The hackers are ready.

Are we ?

Kurt Callewaert

TETRA 'Verboten & industriële security'

HOWEST UNIVERSITY of APPLIED SCIENCES

Lecturer Applied Computer Science- Computer & Cyber Crime Professional

Research manager

ISACA Academic Advocate for Howest University College

Member of the Belgian Cyber Security Coalition and IoTbe.org

Kurt Callewaert

Kurt.Callewaert@howest.be

- Lector Toegepaste informatica
  - * Maths , Problem solving
  - * Cryptography
  - * Cybersecurity Management
  - * IT Governance Cobit 5 / ISO 27000
  - * Risk management / assesment
  - * ERP-CRM-WMS
  - * ICT strategy
- Coördinator onderzoek Toegepaste informatica
  - * Research projects
  - * Internships / Bachelor Proofs
  - * Challenges , studytours , IT fairs ,…
  - * Member of the Belgian Cyber Security Coalition vzw and IoT.be vzw

Toegepaste Informatica

3 afstudeertrajecten

- **SSE : Software and System Engineering**
- **ICTC : ICT Consultant**
- **CCCP : Computer and Cyber Crime Professional**

RECORDS LOST: SINCE 2013

3,430,291,647

RECENT DATA BREACHES

NOVEMBER 29:
Madhya Pradesh police
Unknown Records

NOVEMBER 28:
Rockland Nissan
Unknown Records

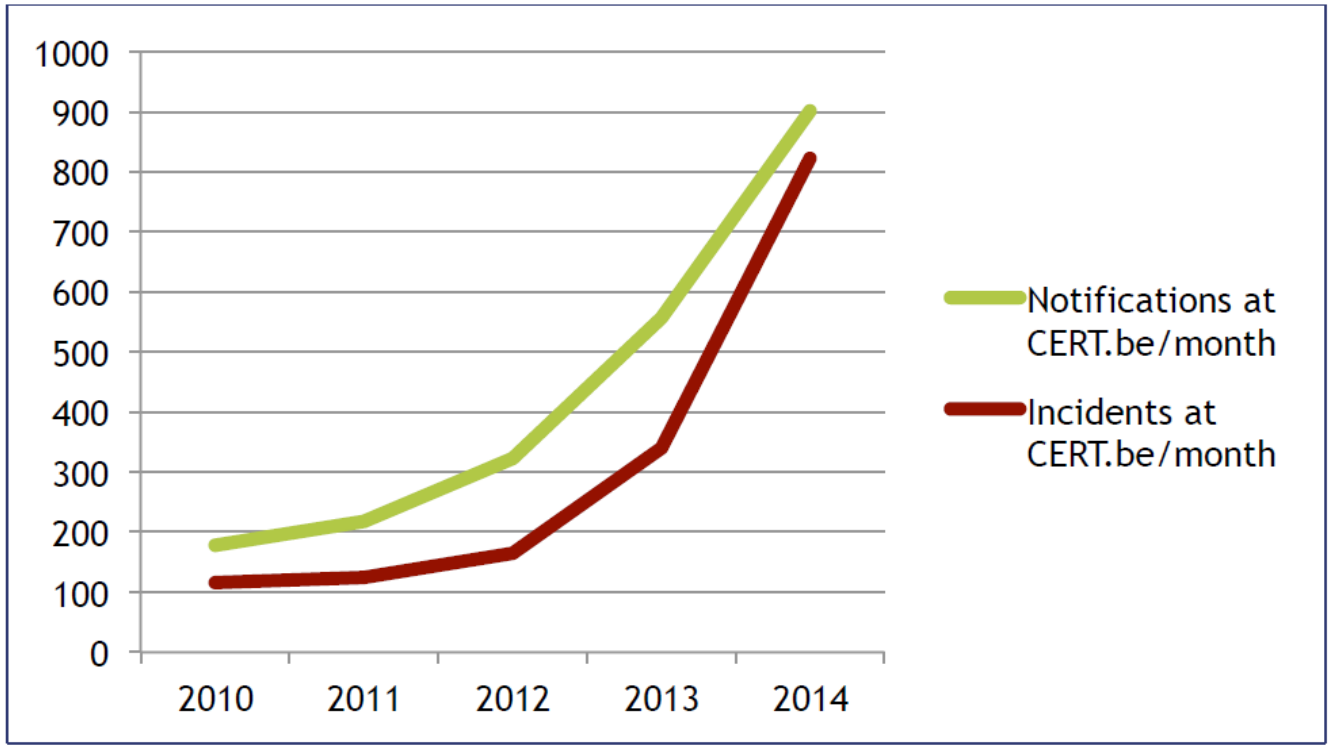
NOVEMBER 28:
Bluebox Broadband
3,000 Records

NOVEMBER 27:
Plan UK
Unknown Records

TOTAL RECORDS LOST BY MONTH IN 2015

BREACH LEVEL INDEX:

Not all breaches are created equal. Breaches are no longer a binary proposition where an organization either has or hasn't been breached. Instead they are wildly variable—having varying degrees of fallout—from breaches compromising entire global networks of highly sensitive data to



The average number of reports of cyber incidents at CERT.be each month, increases since the start of CERT.be in 2010.
Also the number of real incidents, filtered out from these reports, increases significant.

	2010	2011	2012	2013	2014
Notifications at CERT.be/month	178	217	322	557	901
Incidents at CERT.be/month	116	125	165	339	822

Number of infected computers in Belgium

751.000

Notifications of infected computers in Belgium

(until June 2014)

Cyber incident exercise

General situation

You are CEO of a large company specialised in engineering and machine building.

Your company keeps databases containing data of customers, mainly diagrams of new machines to be build.

Selected staff of your customers have VPN access on your environment to handle the files of the customers.

Your customers can also access your services through a web account in order to follow up the projects.

Incident situation

This night at 02:10 +0020 you received via e-mail the following message:

Sent : 23 June 2015 02:10 +0020
From : KingOfTheWorld@RemixMailer.net
To : CEO@MachineBuildingCompany.be
Subject : Compensation for audit of your lousy security.

Dear Mr. CEO

You and your company are extremely negligent and do not take the right security measures to protect customer's (top secret) diagrams of machines.

I've got a copy of your complete databases.

As compensation for my good work, I want the amount of 50.000 € paid in Bitcoins with 48 hours from now.

If you agree to compensate me, contact me via my e-mail address in order to get payment instructions.

If I do not get any reaction from your side or no payment is done before the deadline, I'll make all data from your database publicly available on the internet.

Hope to hear from you.

KingOfTheWorld

Requested

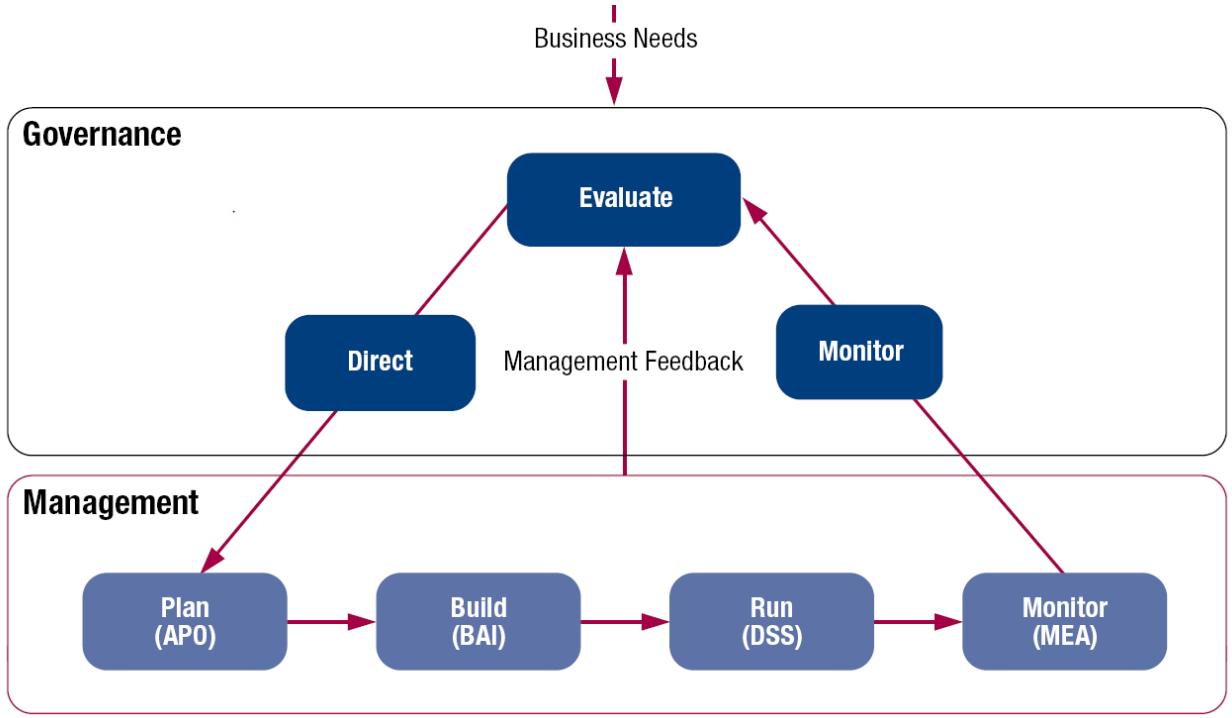
Which first actions do you consider to take in your company?

What is COBIT 5?

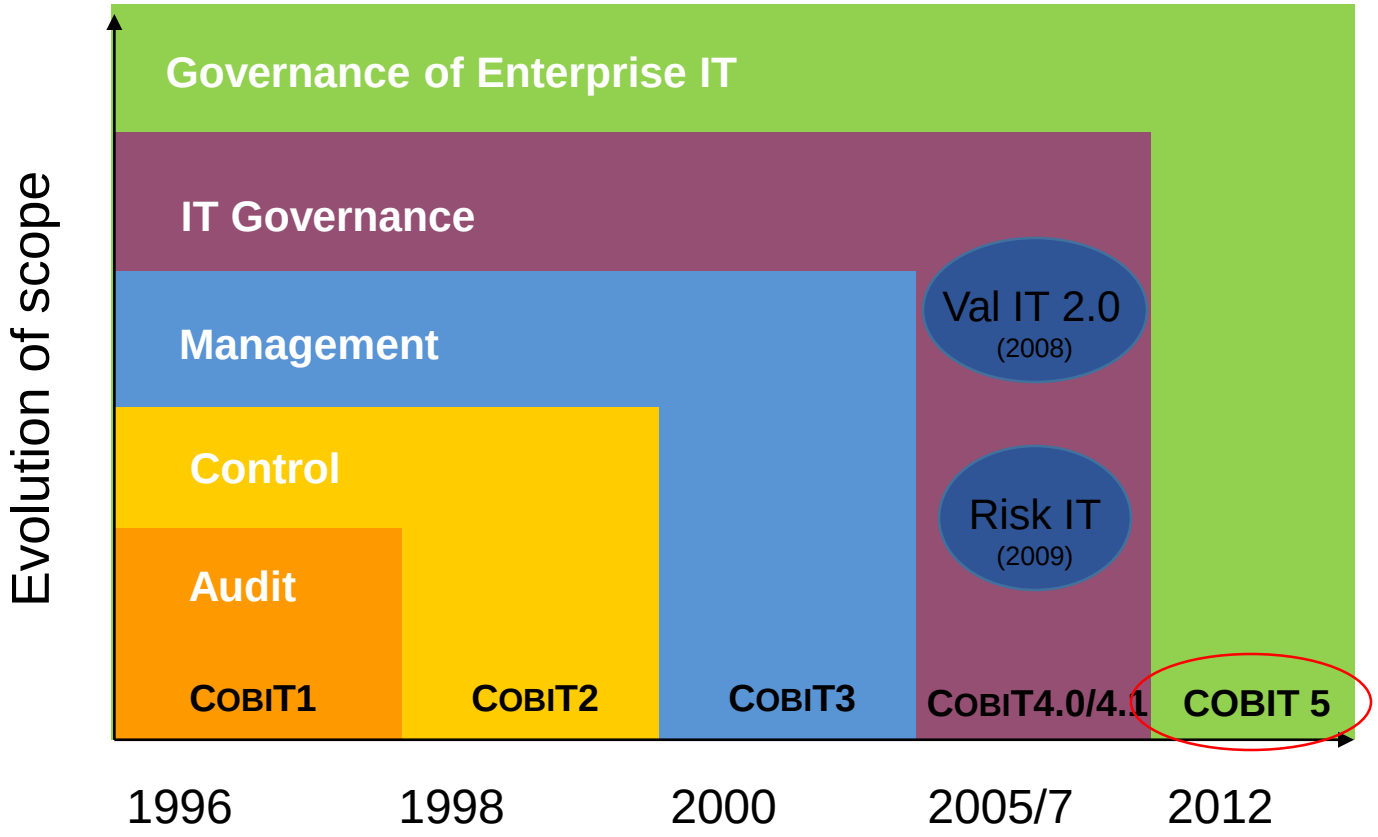
It's the leading framework for the governance and management of enterprise IT.

> Go to COBIT Online

COBIT 5 provides a comprehensive framework that assists enterprises to achieve their goals and deliver value through effective governance and management of enterprise IT.



COBIT 5: Now One Complete Business Framework



An business framework from ISACA, at www.isaca.org/cobit

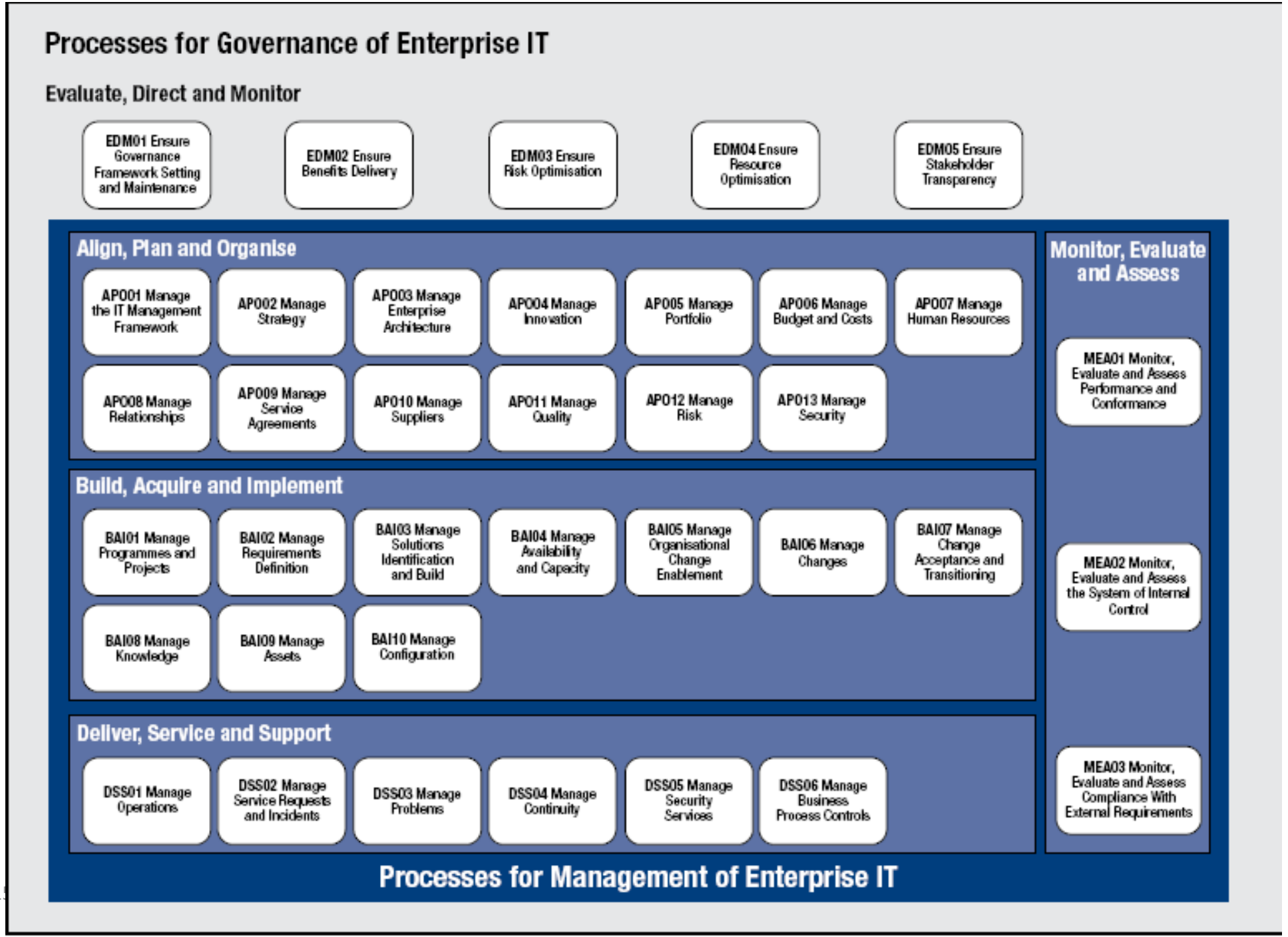
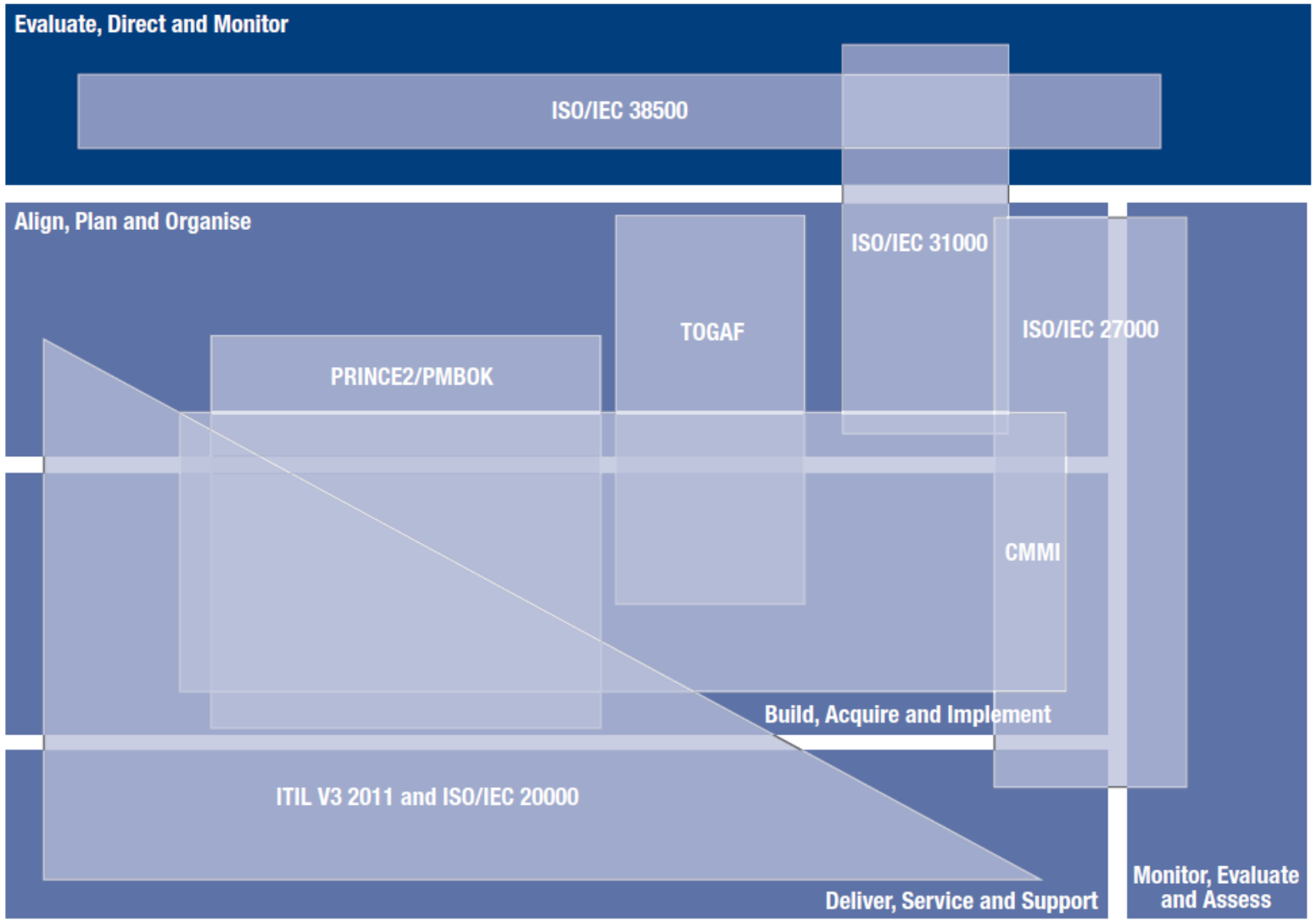
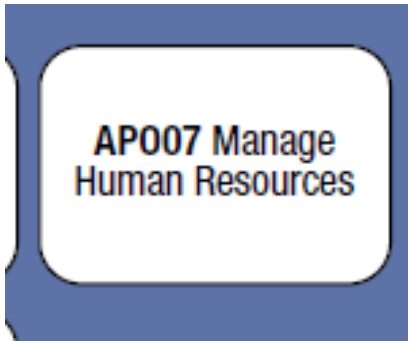
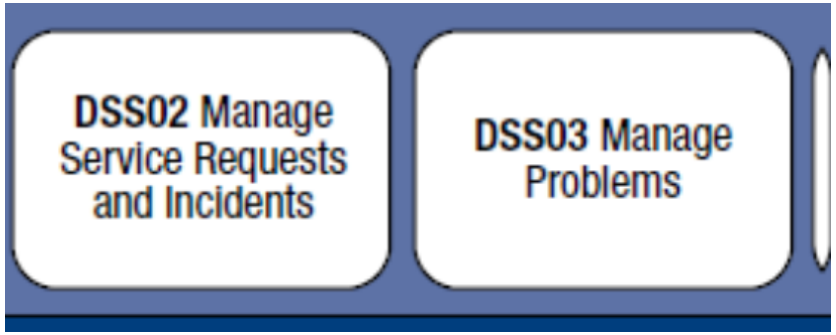

Processes for Governance of Enterprise IT
Evaluate, Direct and Monitor
EDM01 Ensure Governance Framework Setting and Maintenance
EDM02 Ensure Benefits Delivery
EDM03 Ensure Risk Optimisation
EDM04 Ensure Resource Optimisation
EDM05 Ensure Stakeholder Transparency
Align, Plan and Organise
APO01 Manage the IT Management Framework
APO02 Manage Strategy
APO03 Manage Enterprise Architecture
APO04 Manage Innovation
APO05 Manage Portfolio
APO06 Manage Budget and Costs
APO07 Manage Human Resources
APO08 Manage Relationships
APO09 Manage Service Agreements
APO10 Manage Suppliers
APO11 Manage Quality
APO12 Manage Risk
APO13 Manage Security
Build, Acquire and Implement
BAI01 Manage Programmes and Projects
BAI02 Manage Requirements Definition
BAI03 Manage Solutions Identification and Build
BAI04 Manage Availability and Capacity
BAI05 Manage Organisational Change Enablement
BAI06 Manage Changes
BAI07 Manage Change Acceptance and Transitioning
BAI08 Manage Knowledge
BAI09 Manage Assets
BAI10 Manage Configuration
Deliver, Service and Support
DSS01 Manage Operations
DSS02 Manage Service Requests and Incidents
DSS03 Manage Problems
DSS04 Manage Continuity
DSS05 Manage Security Services
DSS06 Manage Business Process Controls
Monitor, Evaluate and Assess
MEA01 Monitor, Evaluate and Assess Performance and Conformance
MEA02 Monitor, Evaluate and Assess the System of Internal Control
MEA03 Monitor, Evaluate and Assess Compliance With External Requirements
Processes for Management of Enterprise IT

Figure 25—COBIT 5 Coverage of Other Standards and Frameworks

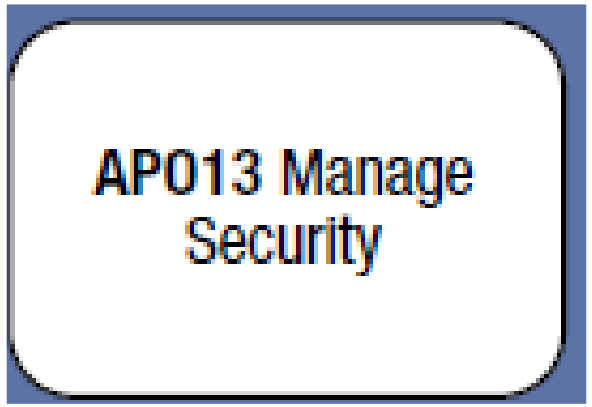



APO07 Manage
Human Resources


European
e-Competence
Framework


DSS02 Manage
Service Requests
and Incidents
DSS03 Manage
Problems


ITIL



Hoe ? Wie ? Wat ?

???????

information security management system (ISMS)


Information Security Management System
ISO
27001
Certified


ISO
27001
ISMS
ISO
27002
Controls
Close relation

Wat is het verschil tussen ISO 27001 en ISO 27002?

De internationale standaard **ISO 27002** (volledige naam: ISO/IEC 27002:2013) definieert **richtlijnen** voor de implementatie van de **maatregelen** die in **ISO 27001** worden genoemd. ISO 27001 specificeert **114 maatregelen** die gebruikt kunnen worden om beveiligingsrisico's te verkleinen, en ISO 27002 levert details over de manieren waarop deze controles kunnen worden geïmplementeerd. Organisaties kunnen gecertificeerd worden voor ISO 27001, maar niet tegen de ISO 27002.

ISO 27001:2013 INFORMATION SECURITY MANAGEMENT SYSTEM

- **A.5: Information security policies (2 controls)**
- **A.6: Organization of information security (7 controls)**
- **A.7: Human resource security - 6 controls that are applied before, during, or after employment**
- **A.8: Asset management (10 controls)**
- **A.9: Access control (14 controls)**
- **A.10: Cryptography (2 controls) → Crypto4SME - General Data Protection Regulation EU**
- **A.11: Physical and environmental security (15 controls)**
- **A.12: Operations security (14 controls)**
- **A.13: Communications security (7 controls)**
- **A.14: System acquisition, development and maintenance (13 controls)**
- **A.15: Supplier relationships (5 controls)**
- **A.16: Information security incident management (7 controls)**
- **A.17: Information security aspects of business continuity management (4 controls)**
- **A.18: Compliance; with internal requirements, such as policies, and with external requirements, such as laws (8 controls)**

A.16 Information security incident management		
A.16.1 Management of information security incidents and improvements		
Objective: To ensure a consistent and effective approach to the management of information security incidents, including communication on security events and weaknesses.		
A.16.1.1	Responsibilities and procedures	*Control* Management responsibilities and procedures shall be established to ensure a quick, effective and orderly response to information security incidents.
A.16.1.2	Reporting information security events	*Control* Information security events shall be reported through appropriate management channels as quickly as possible.
A.16.1.3	Reporting information security weaknesses	*Control* Employees and contractors using the organization's information systems and services shall be required to note and report any observed or suspected information security weaknesses in systems or services.
A.16.1.4	Assessment of and decision on information security events	*Control* Information security events shall be assessed and it shall be decided if they are to be classified as information security incidents.
A.16.1.5	Response to information security incidents	*Control* Information security incidents shall be responded to in accordance with the documented procedures.
A.16.1.6	Learning from information security incidents	*Control* Knowledge gained from analysing and resolving information security incidents shall be used to reduce the likelihood or impact of future incidents.
A.16.1.7	Collection of evidence	*Control* The organization shall define and apply procedures for the identification, collection, acquisition and preservation of information, which can serve as evidence.

16.1.1 Responsibilities and procedures

Control

Management responsibilities and procedures should be established to ensure a quick, effective and orderly response to information security incidents.

Implementation guidance

The following guidelines for management responsibilities and procedures with regard to information security incident management should be considered:

a) management responsibilities should be established to ensure that the following procedures are developed and communicated adequately within the organization:

   1) procedures for incident response planning and preparation;

   2) procedures for monitoring, detecting, analysing and reporting of information security events and incidents;

3) procedures for logging incident management activities;

4) procedures for handling of forensic evidence;

5) procedures for assessment of and decision on information security events and assessment of information security weaknesses;

6) procedures for response including those for escalation, controlled recovery from an incident and communication to internal and external people or organizations;

b) procedures established should ensure that:

1) competent personnel handle the issues related to information security incidents within the organization;

2) a point of contact for security incidents' detection and reporting is implemented;

3) appropriate contacts with authorities, external interest groups or forums that handle the issues related to information security incidents are maintained;

c) reporting procedures should include:

1) preparing information security event reporting forms to support the reporting action and to help the person reporting to remember all necessary actions in case of an information security event;

2) the procedure to be undertaken in case of an information security event, e.g. noting all details immediately, such as type of non-compliance or breach, occurring malfunction, messages on the screen and immediately reporting to the point of contact and taking only coordinated actions;

3) reference to an established formal disciplinary process for dealing with employees who commit security breaches;

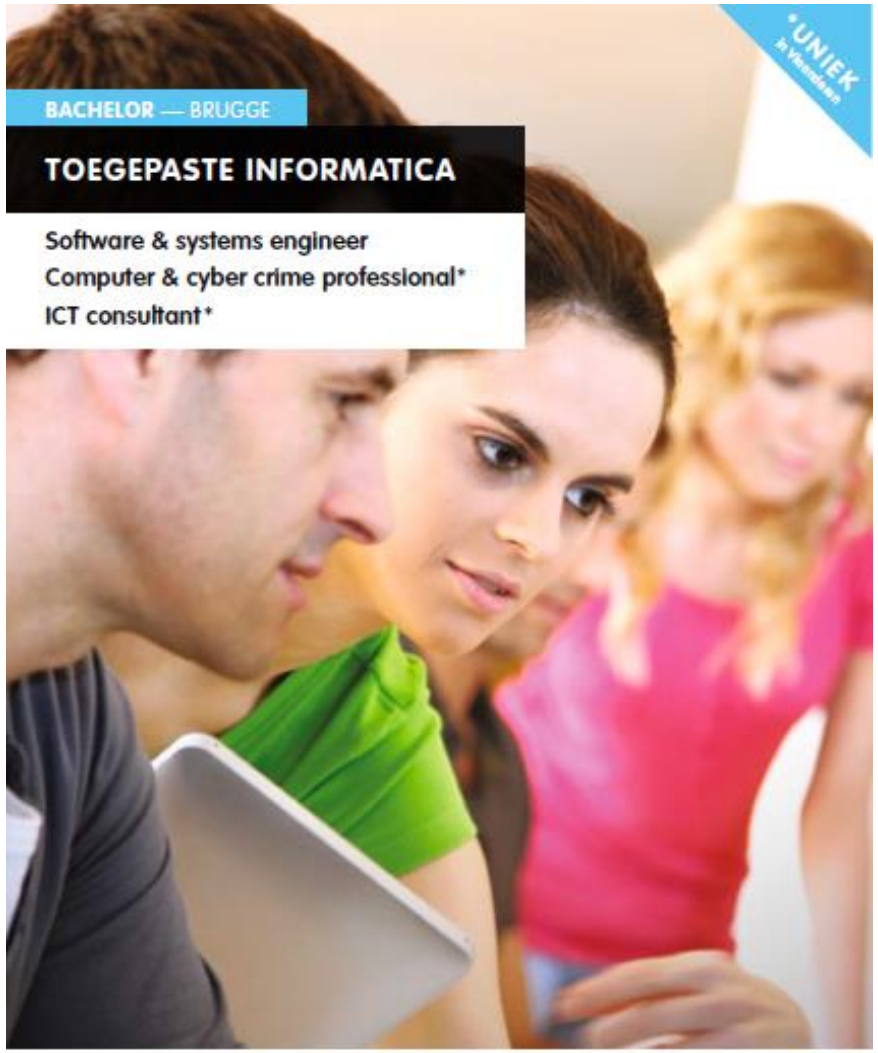
4) suitable feedback processes to ensure that those persons reporting information security events are notified of results after the issue has been dealt with and closed.

The objectives for information security incident management should be agreed with management, and it should be ensured that those responsible for information security incident management understand the organization's priorities for handling information security incidents.

Other information

Information security incidents might transcend organizational and national boundaries. To respond to such incidents there is an increasing need to coordinate response and share information about these incidents with external organizations as appropriate.


CENTRE FOR
CYBER SECURITY
BELGIUM
CYBER SECURITY
COALITION
CYBER SECURITY
INCIDENT MANAGEMENT GUIDE


BACHELOR — BRUGGE
TOEGEPASTE INFORMATICA
Software & systems engineer
Computer & cyber crime professional*
ICT consultant*
*UNIEK
howest
2015 — 2016

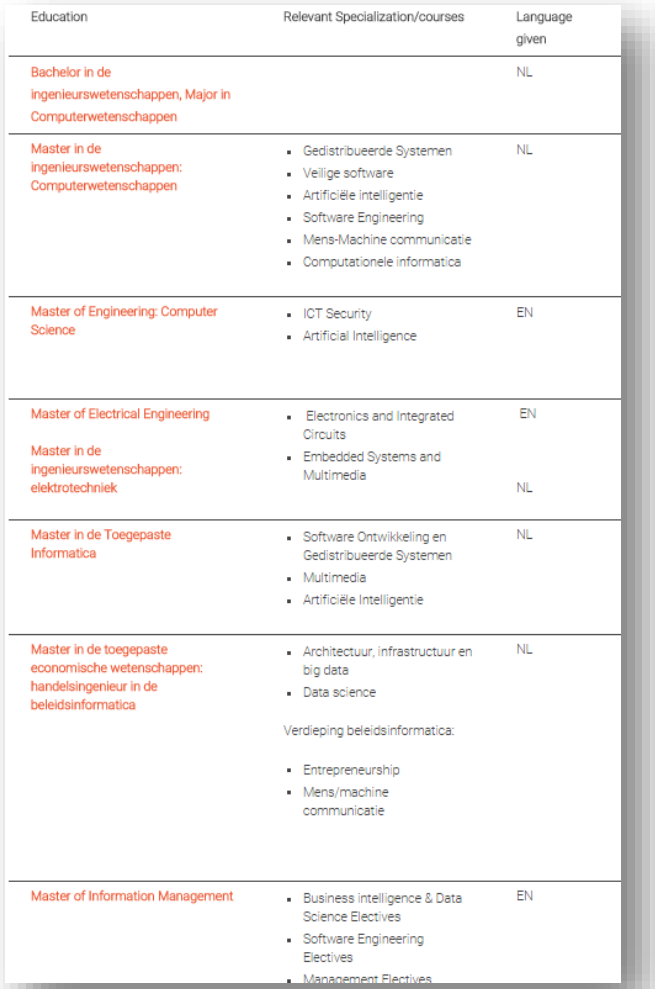
Education Landscape for Cybersecurity

Education in IT and Computer Sciences	Check www.b-ccentre.be/education
Specific courses within other education programs	Check www.b-ccentre.be/education
Education in Information Security and Cybersecurity related domains	Following pages list inventoried options

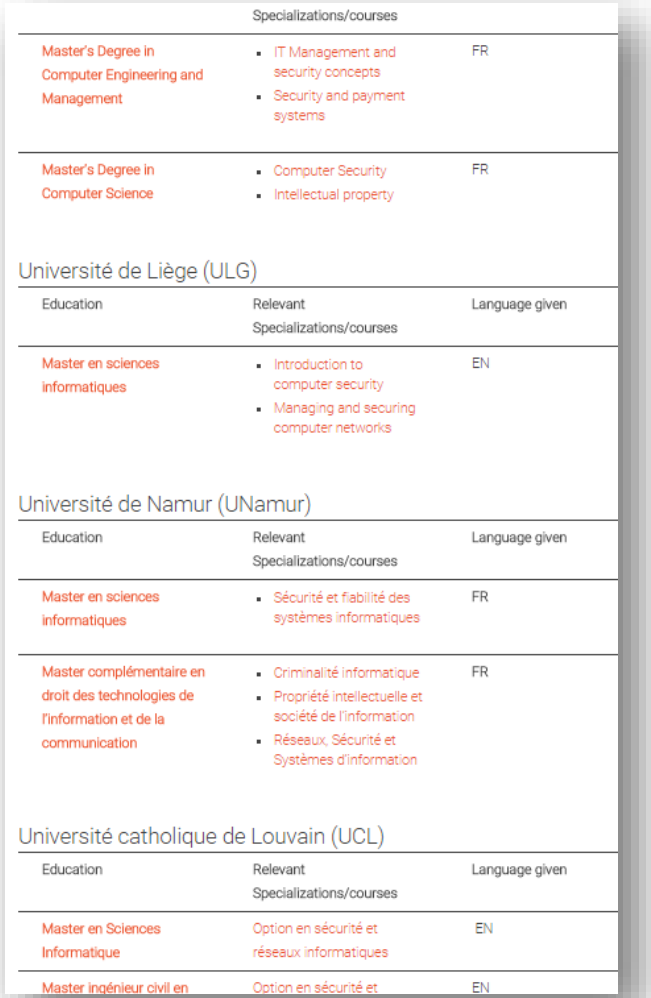
Education in IT and Computer Sciences

Specific courses within other education programs

Check b-ccentre.be/education



Education	Relevant Specialization/courses	Language given
Bachelor in de ingenieurswetenschappen, Major in Computerwetenschappen		NL
Master in de ingenieurswetenschappen: Computerwetenschappen	▪ Gedistribueerde Systemen ▪ Veilige software ▪ Artificiële intelligentie ▪ Software Engineering ▪ Mens-Machine communicatie ▪ Computationele informatica	NL
Master of Engineering: Computer Science	▪ ICT Security ▪ Artificial Intelligence	EN
Master of Electrical Engineering Master in de ingenieurswetenschappen: elektrotechniek	▪ Electronics and Integrated Circuits ▪ Embedded Systems and Multimedia	EN NL
Master in de Toegepaste Informatica	▪ Software Ontwikkeling en Gedistribueerde Systemen ▪ Multimedia ▪ Artificiële Intelligentie	NL
Master in de toegepaste economische wetenschappen: handelsingenieur in de beleidsinformatica	▪ Architectuur, infrastructuur en big data ▪ Data science Verdieping beleidsinformatica: ▪ Entrepreneurship ▪ Mens/machine communicatie	NL
Master of Information Management	▪ Business intelligence & Data Science Electives ▪ Software Engineering Electives ▪ Management Electives	EN



	Specializations/courses	
Master's Degree in Computer Engineering and Management	▪ IT Management and security concepts ▪ Security and payment systems	FR
Master's Degree in Computer Science	▪ Computer Security ▪ Intellectual property	FR

Université de Liège (ULG)

Education	Relevant Specializations/courses	Language given
Master en sciences informatiques	▪ Introduction to computer security ▪ Managing and securing computer networks	EN

Université de Namur (UNamur)

Education	Relevant Specializations/courses	Language given
Master en sciences informatiques	▪ Sécurité et fiabilité des systèmes informatiques	FR
Master complémentaire en droit des technologies de l'information et de la communication	▪ Criminalité informatique ▪ Propriété intellectuelle et société de l'information ▪ Réseaux, Sécurité et Systèmes d'information	FR

Université catholique de Louvain (UCL)

Education	Relevant Specializations/courses	Language given
Master en Sciences Informatique	Option en sécurité et réseaux informatiques	EN
Master ingénieur civil en	Option en sécurité et	EN

Education	Relevant Specialization/courses	Language given
Professionele bachelor in de Toegepaste Informatica	Systeem en Netwerkbeheer	NL

Katholieke Hogeschool Leuven

Education	Relevant Specialization/courses	Language given
Bachelor toegepaste informatica	IT en Recht	NL

Thomas More Antwerpen / Kempen / Mechelen

Education	Relevant Specialization/courses	Language g
Professionele Bachelor in de elektronica-ICT	▪ Netwerkbeveiliging ▪ data-analyse en encryptie	NL
Bachelor in het informaticamanagement en de multimedia	▪ Recht ▪ Information Security	NL

Haute Ecole Francisco FERRER

Education	Relevant Specialization/courses	Language g
Bachelier en électronique appliquée	Gestion d'infrastructure et sécurité informatique	FR

Haute Ecole Paul-Henri Spaak

Education	Relevant Specialization/courses	Language g
Master en sciences de l'ingenieur industriel finalite informatique	Réseaux de communication et sécurité	FR

Haute Ecole de Bruxelles

Education	Relevant	Language given

Education in Information Security and Cybersecurity related domains

Academic education in Information Security, Cybersecurity and related studies

Inventoried education offering:

- **Computer & Cyber Crime Professional (Bachelor)** ,HOWEST University of Applied Sciences (Bruges)
- **Executive Master of IT Governance And Assurance**, Antwerp Management School
- **Advanced Master of Intellectual Property Rights And ICT Law**, Ku Leuven
- **Executive Programme in Security Governance**, Solvay Brussels School Of Economics And Management
- **Executive Programme in Cybersecurity**, Solvay Brussels School Of Economics And Management
- **Executive Programme in Information Security**, Solvay Brussels School Of Economics And Management
- **Executive Master in Information Risk And Cybersecurity**, Solvay Brussels School Of Economics And Management

In de basisopleiding komen vijf pijlers aan bod: ICT Infrastructuur, Informatiemanagement, Softwareontwikkeling, ICT-management en Web en mobiele technologie. Naast de noodzakelijk wetenschappelijke onderbouw krijg je practica en boeiende projecten waarin creativiteit en innovatie ingebed zijn. In de keuzetrajecten komen specialisaties en variaties op de pijlers aan bod.

COMPUTER & CYBER CRIME PROFESSIONAL

HOWEST University of Applied Sciences in Bruges

www.howest.be

- **Unique training from the age of 17 / 18 years**
- **Level : Professional Bachelor Applied Computer Science – 3 years**
- **Technical skills :**

Web pentesting, Network & system pentesting, Forensic analysis , Social engineering, Cryptography , Biometrics, …

- **Non technical skills :**

IT Governance , Information security management , Risk management , Risk assesment , Privacy rules , IT jurisdiction , Cyber crimes, Mobile security management, Cybersecurity , …

- **Frameworks :**

COBIT 5 , ISO 27001/2 , NIST CSF , PTES , ITIL v3 , OWASP , SANS , …

- **Certificates :**

CEH , Cisco CCNA , VMware , CSX (Cyber Security neXus)

Ready for CISSP and CISM

- **Secure development :**

Python, C , C# , PHP, Java , JavaScript , ASP.NET


BACHELOR TOEGEPASTE INFORMATICA
JAAR 1
SEMESTER 1
SEMESTER 2
ICT INFRASTRUCTUUR I
Desktop and
Mobile operating systems
Hardware
6
ICT INFRASTRUCTUUR II
Computernetwerken
6
INFORMATIESYSTEMEN I
Databanken
3
INFORMATIESYSTEMEN II
Analyse- en
modelleringstechnieken
3
SOFTWAREONTWIKKELING I
C#
Programmeervaardigheden
Logica en probleemoplossend
denken
9
SOFTWAREONTWIKKELING II
C#
Algoritmes en datastructuren
6
E-BUSINESS
Digitale economie
ICT-georiënteerd bedrijfsbeleid
Procesmanagement
6
WEBONTWIKKELING
HTML, CSS en JavaScript
6
WEB EN MOBILE I
Server-side scripting (PHP)
Webserverconfiguratie
(Apache)
Web en mobile UI
6
PROJECTEN I
Projectmanagement
Projectcommunicatie
Programmeerproject
9

Traject Computer & Cyber Crime professional HOWEST - Toegepaste informatica

Webbeveiliging I	S2	
Web pentesting		Parcifal Aertssen
Data mining technieken	S3	
Wetgeving i.v.m. privacy en databanken en informaticarecht		Marc Vael
Webbeveiliging II	S3	
Webbeveiligingen en Honeypot		Parcifal Aertssen
Softwareontwikkeling en beveiliging	S4	
C en Python		Jonas Maes
Computercriminaliteit	S4	
Computercriminaliteit		Guy Verbeeren
Projecten III	S4	
Beveiligingsproject in samenwerking met bedrijf of organisatie		Kurt Callewaert
Beveiligingstechnologie II	S5	
VMware, Cloud computing en beveiliging		Tijl Deneut, Alexander Van Maele
Linux Server security		Jonas Maes
Forensische ICT en CCNA Security	S5	
Forensische ICT tools		Tijl Deneut , Alexander Van Maele
CCNA Security		Christiaan Ledoux
Beveiligingsalgoritmes en -software	S5	
Beveiligingsalgoritmes - cryptography		Kurt Callewaert
Netwerk en systeem pentesting		Tijl Deneut , Alexander Van Maele
Beveiligingsbeleid	S5	
IT Governance		Kurt Callewaert
Beveiligingsbeleid, threat en risk assessment		Kurt Callewaert
Webbeveiliging IV	S5	
Gastsprekers uit de security over onderwerpen die niet aan bod kwamen tijdens de lessen vb SCADA		Tijl Deneut
Challenges, seminaries en bedrijfsbezoeken	S6	Kurt Callewaert
Deelname Brucon, Infosecurity, Hacking challenges, Fosdem		
Bachelorproef en stage	S6	Kurt Callewaert
Security stage in een bank, bedrijf of openbare instelling,		

Technische en niet-technische certificaten

Stages en beveiligingsprojecten

TOREON

KBC

BNP PARIBAS FORTIS

TSF

accenture
High performance. Delivered.

Belfius
Bank & Verzekeringen

VASCO

IMPACT IT SOLUTIONS

FCCU

Xiak

SPOT IT
YOUR NETWORK & SECURITY LAYER

nviso
SECURITY. RESEARCH. RISK.

pwc

Secure | IT
Experts in critical IT

telenet

EY

V-ICT-OR
VLAAMSE ICT ORGANISATIE

e2s
SOFTWARE & SECURITY

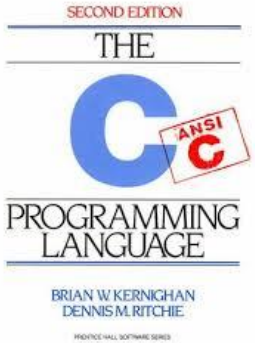
Deloitte.

Wsec

FORCE when facts matter

SPOT IT
YOUR NETWORK & SECURITY LAYER

Secure development



Top vijf IT vacatures in % stijging in 2015 tov 2014:

1. Security Consultant	**+ 59 %**
2. ICT Manager	**+ 50 %**
3. Softwareontwikkelaar	**+ 27 %**
4. Applicatie/Functioneel Beheer	**+ 25 %**
5. Project Manager	**+ 24 %**