

Certifications

BE-CYBER 08/10/2024



Eric Van Cangh

Senior BG Leader Cybersecurity

Eric.vancangh@agoria.be

+32 (0)2 706 78 25

.AGORIA

Cyber Made in Belgium

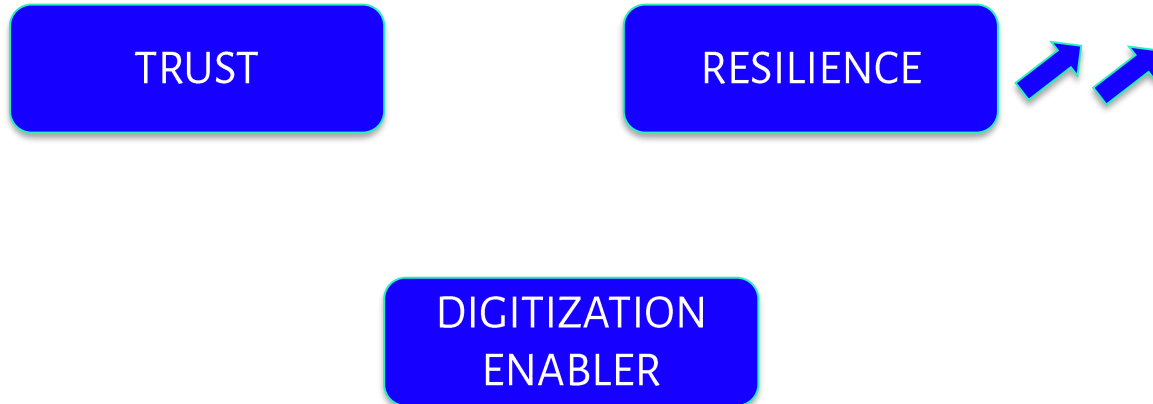


Agenda

- Introduction
 - Value proposition of Cybersecurity
 - Set the scene
 - Demistify the Logical CS world
- Certification and career path ?
 - Foundation blocks
 - Overview of most wellknown worldwide CS Certification bodies.
- The dimensions of a certification
- Added value of a certification
- Key take aways

Introduction – Value Proposition

- The Value proposition of Cyber Security

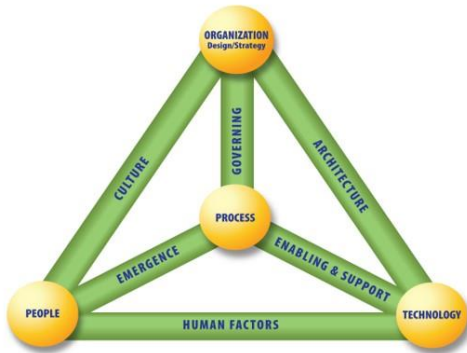


Introduction - Set the scene – CyberSecurity ?



The Security triad

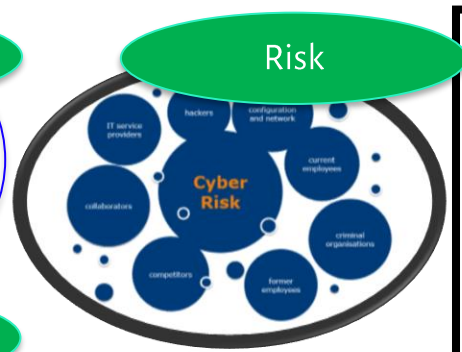
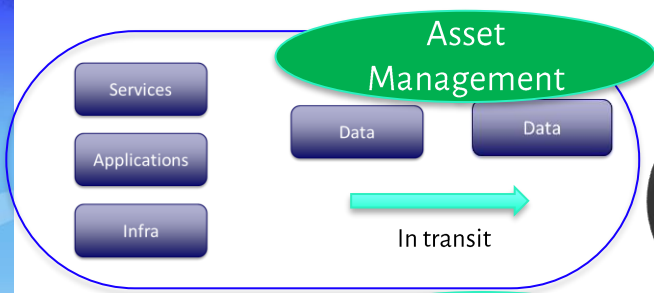
Confidentiality , Integrity , Availability



All the means to secure/protect the information
at People, Process and Technology level

[https://cio-wiki.org/wiki/Business_Model_for_Information_Security_\(BMIS\)](https://cio-wiki.org/wiki/Business_Model_for_Information_Security_(BMIS))

Set the scene - Context



Ownership

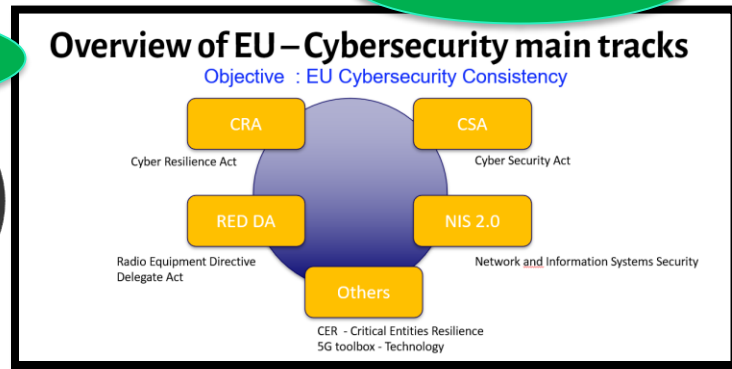
Attributs de Sécurité	Besoin en Sécurité			
C rating	Correctement classifié			
I rating	Correctement classifié			
A rating	Correctement classifié			
Business Owner	Correctement Inventoré	I	A	R
Technical Owner	Correctement Inventoré	I	A	R
Subject Matter Expert (SME) Owner	Correctement Inventoré	I	A	R
CMDB owner	Correctement Inventoré	I	A	R
ENV Environment	Correctement Inventoré	I	A	R
RTO	Besoin en Continuité	C	A	R
RPO	Besoin en Continuité	C	A	R
Web facing	Protégés (gérer risques)	R	R	A
OS (operating system)	Complétude des attributs de sécurité	I	A	R
Config admin group	protégés (accès)	A	R	C
CI Status	Décomissionné en fin de vie	R	A	I
Security OPERATIONAL STATUS				
Classe = CI Type	Correctement Inventoré	I	A	R
Asset type	Correctement Inventoré	I	A	R
Asset subtype	Correctement Inventoré	I	A	R
Last review date	Complétude des attributs de sécurité	I	A	R
Creation date	Demande création actif	R	A	C
Antimalware (installed)	Protégés (gérer risques)			
ISO SEC location	Besoin en Continuité			
CMDB field properties	Complétude des attributs de sécurité			
Security Impact (yes/no)	Protégés (gérer risques)	R		

Ownership

- Confidentiality
- Integrity
- Availability
- Privacy
- Safety

Attributes

Compliance



Nis 2.0 – Network and Information Security Directive

Verticals

Essential entities	Other entities
Energy (electricity, district heating, oil, gas, renewable)	Postal and courier services
Transport (air, sea, water, road)	Waste management
Banking	Chemicals (production, distribution, distribution)
Financial market infrastructures	Food (production, processing, distribution)
Health (healthcare, pharmaceuticals, research and manufacturing of pharmaceuticals, medical devices, computer, electronic and optical products, and medical devices)	Manufacturing (medical devices, computer, electronic and optical products, and medical devices)
Drinking water	Digital providers (search engines, online market places and social networks)
Waste water	
Digital infrastructure (core, data, data centres, DNS, electronic communications and trust services providers)	
Public administrations	
Space	

* New types of entities in electricity, chemicals, production, aggregation, demand response and energy storage

In nutshell

- European directive
- Cybersecurity package of measures
- Further improving the resilience and incident response capabilities
- Set the baseline Security framework inline with trends of Digitalization
- Center for Security Belgium – Single point of contact with European Cooperation Group
- New 2:0 Notion of **Essential** and **Important entities**
- New 2:0 **Scope extended** compared with NIS 1.0
- Impact for Members (ongoing)

TBC: ICT service management Services could potentially be considered as an essential entities (Council proposition)

DEMISTIFY THE “LOGICAL CS” WORLD



ZOOM IN



**ARE YOU KNOWING?
ARE YOU CERTIFIED?**

CISSP

CRISC—CISA—CISM

CEH / C-CISO

COMPTIA A+ / NETWORK+

CSSLP

Certification and Career Path



Agenda

- Introduction
 - Value proposition of Cybersecurity
 - Set the scene
 - Demistify the Logical CS world
- Certification and career path ?
 - Foundation blocks
 - Overview of most well-known worldwide CS Certification bodies.
- The dimensions of a certification
- Added value of a certification
- Key take aways

Certification and career path ?

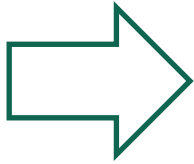
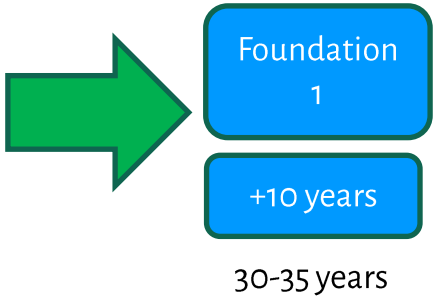
- Understanding the cyber security path with **Attributes / Dimension**



Lauren Wheeler is graduating from Augusta University with a bachelor's degree in cybersecurity, and she was recently named the 2022 Top Cybersecurity Student for the School of Computer and Cyber Sciences.

Lauren Wheeler

<https://jagwire.augusta.edu/graduation-week-2022-cybersecurity-grad-prepares-to-protect-the-world/>



TIME FOR REFLEXION **AND**
CERTIFICATION

Certification and career path ?

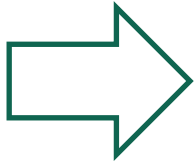
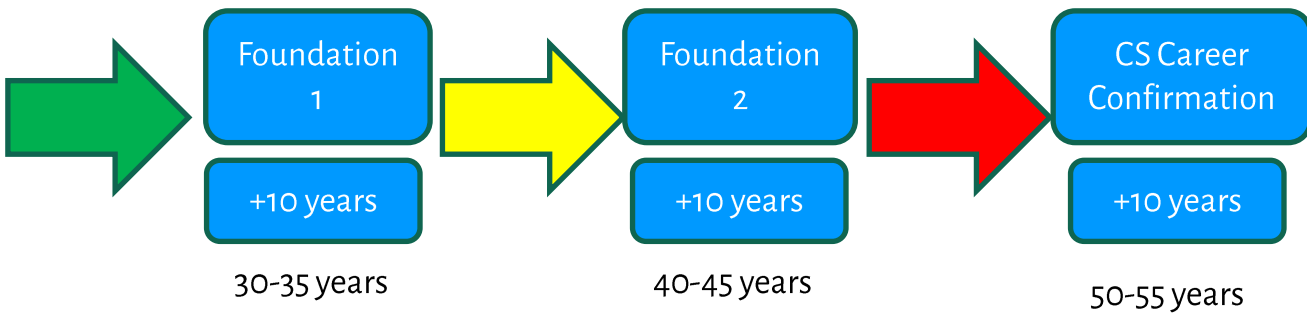
- Understanding the cyber security path with **Attributes / Dimension**



Lauren Wheeler is graduating from Augusta University with a bachelor's degree in cybersecurity, and she was recently named the 2022 Top Cybersecurity Student for the School of Computer and Cyber Sciences.

Lauren Wheeler

<https://jagwire.augusta.edu/graduation-week-2022-cybersecurity-grad-prepares-to-protect-the-world/>



TIME FOR REFLEXION **AND**
CERTIFICATION

Suscitate IT / CS interest very earlier



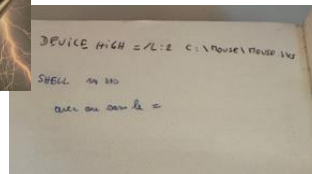
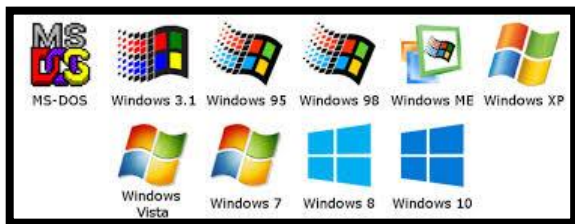
Schneider CPC 6128
8-12 years old –
1983-1987

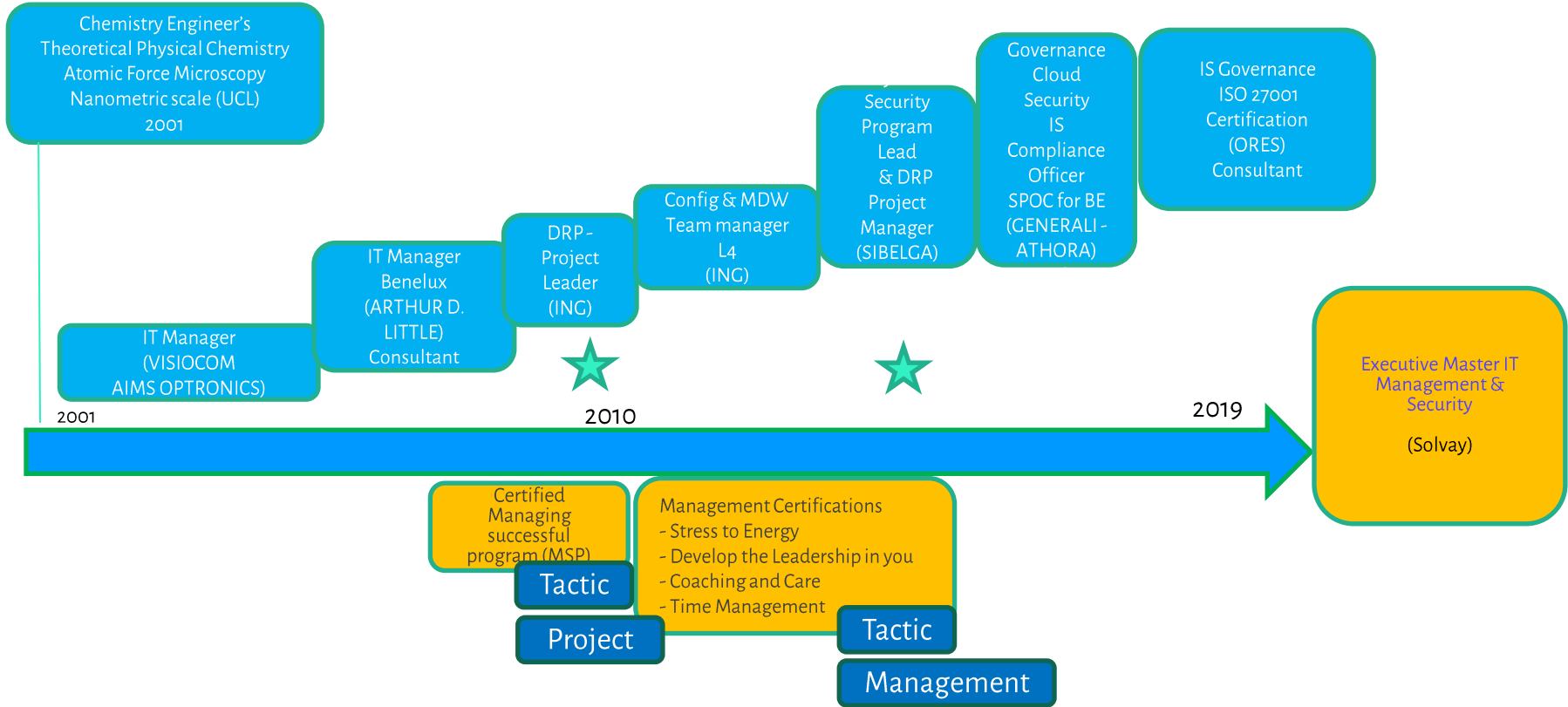


Compaq Deskpro 386
12-18 years old –
1987-1993



Self made computer
SCUSI HDD + DVDRW +
Thermo pasta - overclocking
1994-2001







IS Governance
ISO 27001 Certification
(ORES)
Consultant

Certified ITIL v3 (2019)

Senior BC Leader Digital
Cyber Security
(AGORIA)

2019

2020

2021

2022

GDPR Executive
programme
(Q4 2018)
(Solvay)

Strategic

Executive Master IT Management & Security
IT Security and IT Management (2019)

Strategic

Executive Master IT Management & Security
IT Governance and IT Business (2020)

Strategic

Boot Camp CSX
ISACA (10/2018)

Ops

Certified ITIL v3
(2019)

Tactic

Boot Camp CISSP
— ISC2 (02/2020)

STO

Certified COBIT
2019 Foundations
ISACA (2020)

Strategic

Boot Camp CCISO
EC-council
(04/2021)

Strategic

Certified Data
Privacy Solutions
Engineer
ISACA (2021)

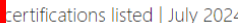
Tactic

THE WORLD OF SECURITY CERTIFICATIONS....

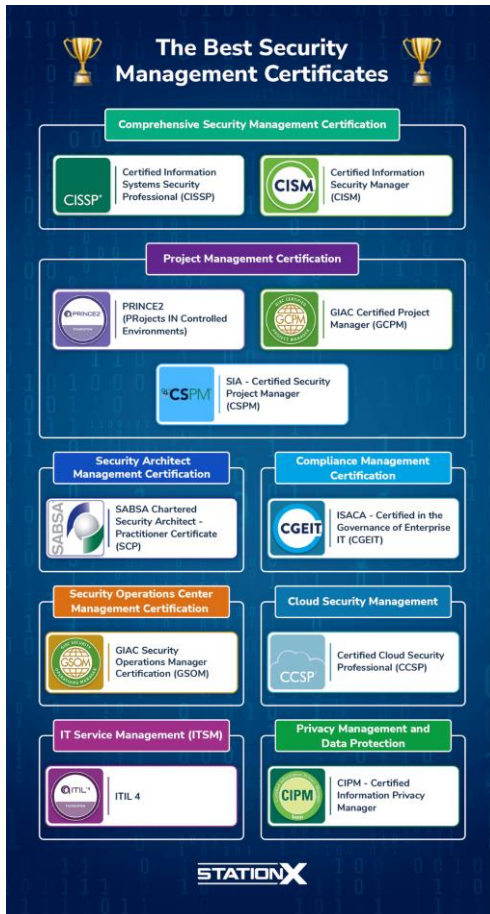
HOW MANY EXISTING CS CERTIFICATION YOU ESTIMATE?

- 0-50
- 50-100
- 100-200
- 250-500
- 500+

Communication and



100



The BEST ? Based on which criterias ?
BUT Indeed they are well known

Overview of certifications

- Here are some organizations that offer certifications that are well-known and highly respected in the cybersecurity space:



[Cybersecurity Certifications](#)[Current Offers](#)

ISC2 CERTIFICATIONS

[Find Your Certification](#)[Register for Exam](#)[Exam Process](#)[Application &
Endorsement](#)[Exam Pricing](#)[Exam Languages](#)

CC

Entry-Level Cybersecurity



SSCP

Security Administrator



CISSP

Leadership & Operations



CCSP

Cloud Security



CGRC

Governance, Risk and
Compliance

CSSLP

Secure Software Development



ISSAP

Security Architecture



ISSEP

Security Engineering



ISSMP

Security Management



The “Holy grale” of Cybersecurity Certification



Training Roadmap

The largest and most trusted source of cyber security training, certification, and research in the world

SANS

GIAC
CERTIFICATIONS

CORE

New to cyber security?

SEC 301
Intro to Information Security

ISC Certification - Information Security Fundamentals

1A You are experienced in technology, but need to learn hands-on, essential security skills and techniques

Core Security Techniques Defend & Maintain

The defence-in-depth techniques taught in SEC401 are essential for every security professional. SEC504 provides additional "offence" knowledge, teaching defence specialists how attacks occur and how to respond. Students with existing core defence skills could begin their training journey with SEC504.

SEC 401
Security Essentials Bootcamp Style

ISC-C - Security Essentials

SEC 504
Hacker Tools, Techniques, Exploits, and Incident Handling

ISC-H - Certified Incident Handler

SEC 308
Digital Forensics Essentials

1B You will be responsible for managing security teams or implementations, but do not require hands-on skills

Security Management

MGT 512
SANS Security Leadership Essentials For Managers (with Knowledge Compression™)

ISC-L - Security Leadership

SEC 566
Implementing and Auditing the Critical Security Controls - In-Depth

ISC-C - Critical Controls

INTERMEDIATE

2 You are experienced in security, preparing for a specialised job role or focus

Security Monitoring & Detection

SEC 503
Intrusion Detection In-Depth

ISC-A - Certified Intrusion Analyst

SEC 511
Continuous Monitoring and Security Operations

ISC-M - Continuation Monitoring

Penetration Testing and Vulnerability Analysis

SEC 460
Enterprise Threat and Vulnerability Assessment

SEC 542
Web App Penetration Testing and Ethical Hacking

OWASP - Web Application Penetration Tester

SEC 560
Network Penetration Testing and Ethical Hacking

ISC-N - Penetration Tester

Incident Response and Enterprise Forensics

FOR 500
Windows Forensics Analysis

ISC-F - Windows Forensics

FOR 572
Advanced Network Forensics and Analysis

ISC-NF - Network Forensic Analyst

FOR 508
Advanced Digital Forensics, Incident Response, and Threat Hunting

ISC-A - Forensic Analyst

Security Management

MGT 414
SANS Training Program for CISSP® Certification

ISC-P - Information Security Professional

ADVANCED/SPECIALISED

3 You are a candidate for specialised or advanced training

SANS' comprehensive curriculum enables professionals to deepen their technical skills in key practice areas. It also directly addresses software developers, industrial control engineers, and non-technical personnel in management, legal, and audit.

Cyber Defence Operations

SEC 450 Blue Team Fundamentals: Security Operations and Analysis
SEC 487 Open-Source Intelligence Gathering (OSINT) and Analysis

ISC-O - Open Source Intelligence

SEC 501 Advanced Security Essentials Enterprise Defender - GCED

SEC 505 Securing Windows and PowerShell Automation

ISC-W - Windows Security

SEC 506 Securing Linux/Unix - GCUX

SEC 530 Defensible Security Architecture - GDSA

SEC 555 SIEM with Tactical Analytics - GCDA

SEC 566 Implementing and Auditing the Critical Security Controls - In-Depth - GCCC

SEC 599 Defeating Advanced Adversaries - Implementing Kill Chain Defences - GCAT

Digital Forensics & Incident Response

FOR 498 Battlefield Forensics & Data Acquisition - GBFA

FOR 518 Mac Forensic Analysis

FOR 526 Memory Forensics In-Depth

FOR 578 Cyber Threat Intelligence - GCTI

FOR 585 Advanced Smartphone Forensics - GASF

FOR 610 Reverse-Engineering Malware: Malware Analysis Tools and Techniques - GREM

Security Management

MGT 514 IT Security Strategic Planning, Policy and Leadership - GSTPE

MGT 516 Managing Security Vulnerabilities: Enterprise and Cloud

MGT 525 IT Project Management, Effective Communication, & PMP® Exam Prep - GCPM

Industrial Control Systems Security

ICS 410 ICS/SCADA Security Essentials - GCSP

ICS 456 Essentials for MERC Critical Infrastructure Protection - GCIPT

ICS 515 ICS Active Defence and Incident Response - GRID

ICS 612 ICS Cyber Security In-Depth

Penetration Testing and Ethical Hacking

SEC 562 CyberCity Hands-on Kinetic Cyber Range Exercise

SEC 573 Python for Penetration Testers - GPIC

SEC 575 Mobile Device Security and Ethical Hacking - GMDS

SEC 617 Wireless Ethical Hacking, Penetration Testing, and Defences - GWIN

SEC 642 Advanced Web App Penetration Testing and Ethical Hacking

SEC 660 Advanced Penetration Testing, Exploit Writing, and Ethical Hacking - GPPN

SEC 699 Purple Team Tactics - Adversary Emulation for Breach Prevention & Detection

SEC 760 Advanced Exploit Development for Penetration Testers

Cloud Security

SEC 488 Cloud Security Essentials

SEC 522 Defending Web Applications Security Essentials - GWEPS

SEC 540 Cloud Security and DevOps Automation

SEC 543 Secure DevOps: A Practical Introduction

SEC 545 Cloud Security Architecture and Operations

SEC 588 Cloud Penetration Testing

Audit / Legal

AUD 507 Auditing & Monitoring Networks, Perimeters & Systems - GDSN

LEG 523 Law of Data Security & Investigations - GLID

GIAC
CERTIFICATIONS



How to Earn a Portfolio Certification

Create a unique portfolio of credentials by focusing where you want.

Choose any of GIAC's 40+ Practitioner Certifications like GSEC, GCIH, GCFA and GPEN.

Choose any of GIAC's Applied Knowledge Certifications like GX-CS, GX-IA, and GX-IH.



DIGITAL BADGES

ANNOUNCING GIAC'S NEW DIGITAL BADGE PROGRAM!

TO LEARN MORE ABOUT THIS ONE-CLICK VERIFICATION,
DIGITAL REPRESENTATION OF YOUR GIAC CERTIFICATION,
VISIT THE LINK IN THIS POST!



<https://www.giac.org/get-certified/giac-portfolio-certifications/?msc=main-nav>



<https://www.isaca.org/credentialing/credentialing-badges>



EC-Council

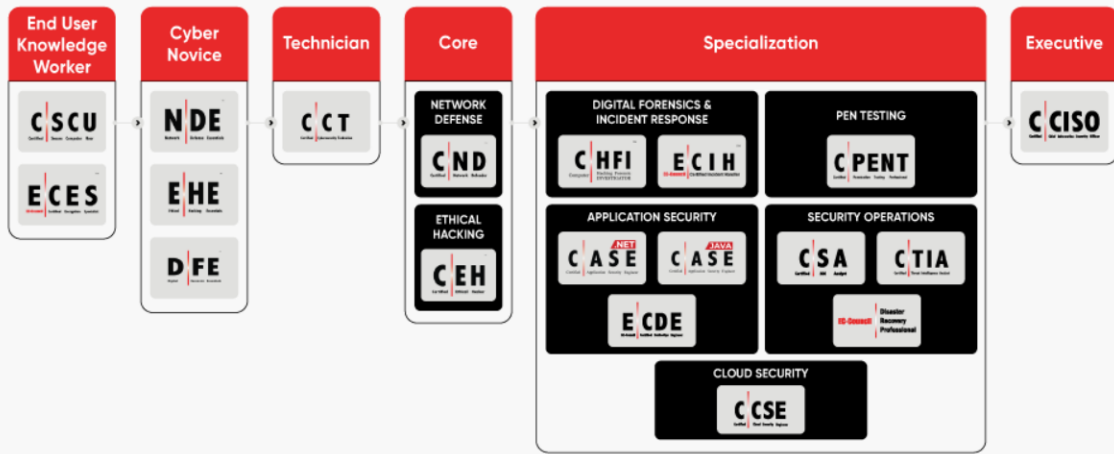


Filter By Career Track

- ☐ Application Security
- ☐ Digital Forensic
- ☐ Incident Handling And Response
- ☐ Network Defense and Operation
- ☐ Vulnerability assessment and penetration testing

Our widely recognized certification credentials

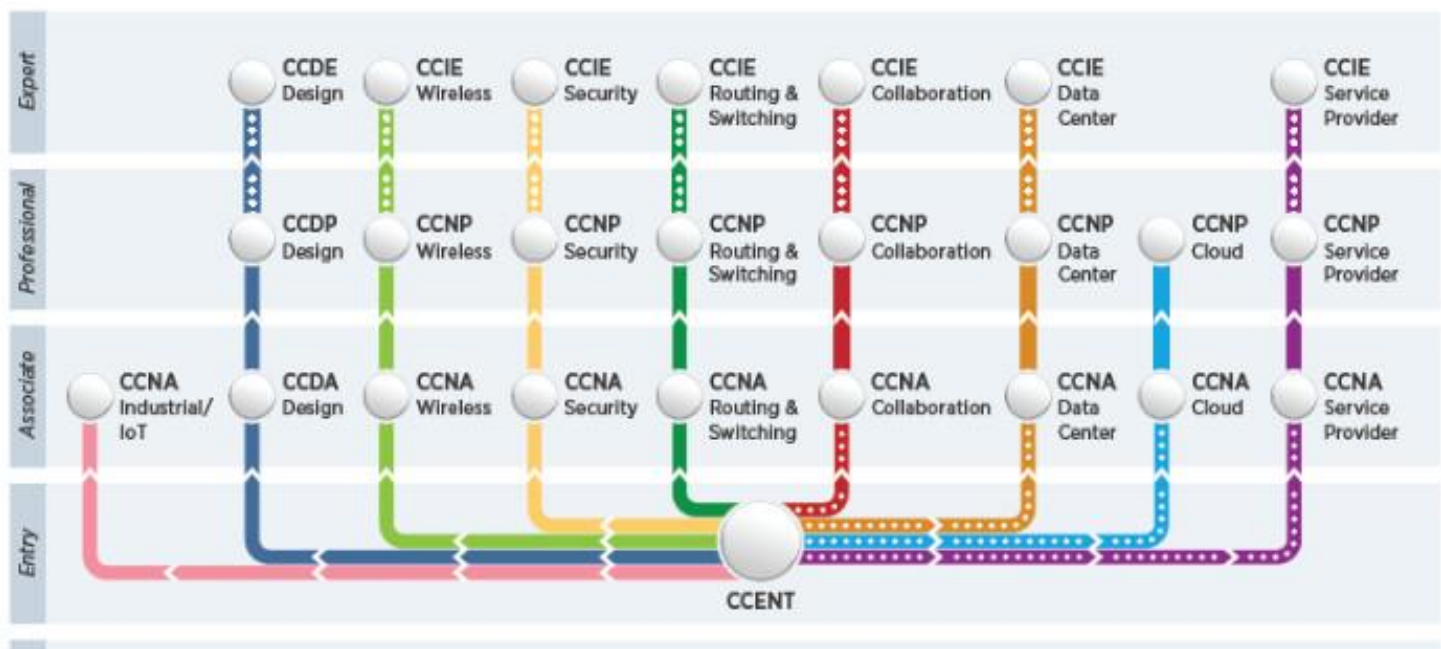
Supporting certification resources available individually or in a track sequence.





Global Knowledge.

Cisco Career Certification Tracks



<https://www.netacad.com/catalogs/learn>

NetAcad

Legacy NetAcad

Explore

Search for courses, articles and resources

Learner

Learning Catalog

Educator Resources

GOALS

Take a free course

Get certified

Learn with an academy

Get job ready

SUBJECT AREAS

Cybersecurity

Networking

AI & Data Science

Programming

Information Technology

Digital Literacy

Professional Skills

Sustainability

Cisco

Browse learning catalog

TAKE A FREE COURSE

Learn topics like networking, cybersecurity, and programming through courses backed by learning science and Cisco expertise - and prepare for certifications and job-ready skills set you up to work anywhere.

Course | Self-paced, Instructor-led

Introduction to Cybersecurity

Explore the exciting field of cybersecurity and why cybersecurity is a future-proof career.

6,954,827 already enrolled

Course | Self-paced

Introduction to IoT and Digital Transformation

Billions of devices connect to the network every day. Learn how IoT is digitally transforming the world and opening up exciting...

266,745 already enrolled

Course | Self-paced, Instructor-led

Networking Basics

Start learning the basics of computer networking and discover how networks operate.

758,383 already enrolled

View all courses

Rik Bleeker

Corporate Social Responsibility

0:14 / 3:47

Rik Bleeker vertelt hoe het NetAcad programma helpt de IT Skills Gap te verkleinen

<https://www.youtube.com/watch?v=846N6vOjdUw>

communication, teamwork, and adaptability to thrive in today's collaborative environments.

Course | Self-paced, Instructor-led

Discovering Entrepreneurship

Build entrepreneurial skills and develop a solution-oriented approach to problem solving through real-world examples an...

Course | Self-paced, Instructor-led

English for IT 1

A course that teaches the English language in a specific IT context at the "B2" proficiency level which is a basic...

25



Core Skills Certifications



Infrastructure Certifications



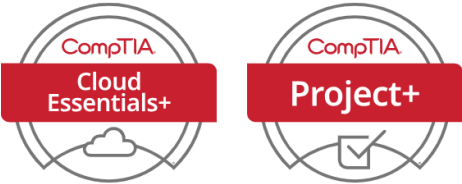
Cybersecurity Certifications



Data & Analytics



Additional Professional Certifications



Figures on the market

CERTIFICATION

NUMBER CERTIFIED

CompTIA Security+	265,992
Certified Information Systems Security Professional (CISSP)	91,765
Global Information Assurance Certification (GIAC)	46,318
Certified Information Systems Auditor (CISA)	35,812
Certified Information Security Officer	20,300
Certified Information Privacy Professional (CIPP)	13,652

This chart shows the number of professionals that hold each type of cybersecurity certification according to 2024 Cyberseek data.

Nearly 6 in 10

IT jobs are cyber-enabled, meaning cybersecurity is part of the job description



Source: Burning Glass | Recruiting Watchers for the Virtual Walls | The State of Cybersecurity Hiring June 2019

cybersecurityguide.org



59 percent

Cybersecurity positions that require a least one certification

Source: Burning Glass | Recruiting Watchers for the Virtual Walls | The State of Cybersecurity Hiring June 2019

cybersecurityguide.org

CERTIFICATION

JOB OPENINGS BY CERT

Certified Information Systems Security Professional (CISSP)	66,011
CompTIA Security+	63,345
Certified Information Systems Auditor (CISA)	42,927
Global Information Assurance Certification (GIAC)	34,092
Certified Information Security Manager (CISM)	31,585
Certified Information Privacy Professional (CIPP)	4,871

This chart shows the number of job postings that mention specific cybersecurity certifications according to 2024 Cyberseek data.

Cyber Security is for geek ?

- “you don’t need to have technological knowledge for a cyber Career”
- YES and NO !
- I would say “Cyber Security is “not” only technical ?”



Adobe stock freepik member



freepik

The dimensions of a certification



The dimensions of a certification

- Industry levels
 - Industry verticality
 - Personal Level of CS experience
 - IT domains (iso 2700x / ITIL) – process focus
 - IT vs CS
 - CS IT or CS OT
 - Technology focus

The CS CONTEXT

- At the industry perspective – 3 Layers



KEY TAKE AWAY

- Vision – Goal – Horizons - Programme
- **Governance** (Cobit...)
- **Risks** (Cyber Risk)
- **Compliance** (GDPR / NIS 2.0 / CSA...)

- Project Management
- New Security Controls (**Trust**)

- Process management (CM / IM / PM)
- **Asset management !!!**
- BCP/ DRP (**resilience**)

Which Cyber Security activities are you teaching or educating today ?

Classification: Internal

27

Strategic Level - GRC

STRATEGIC

TACTIC

OPS

- Policy
- Standard
- Procedures
- R&R
- Setup Teams
- Setup Culture

FLASH

RED FLAG

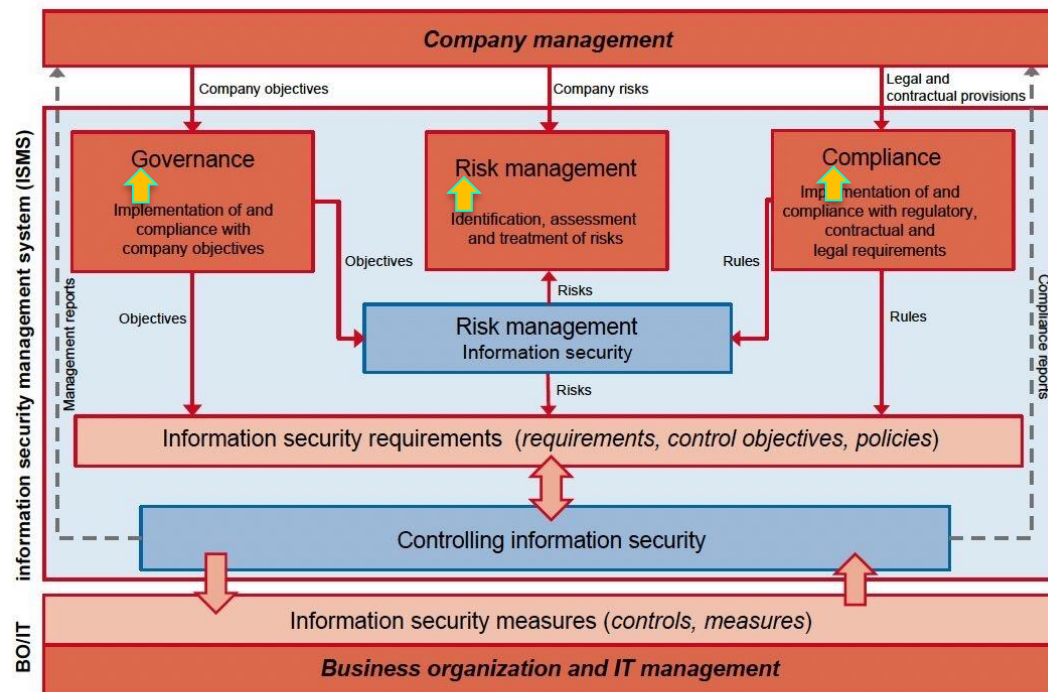
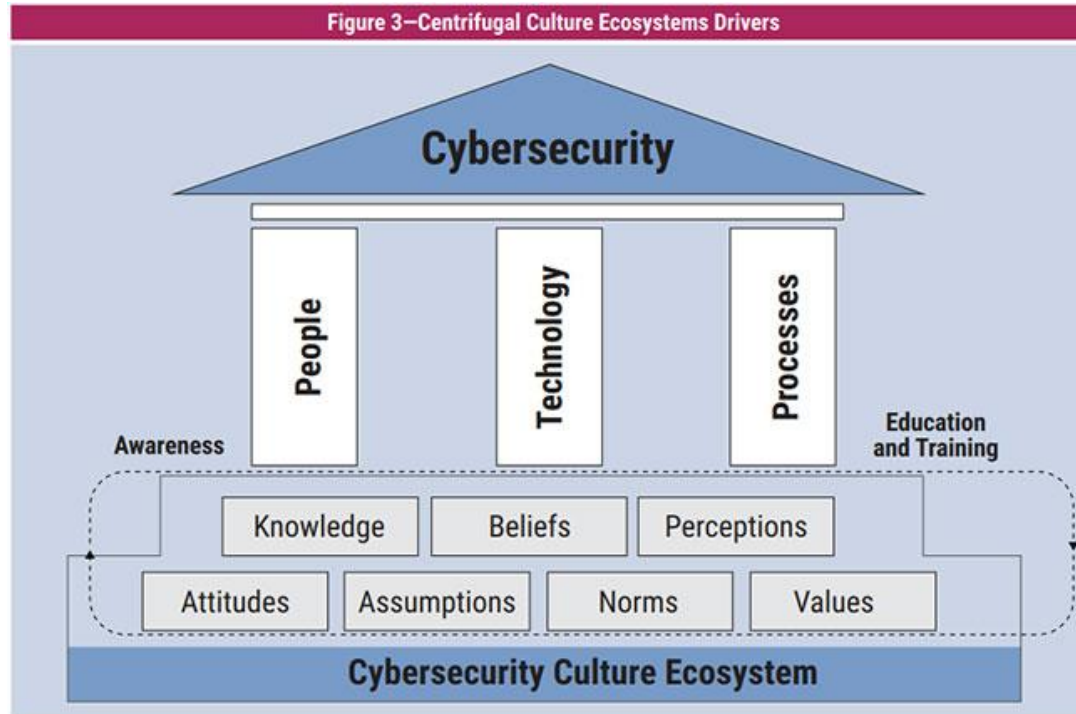


Figure 1: Incorporating the ISMS into corporate control processes²

Cadres (Frameworks): ISACA - Culture

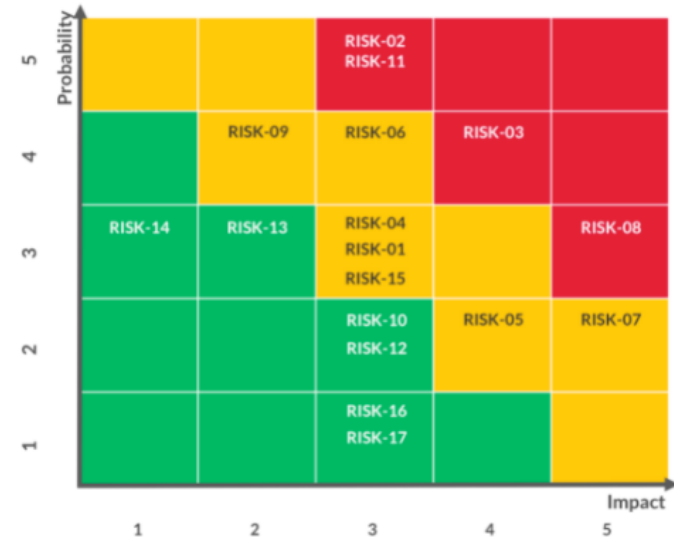


Cybersecurity strategy based on risks



What is a risk? – in a nutshell

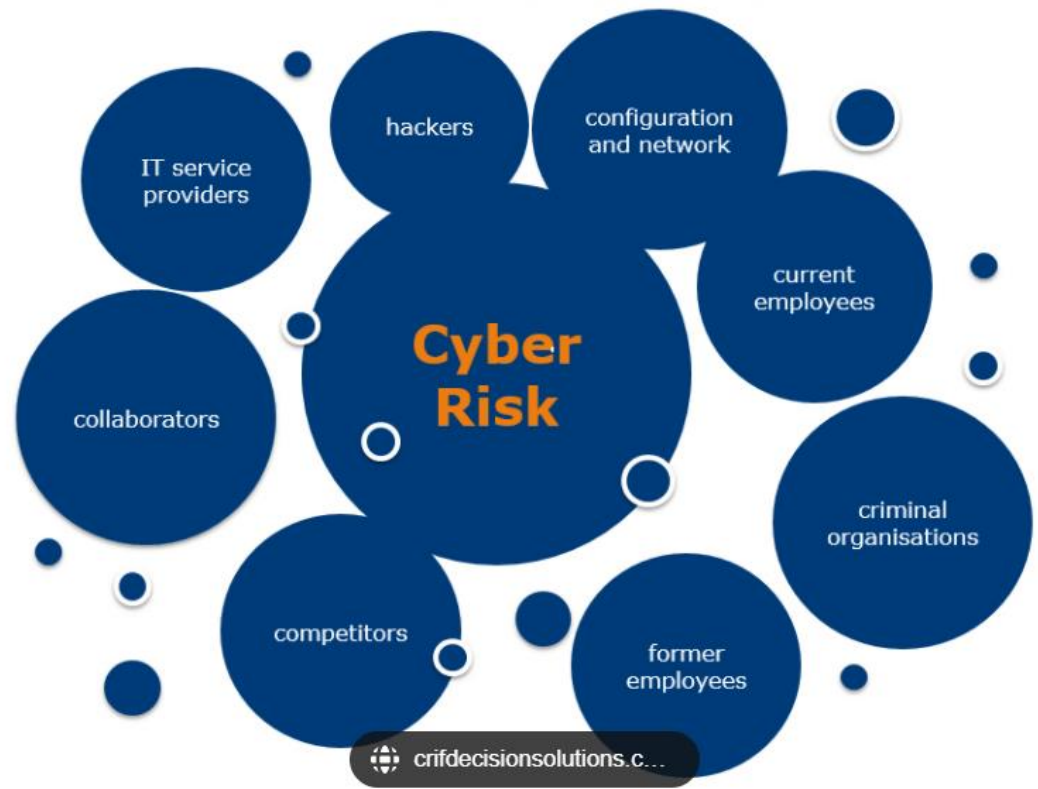
- $R = P \times I$
- “FROC” risks
- Quantitative
- Qualitative
- Risk appetite
- Risk tolerance



If you are not familiar with risks , adress this point quickly

<https://firebrand.training/uk/learn/pmp/course-material/project-risk-management/qualitative-risk-analysis>

Cyber risks ?



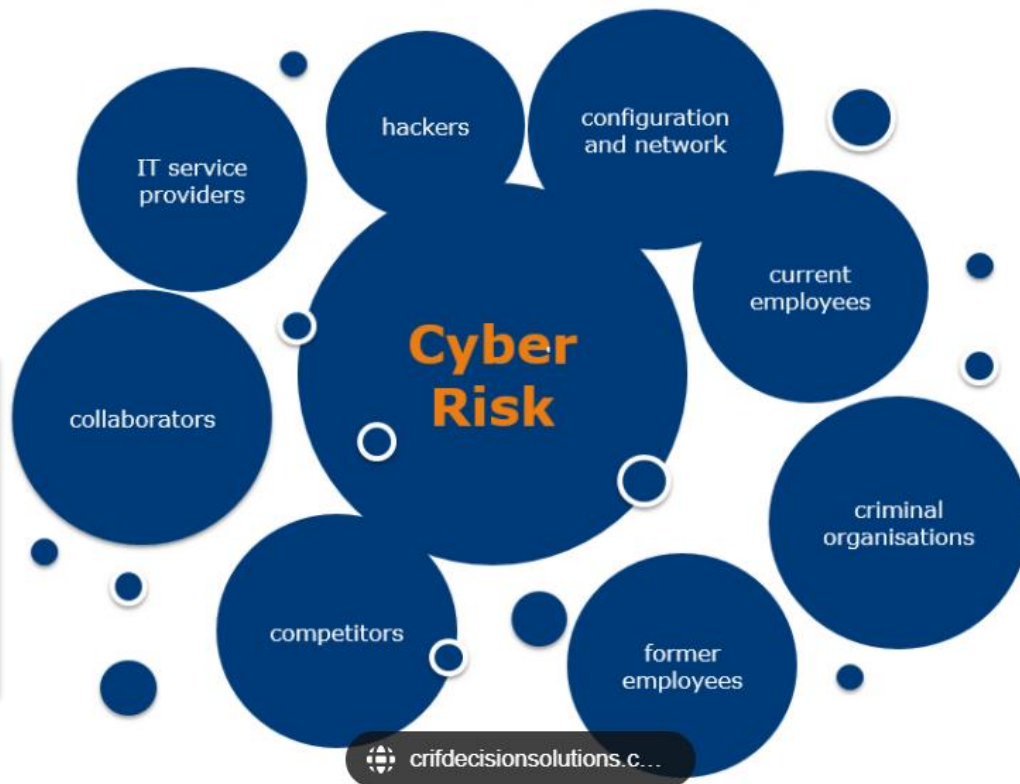
<https://www.at-bay.com/articles/impact-ai-cyber-risk/>

Cyber risks ?



The Impact of AI on Cyber Risk

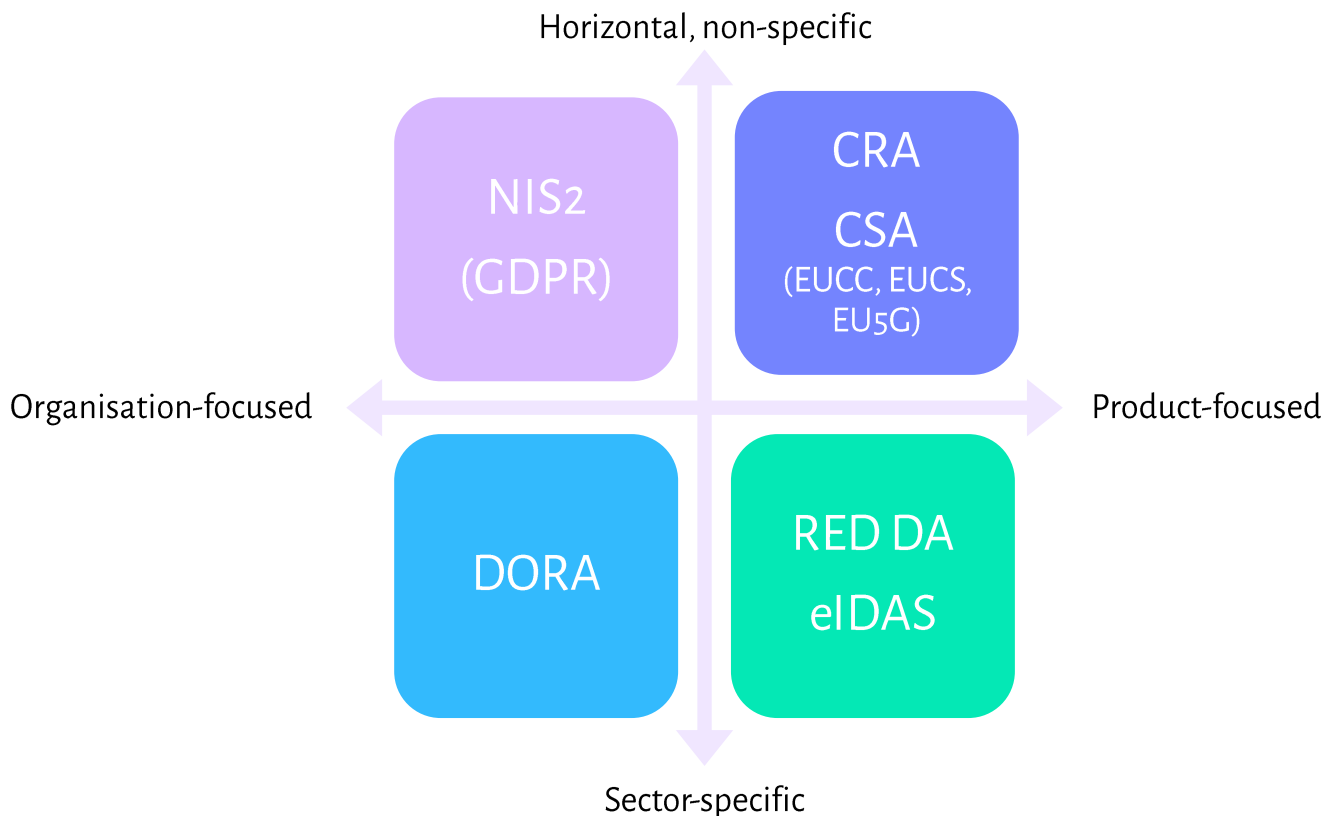
Artificial intelligence has the potential to increase phishing, malware, and at-scale cyber attacks



crifdecisionsolutions.c...

<https://www.at-bay.com/articles/impact-ai-cyber-risk/>

EU Cybersecurity Regulations in a nutshell



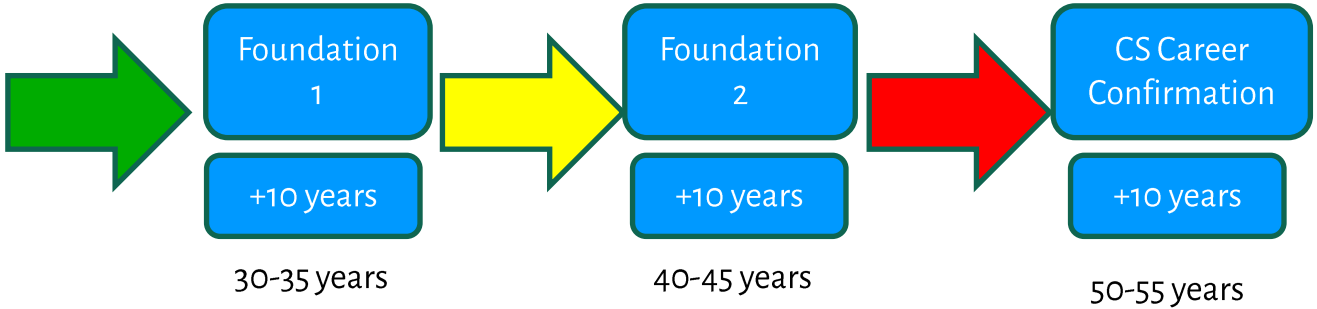
Certification and career path ?

- Understanding the cyber security Path with **Attributes / Dimensions**



Lauren Wheeler

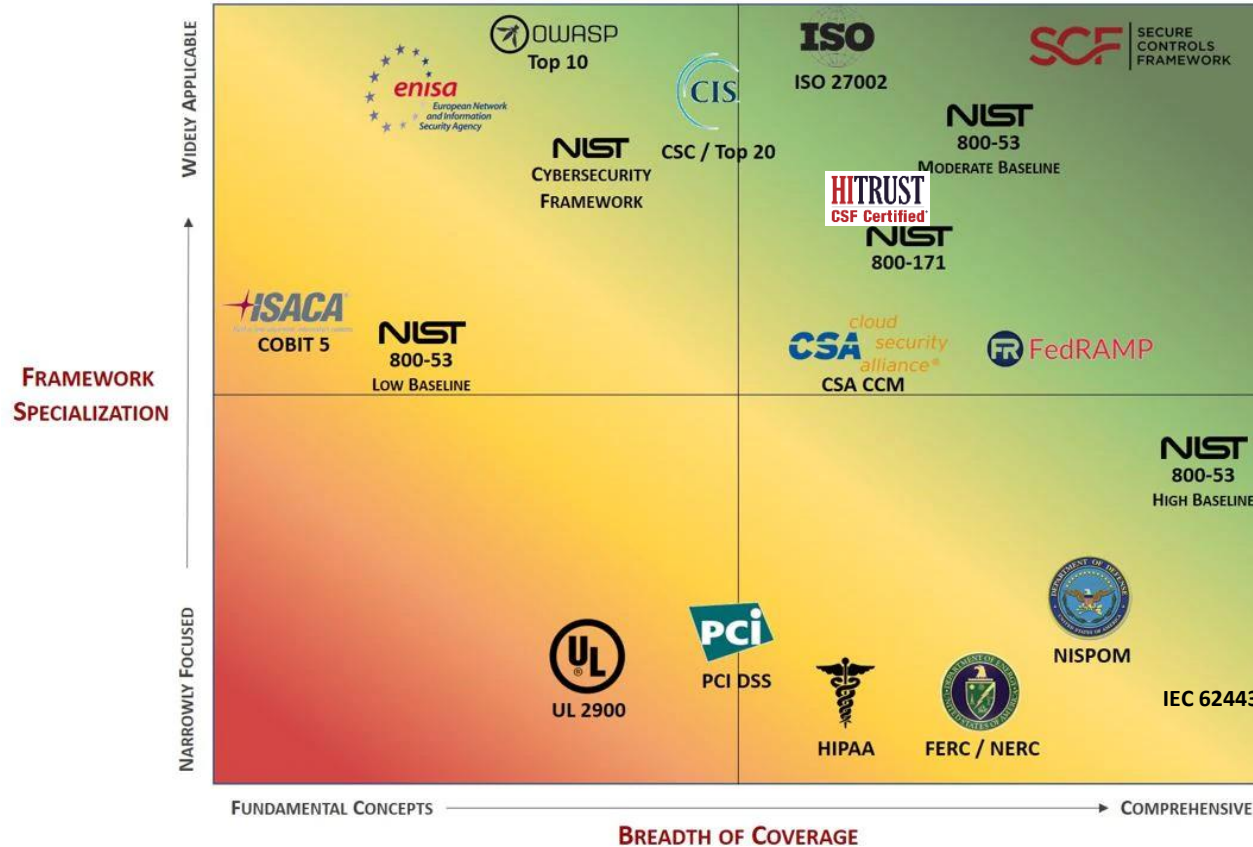
<https://jagwire.augusta.edu/graduation-week-2022-cybersecurity-grad-prepares-to-protect-the-world/>



The dimensions of a certification

- Industry levels
- Industry verticality
- Personal Level of CS experience
- IT domains (iso 2700x / ITIL) – process focus
- IT vs CS
- CS IT or CS OT
- Technology focus

Industry verticality - Frameworks and certifications



FLASH

RED FLAG

ISO 27001

NIST SP 800-53

ITIL

Cobit 2019

→ OT world

The dimensions of a certification

- Industry levels
- Industry verticality
- Personal Level of CS experience
- IT domains (iso 2700x / ITIL) – process focus
- IT vs CS
- CS IT or CS OT
- Technology focus

Personal Level of CS experience (consultancy)

- **Junior** : < 3 years of CS experience
- **Medior** : 3 - 7 years of CS experience
- **Senior** : 7- 15 years of CS experience OR 5+ on a niche
- **Expert** : > 15 years of CS experience OR 10+ on a niche

What is your target ?



European Cybersecurity Skills Framework Role Profiles

The ECSF role profiles document lists the 12 typical cybersecurity professional role profiles along with their identified titles, missions, tasks, skills, knowledge, competences. The main purpose of this framework is to create a common understanding between individuals, employers and providers of learning programmes across EU Member States, making it a valuable tool to bridge the gap between the cybersecurity professional workplace and learning environments.

Published
Language

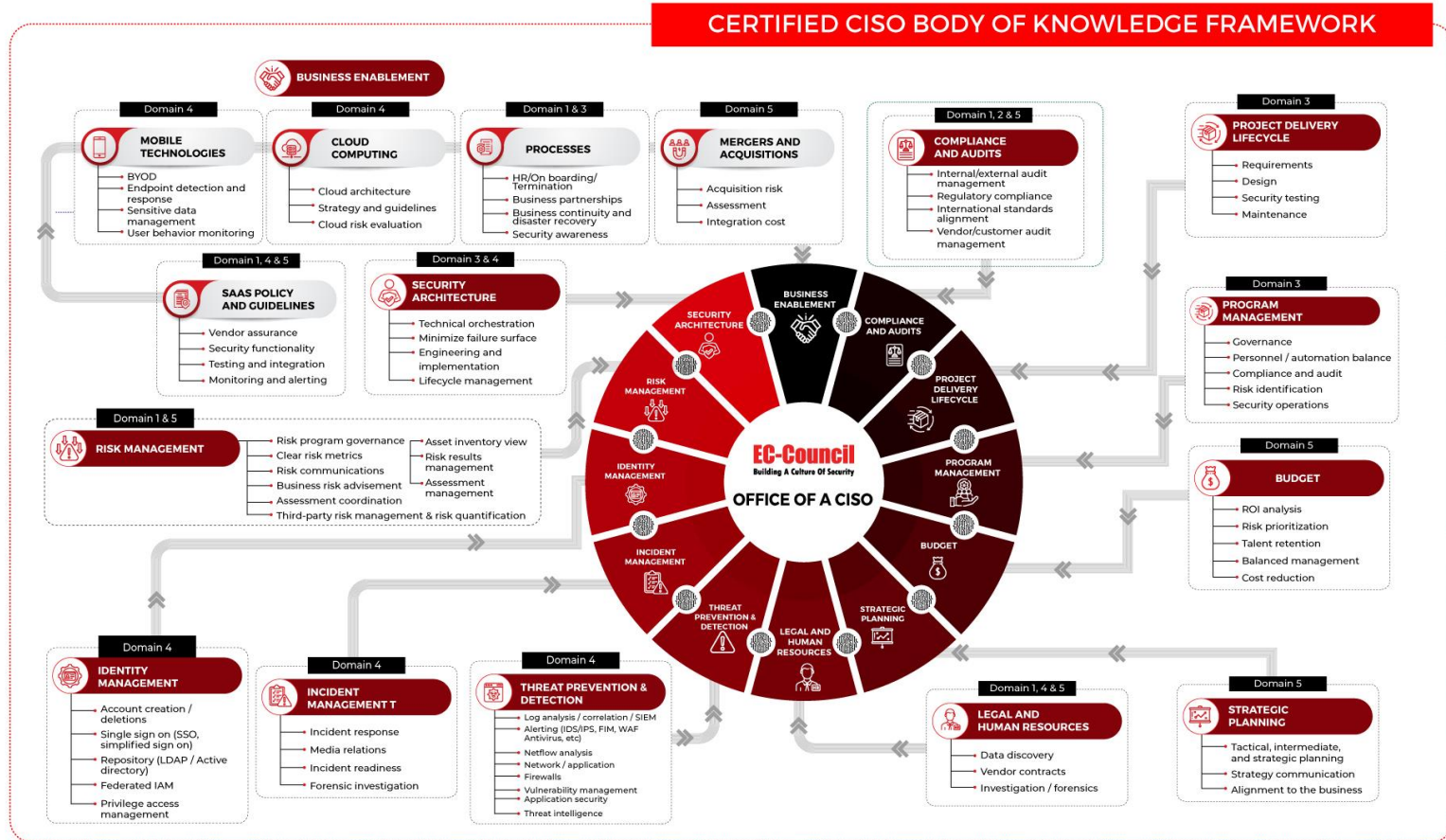
September 19, 2022



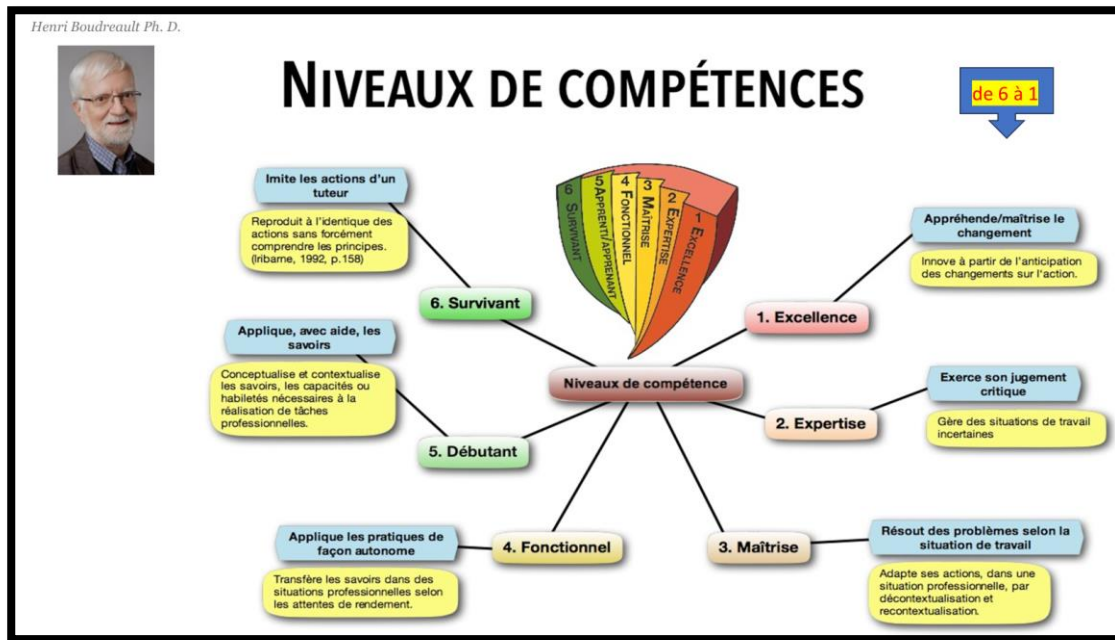
Download

PDF document, 960 KB

CISO?



What is your level of competence ?



(credit) Carl Vastman



SFIA (1) : level 1-7

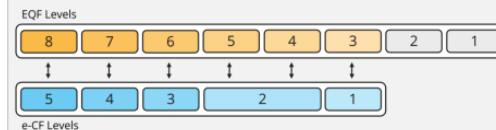
E-CSF (2) level e1-e6

European e-Competence Framework (e-CF),

EQF : level 1-8

The European Qualifications Framework

Figure 14: Relationship between EQF and e-CF levels



(1) <https://sfia-online.org/en>

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

<https://www.enisa.europa.eu/publications/european-cybersecurity-skills-framework-ecsf>

If you don't know ?

Skillsbeam HOME ENTERPRISES DIGITAL SKILLS ASSESSMENT CONTACT US LOGIN Search ...

CYBERSEC PROFILES SKILLS ASSESSMENT
Please select the job role that you wish to assess.

Security

CISO	Cyber Incident Responder	Cyber Legal & Compliance Officer	Cyber Threat Intelligence Specialist	Cybersecurity Architect	Cybersecurity Auditor
Cybersecurity Educator	Cybersecurity Implementer	Cybersecurity Researcher	Cybersecurity Risk Manager	Digital Forensics Investigator	Penetration Tester

SFIA © Based on SFIA Framework

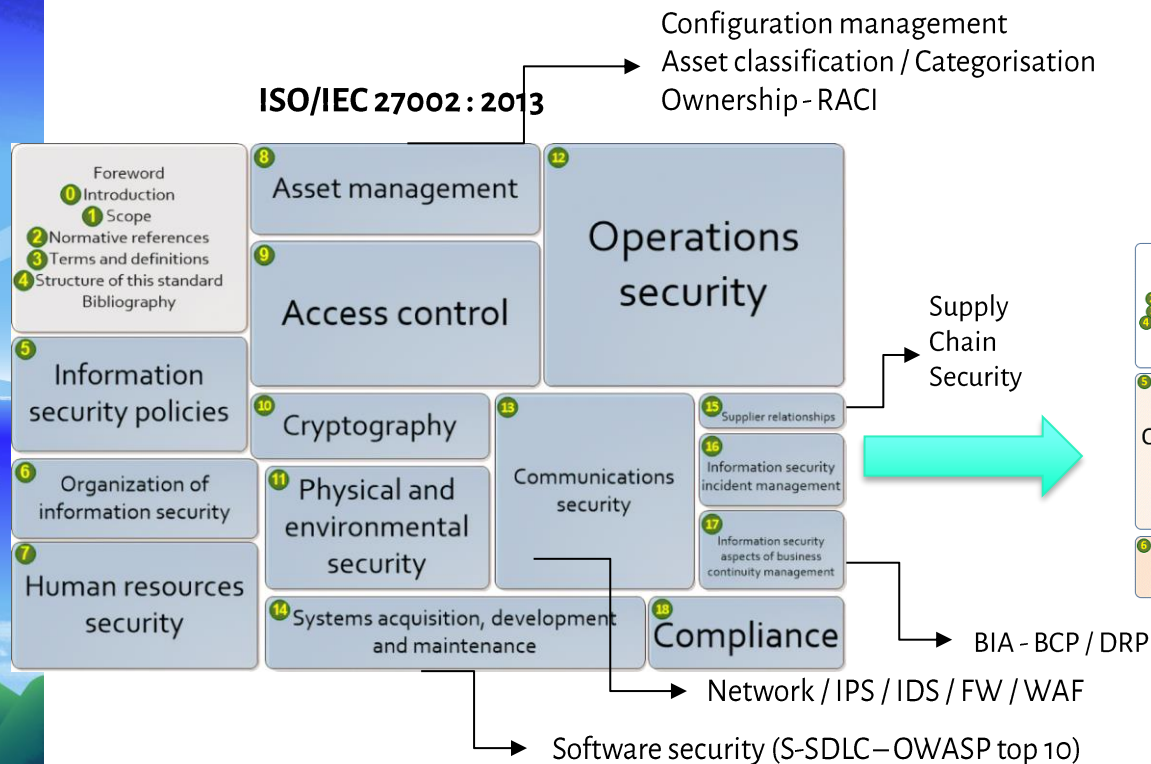
Chartered Institute of Information Security ©
Based on CIISEC Framework

<https://cyber.skillsbeam.io/index.php/sfia-assessment>

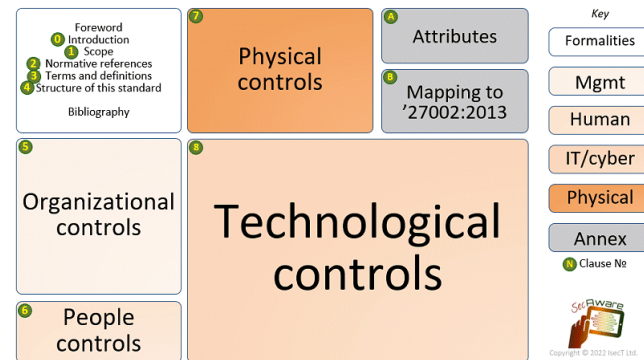
The dimensions of a certification

- Industry levels
- Industry verticality
- Personal Level of CS experience
- IT domains (iso 2700x / ITIL) – process focus
- IT vs CS
- CS IT or CS OT
- Technology focus

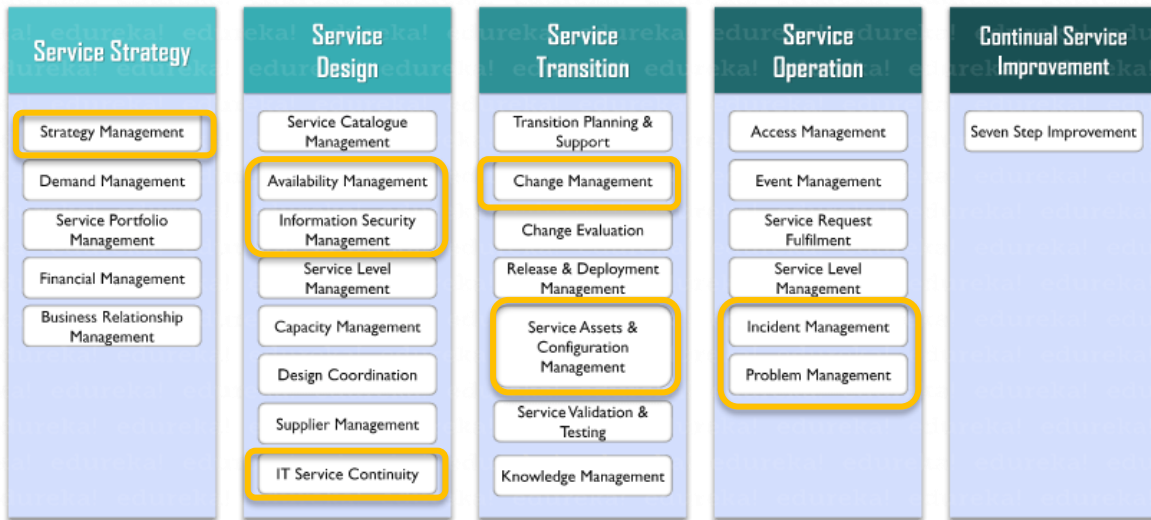
ISO 27002 – Overview- “processes”



ISO/IEC 27002:2022



ITIL v3 (*) illustrate importance of some Cybersecurity **Processes** (PPT)



ITIL® v3 is built on 26 processes which have been segregated into 5 service lifecycle stages. These are:

1. Service Strategy
2. Service Design
3. Service Transition
4. Service Operations
5. Continual Service Improvement (CSI)



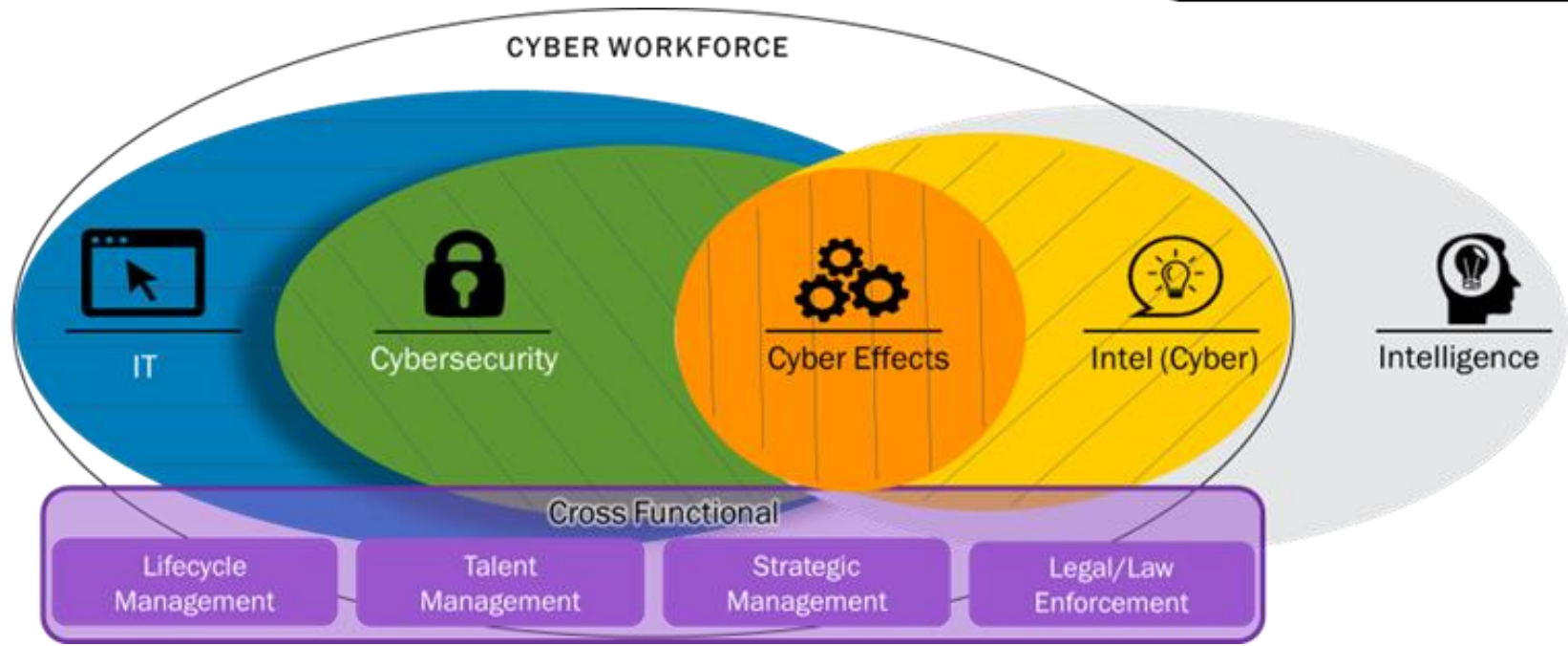
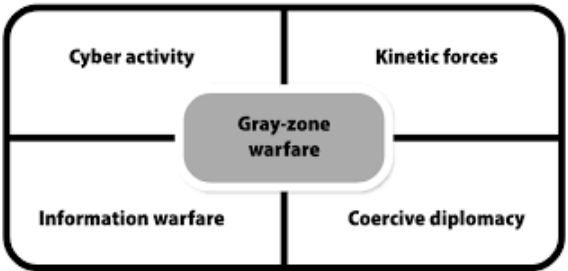
ITIL® is one of the most heavily used ITSM frameworks

(*) v4 is out in 2020

The dimensions of a certification

- Industry levels
- Industry verticality
- Personal Level of CS experience
- IT domains (iso 2700x / ITIL) – process focus
- IT vs CS
- CS IT or CS OT
- Technology focus

The grey/gray zones IT vs CS

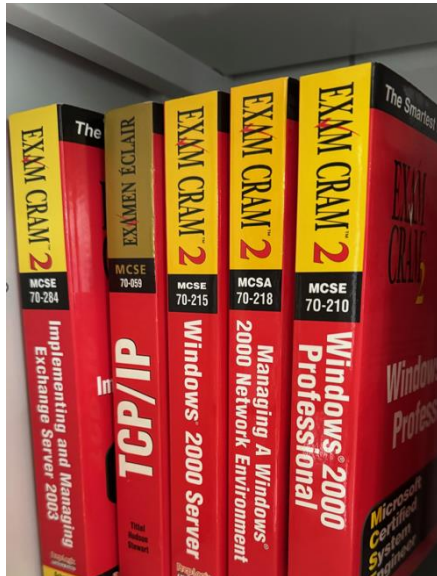


DCWF (defence cyber work force)

IT (Cyberspace)	IT (CYBERSPACE) Database Administrator 421 Enterprise Architect 651	IT (CYBERSPACE) Knowledge Manager 431 Network Operations Specialist 441	IT (CYBERSPACE) Research and Development Specialist 661	IT (CYBERSPACE) System Administrator 451 System Testing & Evaluation Specialist 671 Systems Developer 632	IT (CYBERSPACE) Systems Requirements Planner 641 Technical Support Specialist 411		
	CYBERSECURITY Authorizing Official/ Designating Representative 611 COMSEC Manager 723	CYBERSECURITY Cyber Defense Analyst 511 Cyber Defense Forensics Analyst 212	CYBERSECURITY Cyber Defense Incident Responder 531 Cyber Defense Infrastructure Support Specialist 521	CYBERSECURITY Information Systems Security Developer 631 Information Systems Security Manager 722	CYBERSECURITY Secure Software Assessor 622 Security Architect 652	CYBERSECURITY Security Control Assessor 612	CYBERSECURITY Vulnerability Assessment Analyst 541

<https://dl.dod.cyber.mil/wp-content/uploads/dcwf/ElementsMap/story.html>

IT Certification Roadmap (IT vs CS) example

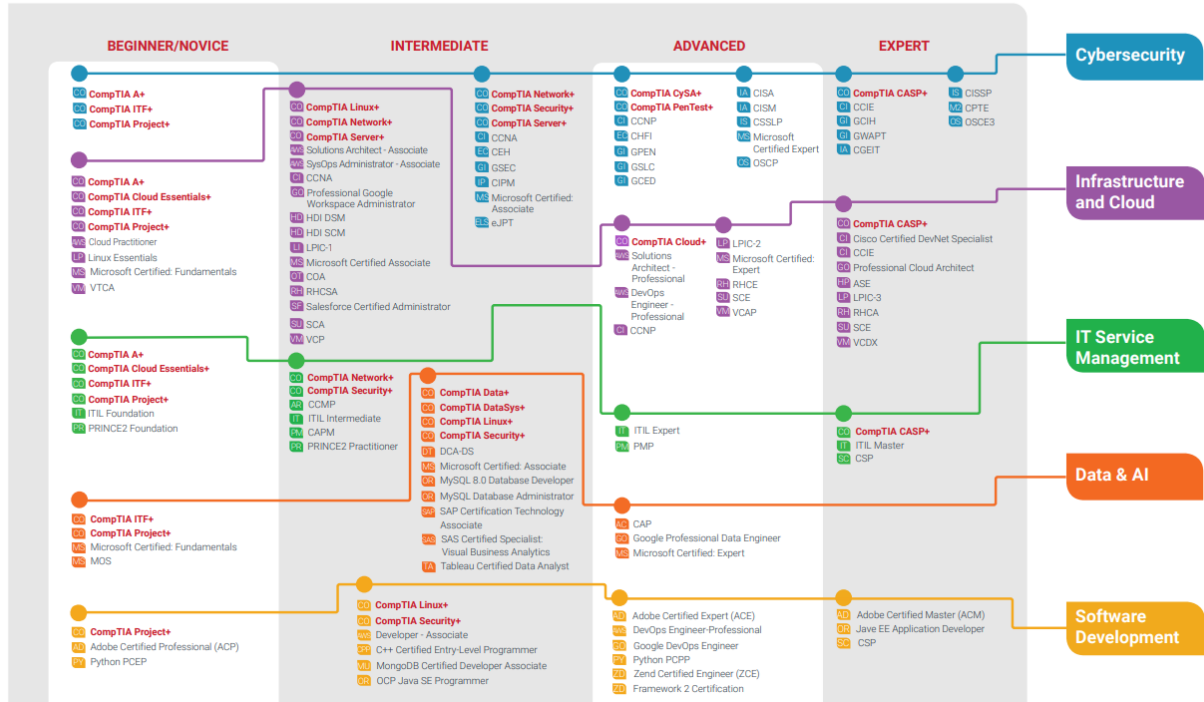


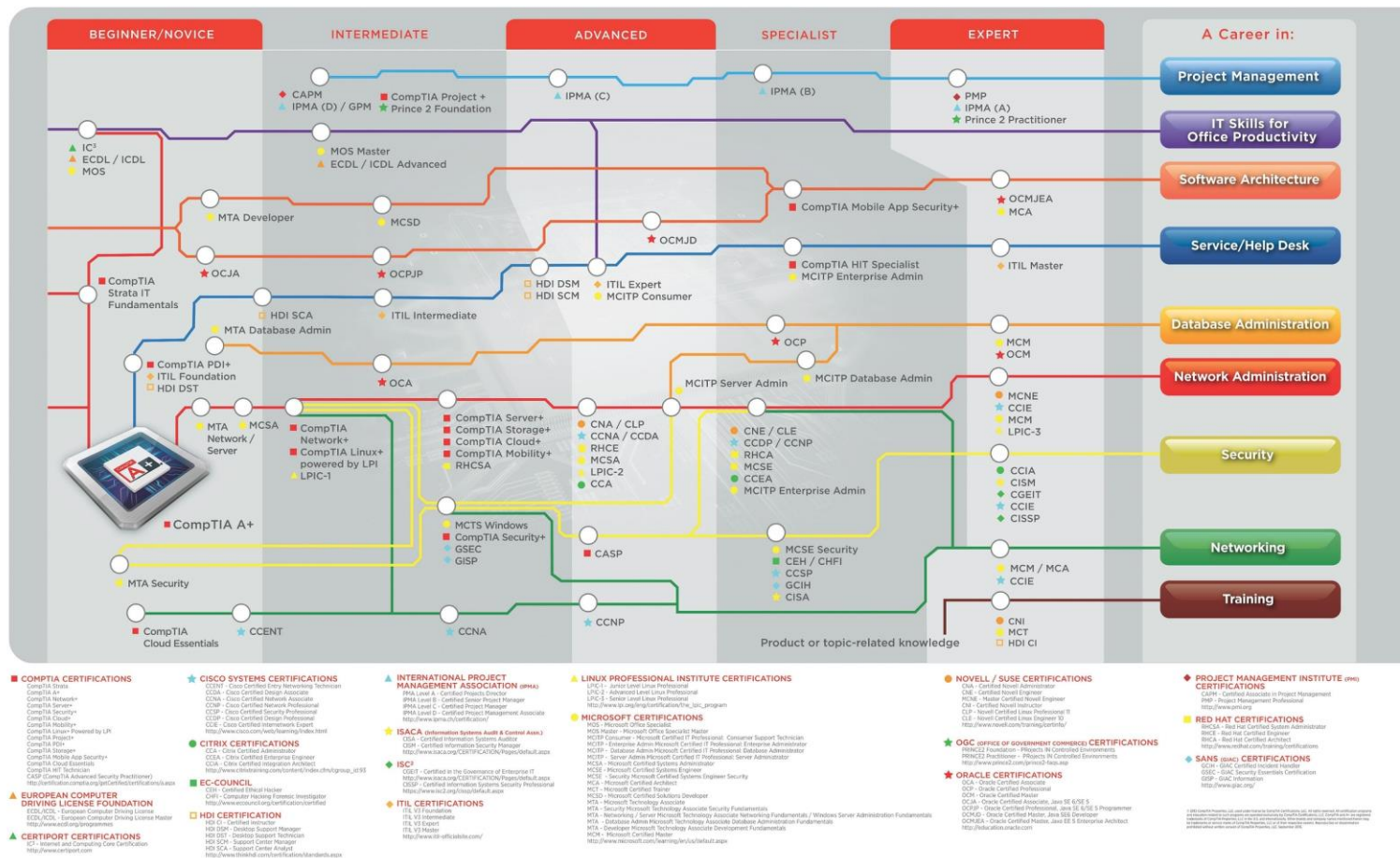
IT Certification Roadmap

Explore the possibilities with the CompTIA Interactive IT Roadmap at:
CompTIA.org/CertsRoadmap

CompTIA

Certifications validate expertise in your chosen career.



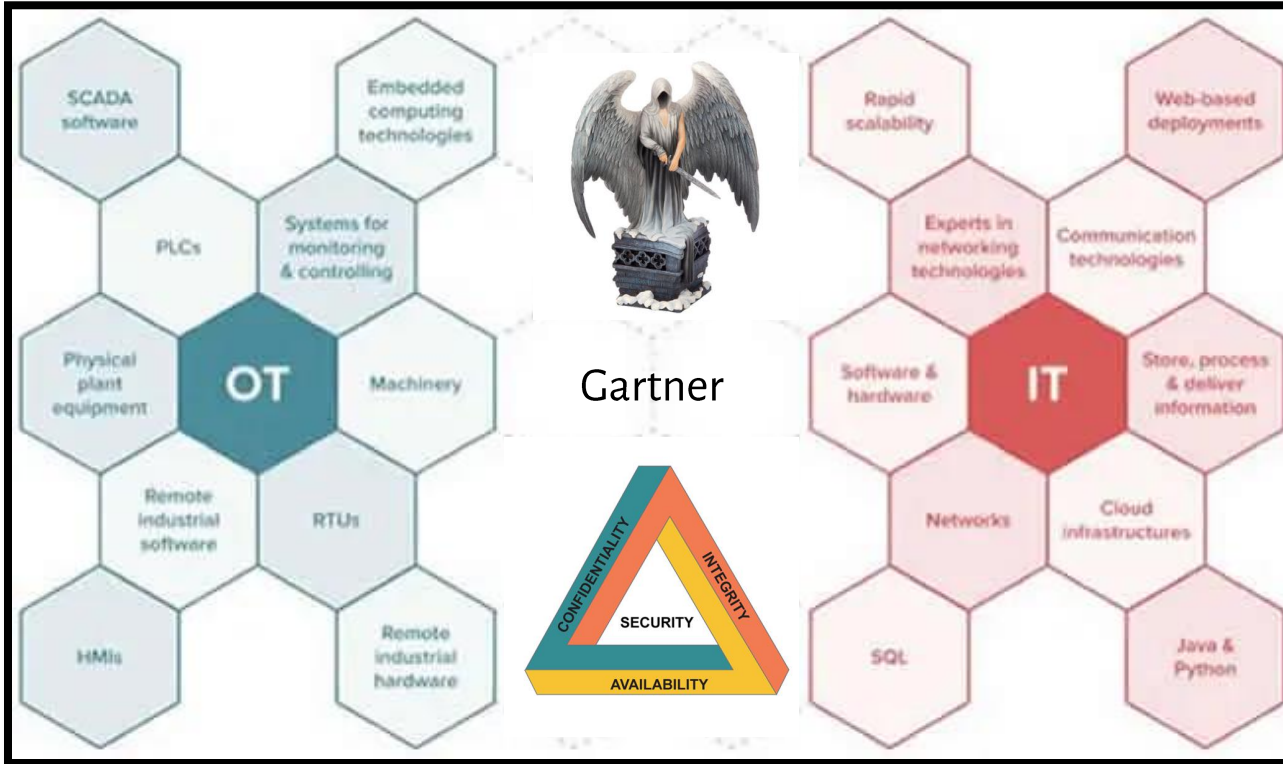




The dimensions of a certification

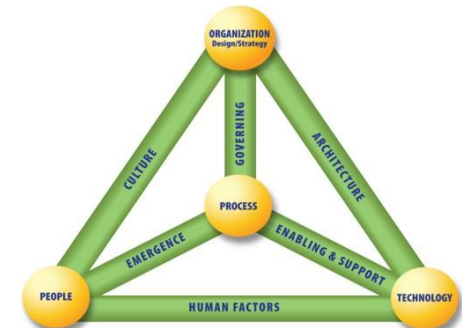
- Industry levels
- Industry verticality
- Personal Level of CS experience
- IT domains (iso 2700x / ITIL) – process focus
- IT vs CS
- CS IT or CS OT
- Technology focus

The Battle field IT / OT



All the means to secure/protect the information at

- People
- Process
- Technology level

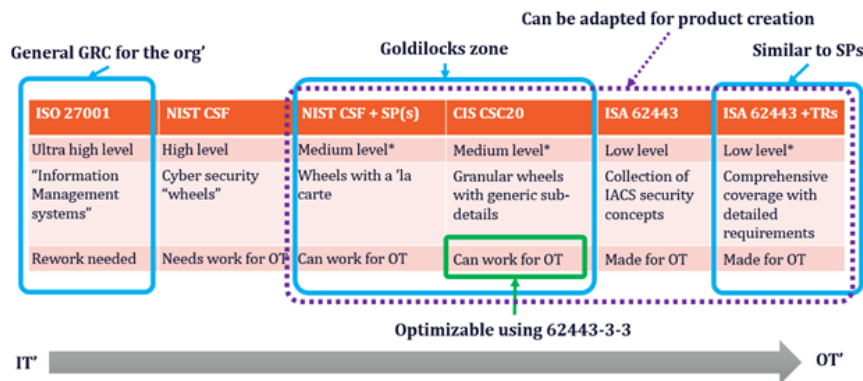


BMIS model

IT/OT World

Blending IEC 62443 with other frameworks and standards

IEC 62443 standards are fully compatible and mostly map directly with other well-known guidance such as the NIST CSF. There can be, however, substantial differences in language and application that require the use of OT-specific overlays and adaptation of IT variations in order to manage exceptions in a converged OT/IT environment. Getting the best of both worlds requires organizations to get a little creative.



How to implement CS activities?

“The 3-legged stool of People-Process-Technology (PPT)”



The dimensions of a certification

- Industry levels
- Industry verticality
- Personal Level of CS experience
- IT domains (iso 2700x / ITIL) – process focus
- IT vs CS
- CS IT or CS OT
- Technology focus

FOCUS ON TECHNOLOGY

Filter

Clear all

Products

Find a product

- ✓ ☐ Azure
- ✓ ☐ Dynamics 365
- ✓ ☐ Microsoft 365
- ✓ ☐ Microsoft Defender
- ✓ ☐ Microsoft Entra
- ☐ Microsoft Fabric
- ✓ ☐ Microsoft Power Platform
- ☐ Office 365
- ✓ ☐ Windows

Search

Certification ✕

74 results

CERTIFICATION

Microsoft 365 Certified: Administrator Expert

ExamMS-102
Microsoft 365 • Administrator • Advanced

⊕ Add

CERTIFICATION

Microsoft 365 Certified: Collaboration Communications Systems Engineer Associate

Microsoft 365 • Administrator • Intermediate

⊕ Add

CERTIFICATION

Microsoft 365 Certified: Endpoint Administrator Associate

Microsoft 365 • Administrator • Intermediate

⊕ Add

CERTIFICATION

CERTIFICATION

CERTIFICATION

Filter

Clear all

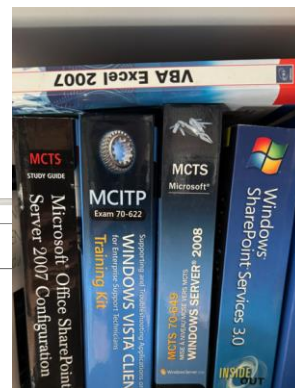
Products

- ✓ ☐ Azure

Search

Security ✕

7 results

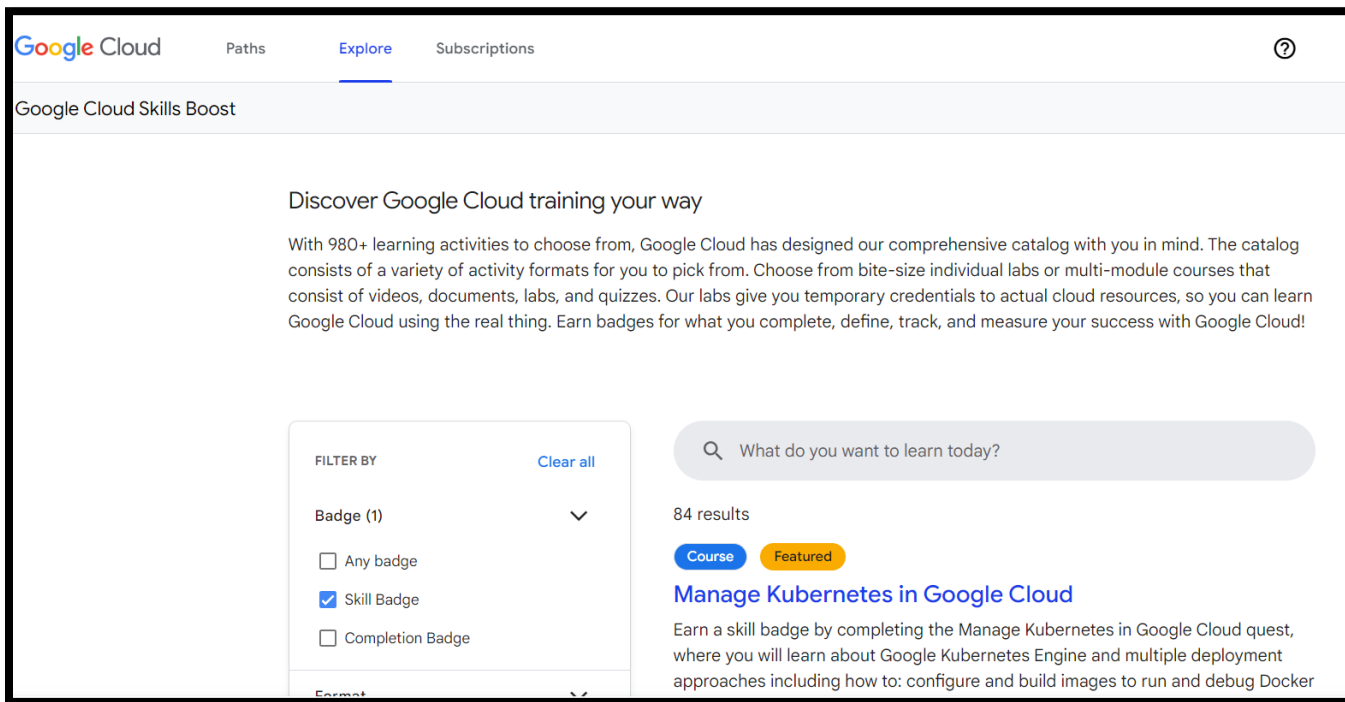


Search

Sort by: Alphabetical (A-Z) ▾

<https://learn.microsoft.com/>

FOCUS ON TECHNOLOGY









The screenshot shows the Google Cloud Skills Boost interface. At the top, there's a navigation bar with 'Google Cloud' logo, 'Paths', 'Explore' (selected), and 'Subscriptions'. A search icon is in the top right. Below the navigation bar is a header 'Google Cloud Skills Boost'. The main content area has the heading 'Discover Google Cloud training your way' followed by a paragraph: 'With 980+ learning activities to choose from, Google Cloud has designed our comprehensive catalog with you in mind. The catalog consists of a variety of activity formats for you to pick from. Choose from bite-size individual labs or multi-module courses that consist of videos, documents, labs, and quizzes. Our labs give you temporary credentials to actual cloud resources, so you can learn Google Cloud using the real thing. Earn badges for what you complete, define, track, and measure your success with Google Cloud!'

Below the text, there's a 'FILTER BY' section on the left with a 'Clear all' link. It shows 'Badge (1)' with a dropdown arrow. Underneath, there are three checkboxes: 'Any badge' (unchecked), 'Skill Badge' (checked), and 'Completion Badge' (unchecked). To the right of the filters is a search bar with the placeholder text 'What do you want to learn today?'. Below the search bar, it says '84 results'. There are two buttons: 'Course' (blue) and 'Featured' (yellow). Below these buttons is the title 'Manage Kubernetes in Google Cloud' in blue. Under the title is a paragraph: 'Earn a skill badge by completing the Manage Kubernetes in Google Cloud quest, where you will learn about Google Kubernetes Engine and multiple deployment approaches including how to: configure and build images to run and debug Docker'.

MIX FOCUS AREA

Find Certifications by Focus Area

GIAC certifications are now organized by focus areas that align with industry trends and needs - making it easier for employers and practitioners to find the certs that will take their security teams to the next level.

 <p>Offensive Operations</p> <p>GIAC's offensive operations certifications cover critical domains and highly specialized usages, ensuring professionals are well-versed in essential offensive abilities.</p> <p>></p>	 <p>Cyber Defense</p> <p>GIAC's cyber defense certifications span the entire defense spectrum and are focused in two areas: cyber defense essentials and blue teaming.</p> <p>></p>	 <p>Cloud Security</p> <p>GIAC's cloud security certifications are designed to help you master the practical steps necessary for defending systems and applications in the cloud against the most dangerous threats.</p> <p>></p>
 <p>Industrial Control Systems</p> <p>GIAC's industrial control systems certifications cover what ICS professionals need to know: how to protect and defend critical industrial systems and respond to incidents that will inevitably occur.</p> <p>></p>	 <p>Digital Forensics & Incident Response</p> <p>GIAC's digital forensics and incident response certifications encompass abilities that DFIR professionals need to succeed, confirming that professionals can detect compromised systems and identify how and when a breach occurred.</p> <p>></p>	 <p>Management, Legal & Audit</p> <p>GIAC's management certifications confirm the practical skills to build and lead security teams, communicate with both technical teams and business leaders, and develop capabilities that strengthen your organization's security posture.</p> <p>></p>

<https://www.giac.org/focus-areas/?msc=main-nav>

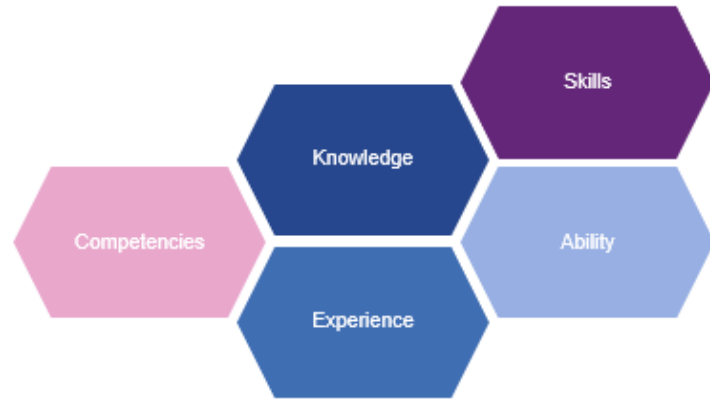
Added Value of a certification



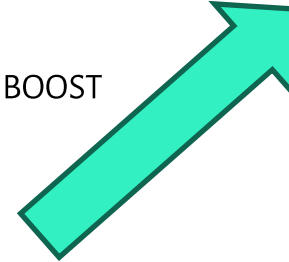
Agenda

- Introduction
 - Value proposition of Cybersecurity
 - Set the scene
 - Demistify the Logical CS world
- Certification and career path ?
 - Foundation blocks
 - Overview of most wellknown worldwide CS Certification bodies.
- The dimensions of a certification
- Added value of a certification
- Key take aways

Added value of a certification ?



BOOST



Added value of a certification ?

- **Junior :**
 - Show to the recruiter the willingness to learn and competitive advantages to be recruited on the market needs
- **Medior :**
 - Increase the credibility / assurance level of expertise
- **Senior :**
 - Confirm the expertise / experience + possibility to increase the competences and skills to an executive/strategic position
- **Expert :**
 - Interlink expertises and experiences with new technology trends / treats and mainly focus on strategic projects and visions
(Ex IA / CYBER / REGULATION..)



Salary Negotiation
Mission selection
!!!! Reputation (*) !!!

Added value of a certification ?

NICCS®

NATIONAL INITIATIVE FOR CYBERSECURITY CAREERS AND STUDIES







Education & Training

Cybersecurity & Career Resources > Interactive Cybersecurity Career Map

Provided by [USAJOBS](#)

154 distinct job openings in the United States across 57 states/territories and 1338 cities

Displaying 1 - 50 rows out of 154 total; page 1 of 4

Title	City	State	Minimum	Maximum	Apply By
 Senior IT Cybersecurity Specialist, CG-2210-14 - 806577700	Washington	District of Columbia	\$153,507	\$250,360	09/09/2024
  Deputy Chief Financial Officer - 806619100	Arlington	Virginia	\$147,649	\$221,900	09/17/2024
 Chief Information Officer / Assistant Director / Supervisory IT Specialist (Policy and Planning) - 806100600	Glynco	Georgia	\$147,649	\$221,900	09/23/2024
 Assistant Inspector General, Technology Services - 803741900	5 cities	5 states and/or territories	\$147,649	\$221,900	09/09/2024
 Acquisition Organization Technical Advisor - 806971000	Fort Meade	Maryland	\$147,649	\$221,900	09/16/2024

<https://niccs.cisa.gov/cybersecurity-career-resources/interactive-cybersecurity-career-map?>

Use case 1 – Junior -> medior

COMMON TRUNK -> Foundation 1

- Follow the CC from ISC2 (1 millions licences free)
- -> foundations
- Google “free cybersecurity certifications”



Join the **SANS Belgium Cybersecurity Training Community**

SANS is the world's largest provider of cybersecurity training. Joining the SANS Cybersecurity Community grants you **FREE** access to cutting-edge cybersecurity training, tools, and resources.

[Join Today](#)

1,000+ Cybersecurity Resources. 100% Free. Forever.

<https://www.sans.org/mlp/be-cybersecurity-training-community/>



Certified in Cybersecurity (CC) Courses

Related topics **IT & Software, IT Certifications**

165,708 Learners | Issued by ISC2 [Learn more](#)

The vendor-neutral CC credential starts newcomers on their path to advanced cybersecurity certifications and for organizations that newly certified team members understand fundamental security principles and operations, net and that they have the skills to meet and exceed performance standards in their beginning roles. All this allows of defense.

Featured course

Many learners enjoyed this highly rated course for its engaging content.

The Complete Certified in Cybersecurity CC course ISC2 2024

Start your Cyber security career today! Take the Complete Certified in Cybersecurity (CC) beginners course ISC2 - 2024

By Thor Pedersen | 590,000+ Enrollments Worldwide and 1 other

Updated **September 2024** | 17.5 total hours - 143 lectures - All Levels

4.6 ★★★★★ (9,270) **Bestseller**

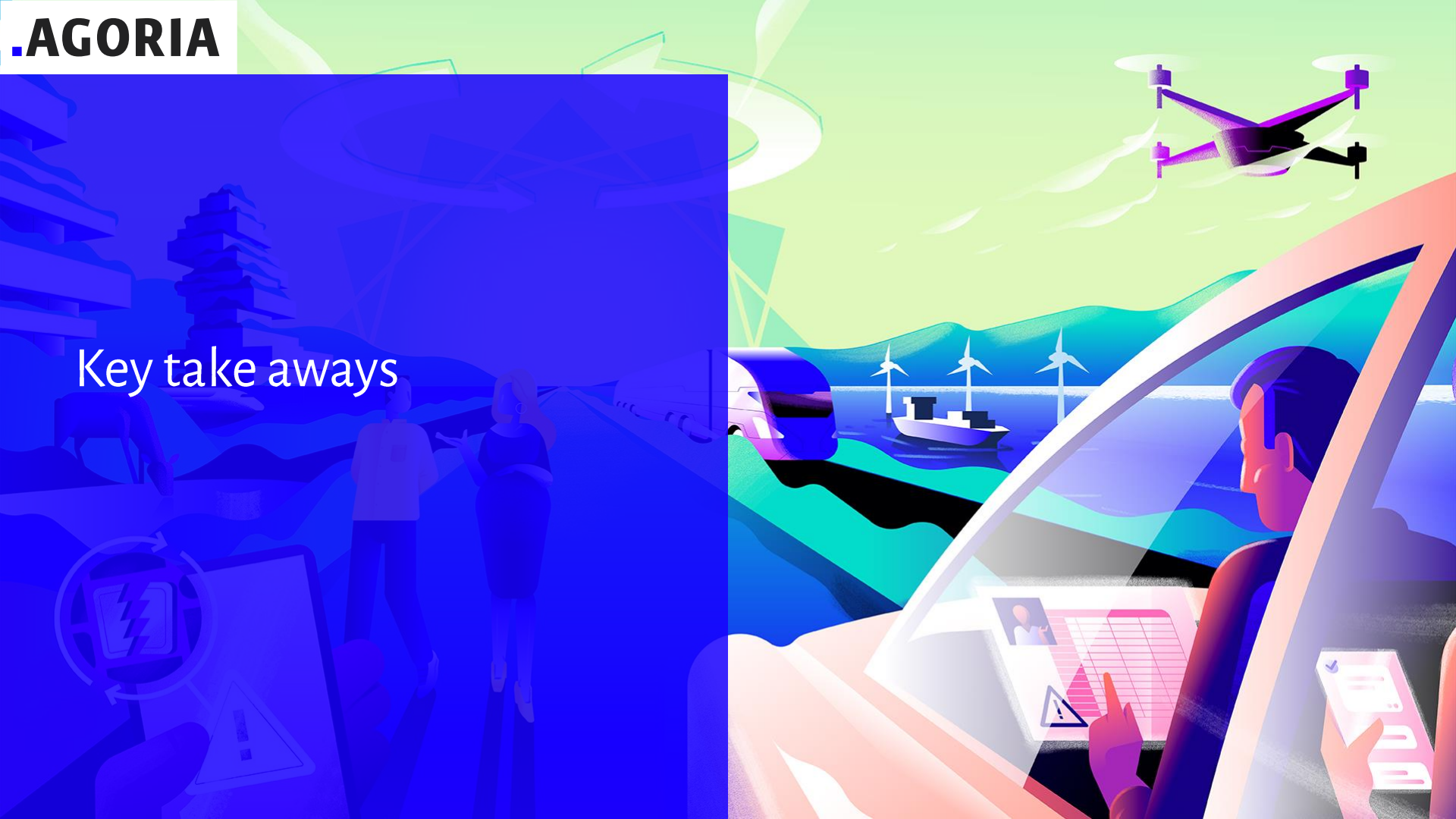
9 FREE Cyber Security Courses Online With Certificates from EC-Council Learning for all

Enroll for our free and comprehensive [online cyber security courses](#) today to kickstart your cybersecurity career!

Free Cyber Security Courses for Beginners for all.

<https://www.eccouncil.org/cybersecurity-exchange/cyber-novice/free-cybersecurity-courses-beginners/>

Key take aways



Key take aways

- Make a LIFE BREAK
 - Think about your CS vision (VST (2-5 y) , ST (5-10 y) , MT (10-20 y) , LT (20-30 y))
- Prepare your foundation blocks (1 and 2) – 10 -20 years of CS experience “milestones”
 - Take into consideration the CS level of experience (junior-> expert)
- Remember the dimensions of a certification
 - IT or CS IT or CS OT
 - Personal / Industry Level
 - Focus (process , vertical , specific technology)
- Certification will for sure will consolidate your SCK (1) and reinforce your foundation blocks
- Cyber is evolving 24/24
 - so you MUST acquire new competences / skills / knowledge on a regular basis
-> Continuing Professional Education (CPE) credit (2)

(1) SCK = Skills, Competences and Knowledge

(2) what you earn for completing a learning activity that improves your professional competence.

Questions & Answers

Thank you for your attention

Eric Van Cangh
Senior Business Group Leader Digital
Cybersecurity

T: +32 2 706 78 25
M: +32 492.23.24.34

Eric.Vancangh@agoria.be

