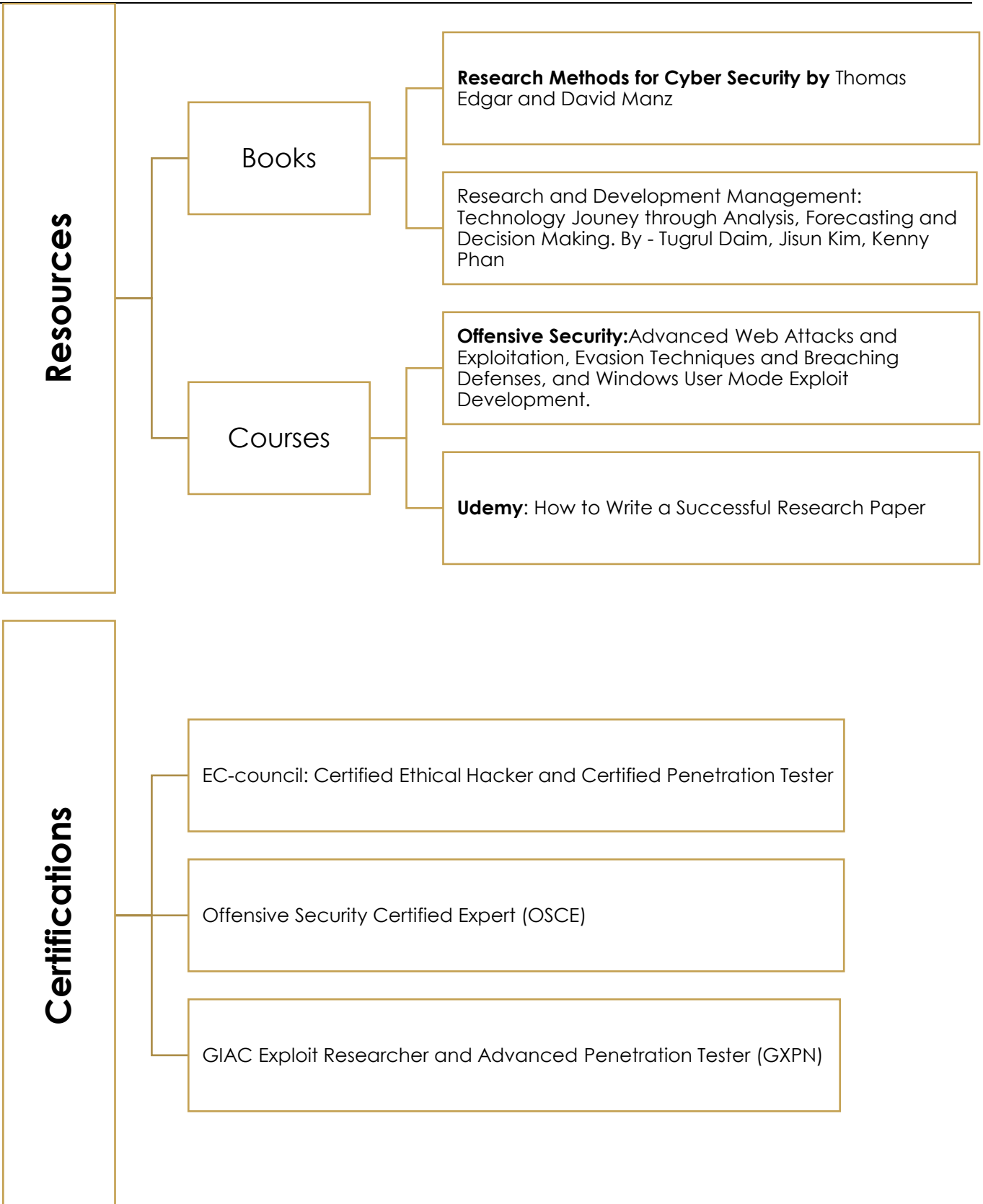
- Cybersecurity-related research, development and innovation (RDI)
- Cybersecurity standards, methodologies and frameworks
- Legal, regulatory and legislative requirements on releasing or using cybersecurity related technologies
- Multidiscipline aspect of cybersecurity
- Responsible information disclosure procedures

**EFFORT LEVEL**





# CYBERSECURITY RESEARCHER





# CYBERSECURITY EDUCATOR

## MISSION

Designs, develops and conducts awareness, training and educational programmes in cybersecurity and data protection-related topics. Uses appropriate teaching and training methods, techniques and instruments to communicate and enhance the cybersecurity culture, capabilities, knowledge and skills of human resources. Promotes the importance of cybersecurity and consolidates it into the organization.

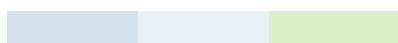
## RELATED FUNCTIONAL TITLES

- Cybersecurity Awareness Specialist
- Cybersecurity Trainer
- Faculty in Cybersecurity (Professor, Lecturer)

## KNOWLEDGE

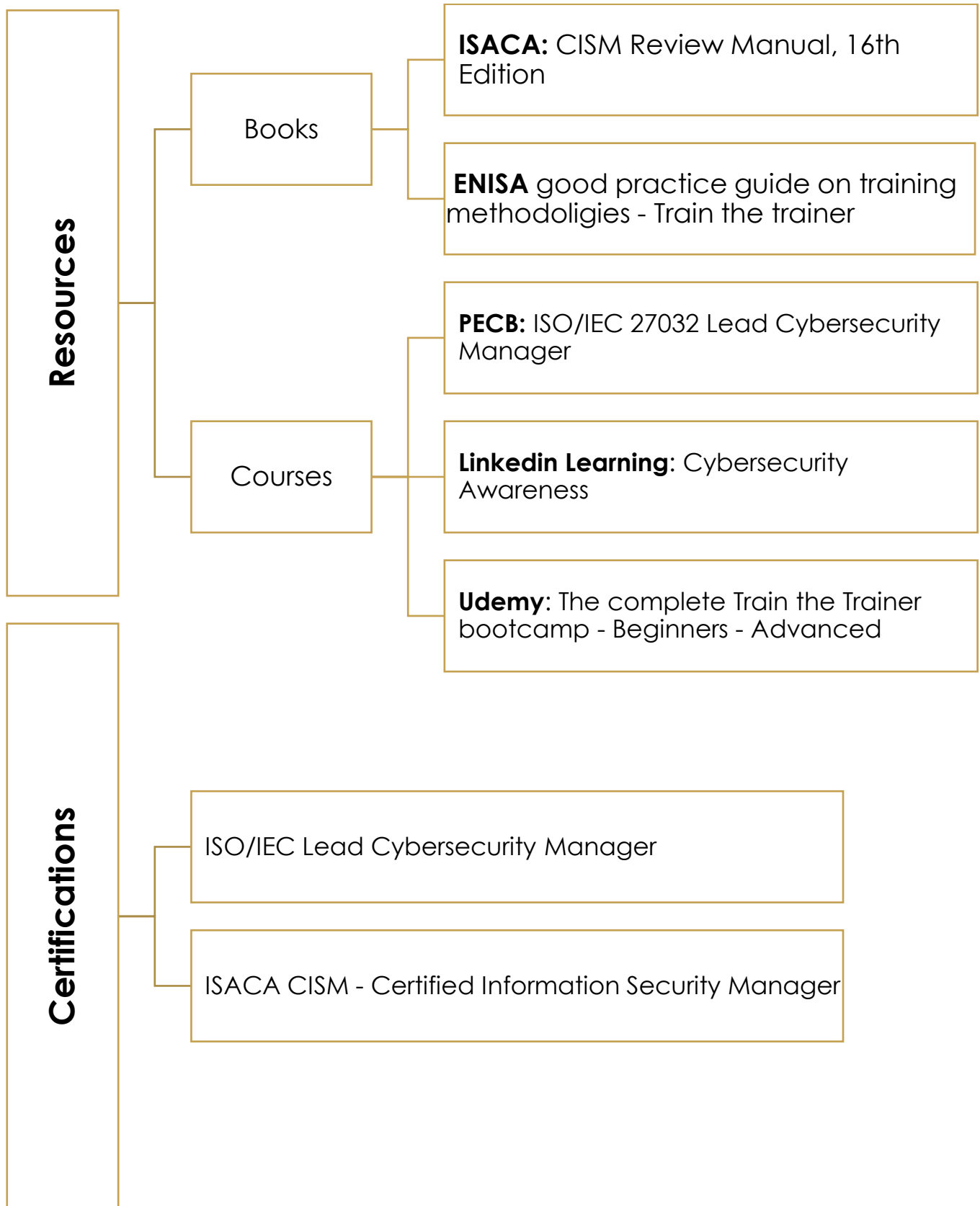
- Pedagogical standards, methodologies and frameworks
- Cybersecurity awareness, education and training programme development
- Cybersecurity-related certifications
- Cybersecurity education and training standards, methodologies and frameworks
- Cybersecurity related laws, regulations and legislations
- Cybersecurity recommendations and best practices
- Cybersecurity standards, methodologies and frameworks
- Cybersecurity controls and solutions

LEVEL  
EFFORT





# CYBERSECURITY EDUCATOR





## CYBERSECURITY RISK OFFICER

### MISSION

Continuously manages (identifies, analyses, assesses, estimates, mitigates) the cybersecurity-related risks of ICT infrastructures, systems and services by planning, applying, reporting and communicating risk analysis, assessment and treatment. Establishes a risk management strategy for the organization and ensures that risks remain at an acceptable level for the organization by selecting mitigation actions and controls.

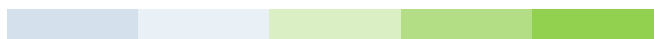
### RELATED FUNCTIONAL TITLES

- Information Security Risk Analyst
- Cybersecurity Risk Assurance Consultant
- Cybersecurity Risk Assessor
- Cybersecurity Impact Analyst
- Cyber Risk Manager

### KNOWLEDGE

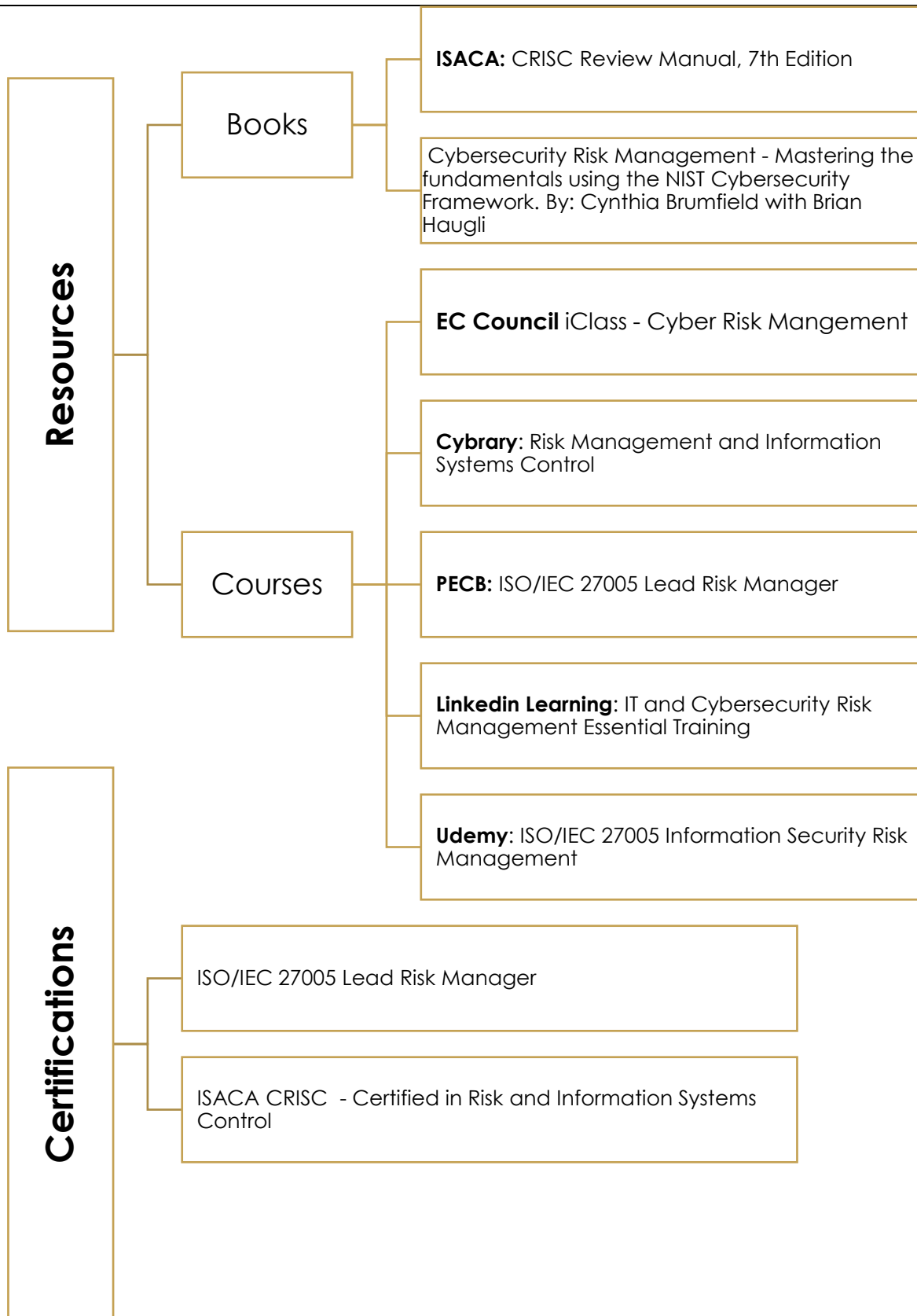
- Risk management standards, methodologies and frameworks
- Risk management tools
- Risk management recommendations and best practices
- Cyber threats
- Computer systems vulnerabilities
- Cybersecurity controls and solutions
- Cybersecurity risks
- Monitoring, testing and evaluating cybersecurity controls' effectiveness
- Cybersecurity-related certifications
- Cybersecurity-related technologies

**EFFORT  
LEVEL**





# CYBERSECURITY RISK OFFICER







# DIGITAL FORENSICS INVESTIGATOR

## MISSION

Connects artefacts to natural persons, captures, recovers, identifies and preserves data, including manifestations, inputs, outputs and processes of digital systems under investigation. Provides analysis, reconstruction and interpretation of the digital evidence based on a qualitative opinion. Presents an unbiased qualitative view without interpreting the resultant findings.

## RELATED FUNCTIONAL TITLES

- Digital Forensics Analyst
- Cybersecurity & Forensic Specialist
- Computer Forensics Consultant

## KNOWLEDGE

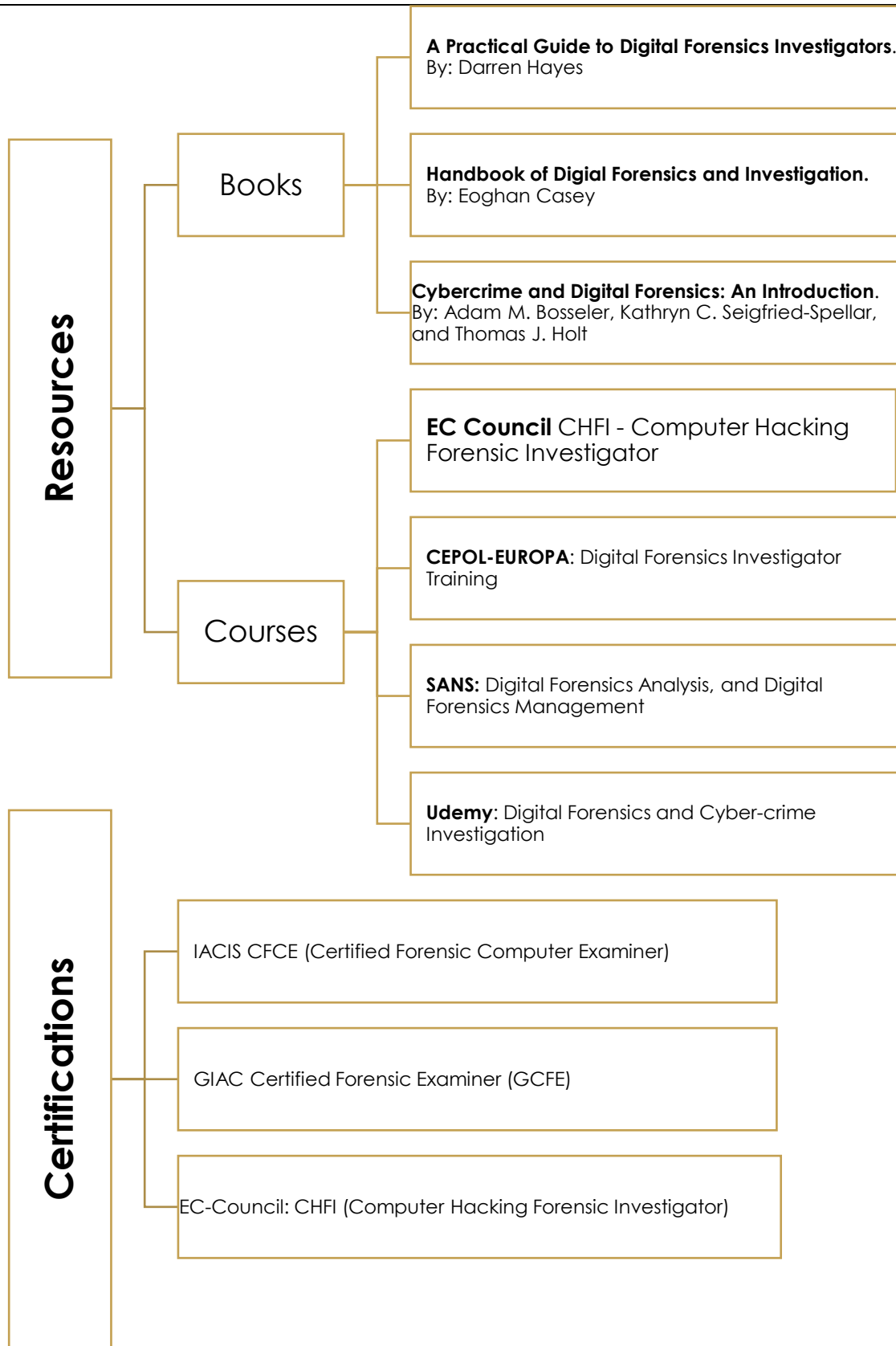
- Digital forensics recommendations and best practices
- Digital forensics standards, methodologies and frameworks
- Digital forensics analysis procedures
- Testing procedures
- Criminal investigation procedures, standards, methodologies and frameworks
- Cybersecurity related laws, regulations and legislations
- Malware analysis tools
- Cyber threats
- Computer systems vulnerabilities
- Cybersecurity attack procedures
- Operating systems security
- Computer networks security
- Cybersecurity-related certifications

## EFFORT LEVEL





# DIGITAL FORENSICS INVESTIGATOR





# PENETRATION TESTER

## MISSION

Plans, designs, implements and executes penetration testing activities and attack scenarios to evaluate the effectiveness of deployed or planned security measures. Identifies vulnerabilities or failures on technical and organizational controls that affect the confidentiality, integrity and availability of ICT products (e.g. systems, hardware, software and services).

## RELATED FUNCTIONAL TITLES

- Pen-tester
- Ethical Hacker
- Vulnerability Analyst
- Cybersecurity Tester
- Offensive Cybersecurity Expert
- Defensive Cybersecurity Expert
- Red Team Expert
- Red Teamer

## KNOWLEDGE

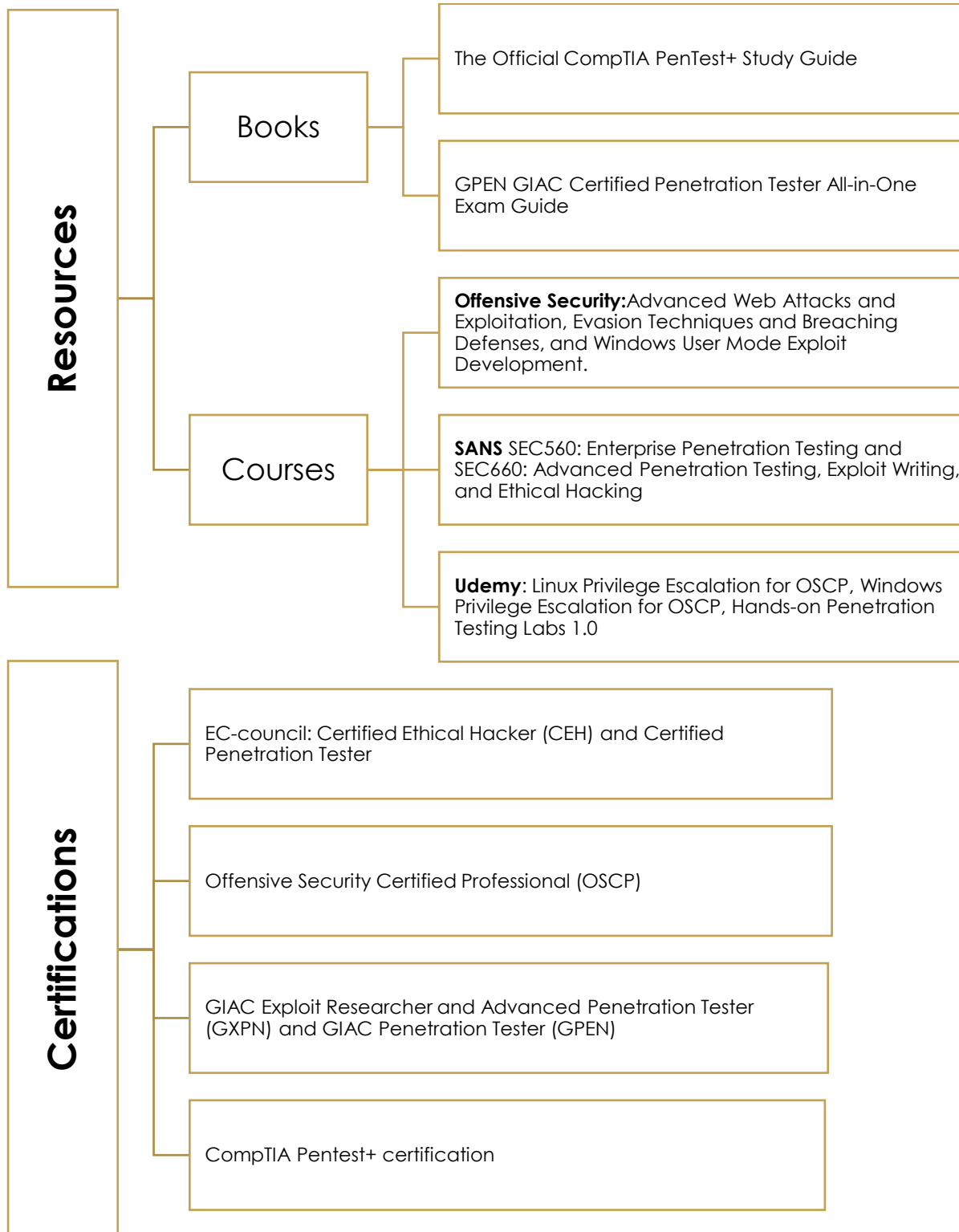
- Cybersecurity attack procedures
- Information technology (IT) and operational technology (OT) appliances
- Offensive and defensive security procedures
- Operating systems security
- Computer networks security
- Penetration testing procedures
- Penetration testing standards, methodologies and frameworks
- Penetration testing tools
- Computer programming
- Computer systems vulnerabilities
- Cybersecurity recommendations and best practices
- Cybersecurity-related certifications

**EFFORT LEVEL**





# PENETRATION TESTER



## Placing the European Cybersecurity Skills Framework role profiles in the context of a management circle

