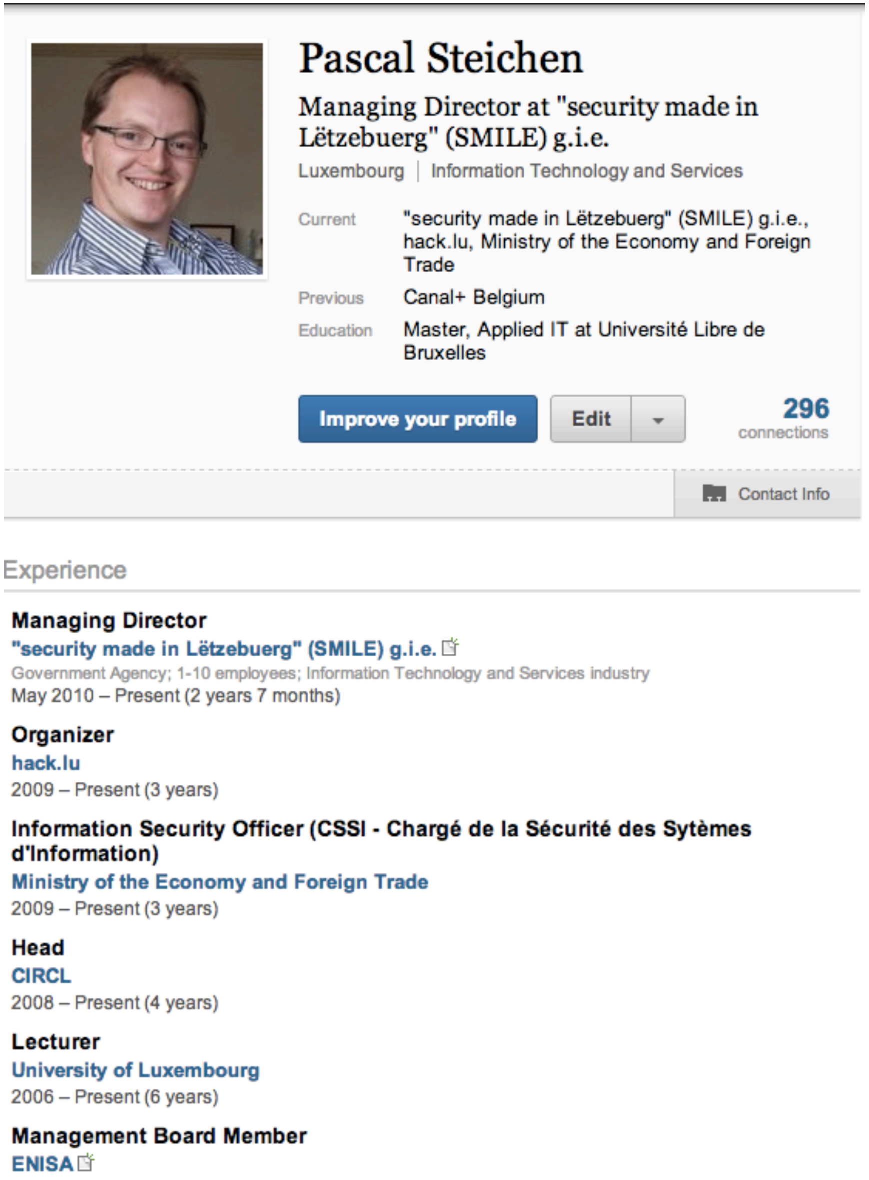
Cyber Security players

from Hackers, to CISOs and beyond

Whoami



Pascal Steichen

Managing Director at "security made in Lëtzebuerg" (SMILE) g.i.e.

Luxembourg | Information Technology and Services

Current "security made in Lëtzebuerg" (SMILE) g.i.e., hack.lu, Ministry of the Economy and Foreign Trade

Previous Canal+ Belgium

Education Master, Applied IT at Université Libre de Bruxelles

Experience

Managing Director
"security made in Lëtzebuerg" (SMILE) g.i.e.
Government Agency; 1-10 employees; Information Technology and Services industry
May 2010 – Present (2 years 7 months)

Organizer
hack.lu
2009 – Present (3 years)

Information Security Officer (CSSI - Chargé de la Sécurité des Sytèmes d'Information)
Ministry of the Economy and Foreign Trade
2009 – Present (3 years)

Head
CIRCL
2008 – Present (4 years)

Lecturer
University of Luxembourg
2006 – Present (6 years)

Management Board Member
ENISA

Hack.lu 2012

Your feedback

“Cyber criminals”

Hacker, Script Kiddies and other cyber nerds

Hackers

Yes, I am a criminal. My crime is that of curiosity. My crime is that of judging people by what they say and think, not what they look like.

My crime is that of outsmarting you, something that you will never forgive me for.

I am a hacker, and this is my manifesto. You may stop this individual, but you can't stop us all... after all, we're all alike.

Hackers

Yes, I am a criminal. My crime is that of curiosity. My crime is that of judging people by what they say and think, not what they look like.

My crime is that of outsmarting you, something that you will never forgive me for.

I am a hacker, and this is my manifesto. You may stop this individual, but you can't stop us all... after all, we're all alike.

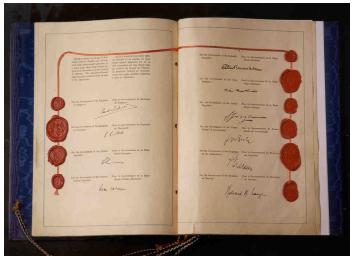
+++The Mentor +++

Script Kiddie

A script kiddie or script running juvenile (SRJ) are individuals who use scripts or programs developed by others to attack computer systems and networks and deface websites. This may include those who do so with a poor understanding of programming or computer networks. The term is typically pejorative.

Council of Europe - Cybercrime convention

Title 1 – Offences against the confidentiality, integrity and availability of computer data and systems



Article 2 – Illegal access

Article 3 – Illegal interception

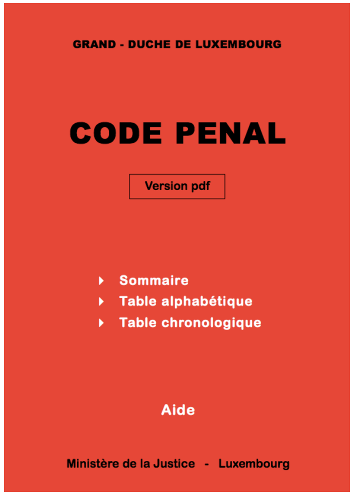
Article 4 – Data interference

Article 5 – System interference

Article 6 – Misuse of devices

e.g. “code pénal” - LU

Section VII.1 - De certaines infractions en matière informatique.



GRAND - DUCHE DE LUXEMBOURG

CODE PENAL

Version pdf

- Sommaire
- Table alphabétique
- Table chronologique

Aide

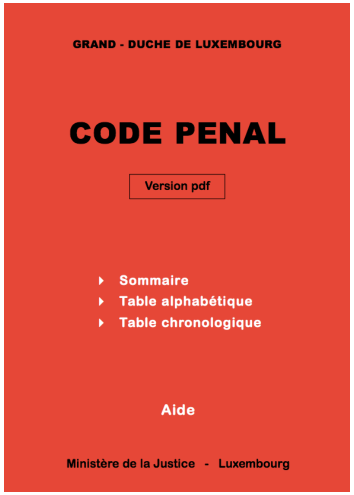
Ministère de la Justice - Luxembourg

Art. 509-1. (L. 14 août 2000) Quiconque, frauduleusement, aura accédé ou se sera maintenu dans tout ou partie d’un système de traitement ou de transmission automatisé de données sera puni d’un emprisonnement de deux mois à deux ans et d’une amende de 500 euros à 25.000 euros ou de l’une de ces deux peines.

Lorsqu’il en sera résulté soit la suppression ou la modification de données contenues dans le système, soit une altération du fonctionnement de ce système, l’emprisonnement sera de quatre mois à deux ans et l’amende de 1.250 euros à 25.000 euros.

e.g. “code pénal” - LU

Section VII.1 - De certaines infractions en matière informatique.



GRAND - DUCHE DE LUXEMBOURG

CODE PENAL

Version pdf

- Sommaire
- Table alphabétique
- Table chronologique

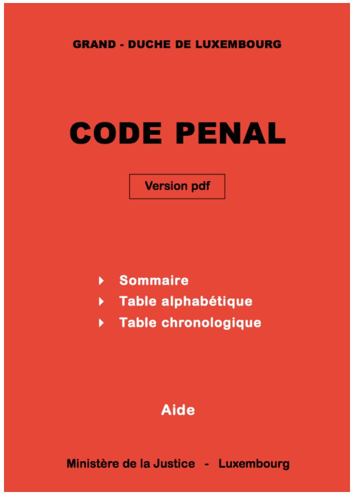
Aide

Ministère de la Justice - Luxembourg

Art. 509-2. (L. 15 juillet 1993) Quiconque aura, intentionnellement et au mépris des droits d’autrui, entravé ou faussé le fonctionnement d’un système de traitement ou de transmission automatisé de données sera puni d’un emprisonnement de trois mois à trois ans et d’une amende de 1.250 euros à 12.500 euros ou de l’une de ces deux peines.

e.g. "code pénal" - LU

Section VII.1 - De certaines infractions en matière informatique.



GRAND - DUCHE DE LUXEMBOURG

CODE PENAL

Version pdf

- Sommaire
- Table alphabétique
- Table chronologique

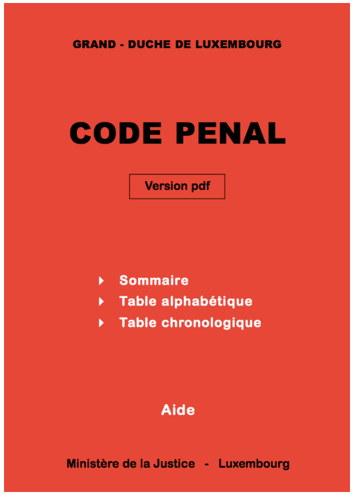
Aide

Ministère de la Justice - Luxembourg

Art. 509-3. (L. 14 août 2000) Quiconque aura, intentionnellement et au mépris des droits d'autrui, directement ou indirectement, introduit des données dans un système de traitement ou de transmission automatisé ou supprimé ou modifié les données qu'il contient ou leurs modes de traitement ou de transmission, sera puni d'un emprisonnement de trois mois à trois ans et d'une amende de 1.250 euros à 12.500 euros ou de l'une de ces deux peines.

e.g. “code pénal” - LU

Section VII.1 - De certaines infractions en matière informatique.



GRAND - DUCHE DE LUXEMBOURG

CODE PENAL

Version pdf

- Sommaire
- Table alphabétique
- Table chronologique

Aide

Ministère de la Justice - Luxembourg

Art. 509-4. (L. 10 novembre 2006) Lorsque dans les cas visés aux articles 509-1 à 509-3, il y a eu transfert d’argent ou de valeur monétaire, causant ainsi une perte de propriété à un tiers dans un but de procurer un avantage économique à la personne qui commet l’infraction ou à une tierce personne, la peine encourue sera un emprisonnement de quatre mois à cinq ans et une amende de 1.250 euros à 30.000 euros.

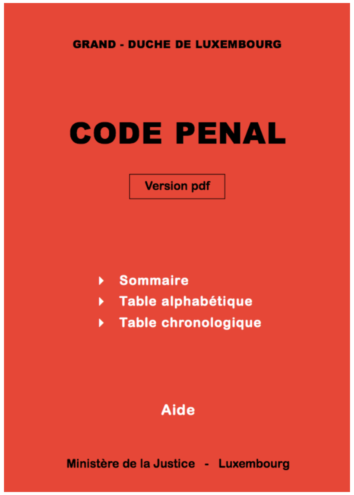
Encourront les mêmes peines, ceux qui auront fabriqué, reçu, obtenu, détenu, vendu ou cédé à un tiers des logiciels ayant pour objet de rendre possible une infraction visée à l’alinéa qui précède.

e.g. “code pénal” - LU

Section VII.1 - De certaines infractions en matière informatique.

Art. 509-6. (L. 15 juillet 1993) La tentative des délits prévus par les articles 509-1 à 509-5 est punie des mêmes peines que le délit lui-même.

Art. 509-7. (L. 15 juillet 1993) Quiconque aura participé à une association formée ou à une entente établie en vue de la préparation, concrétisée par un ou plusieurs faits matériels, d’une ou de plusieurs infractions prévues par les articles 509-1 à 509-5 sera puni des peines prévues pour l’infraction elle- même ou pour l’infraction la plus sévèrement réprimée.



GRAND - DUCHE DE LUXEMBOURG

CODE PENAL

Version pdf

- Sommaire
- Table alphabétique
- Table chronologique

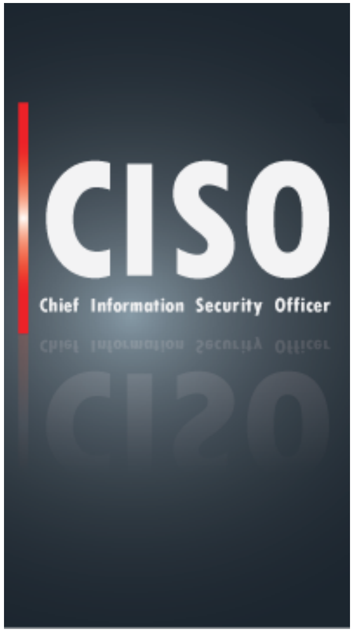
Aide

Ministère de la Justice - Luxembourg

(Chief) Information Security Officer

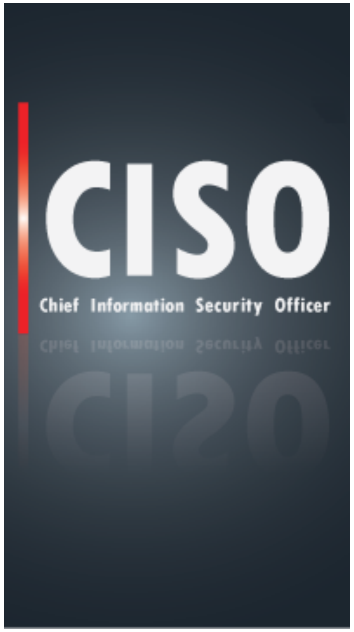
aka CISO, ISO, ITSO, RSSI, RSI

CISO – roles and responsibilities



A chief information security officer (CISO) is the senior-level executive within an organization responsible for **establishing** and **maintaining** the enterprise vision, **strategy and program** to ensure **information assets** are **adequately protected**. The CISO directs staff in identifying, developing, implementing and maintaining processes **across the organization** to **reduce** information and information technology (IT) **risks**, **respond to incidents**, establish appropriate **standards and controls**, and direct the establishment and implementation of **policies and procedures**. The CISO is also usually responsible for information-related **compliance**.

CISO – roles and responsibilities



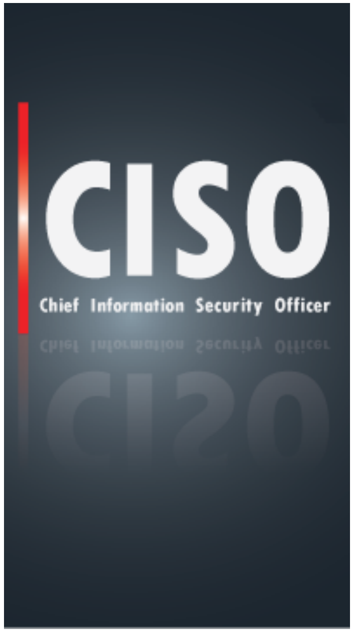
- Typically, the CISO's influence reaches the whole organization. Responsibilities include:
  - Information security and information assurance
  - Information regulatory compliance
    (e.g. PCI-DSS, Basel II ; VPPA, SOX, FISMA, GLBA, HIPAA ; 1999/93/EC, 2002/58/EC, 2006/24/EC ; Cyber security strategies ; ISO270XX)
  - Information risk management
  - Information technology controls
  - Information privacy
  - CERT / CSIRT activities
  - Identity and access management
  - Information security architecture
  - IT investigations, digital forensics
  - Disaster recovery and business continuity management
  - Information Security Operations Center

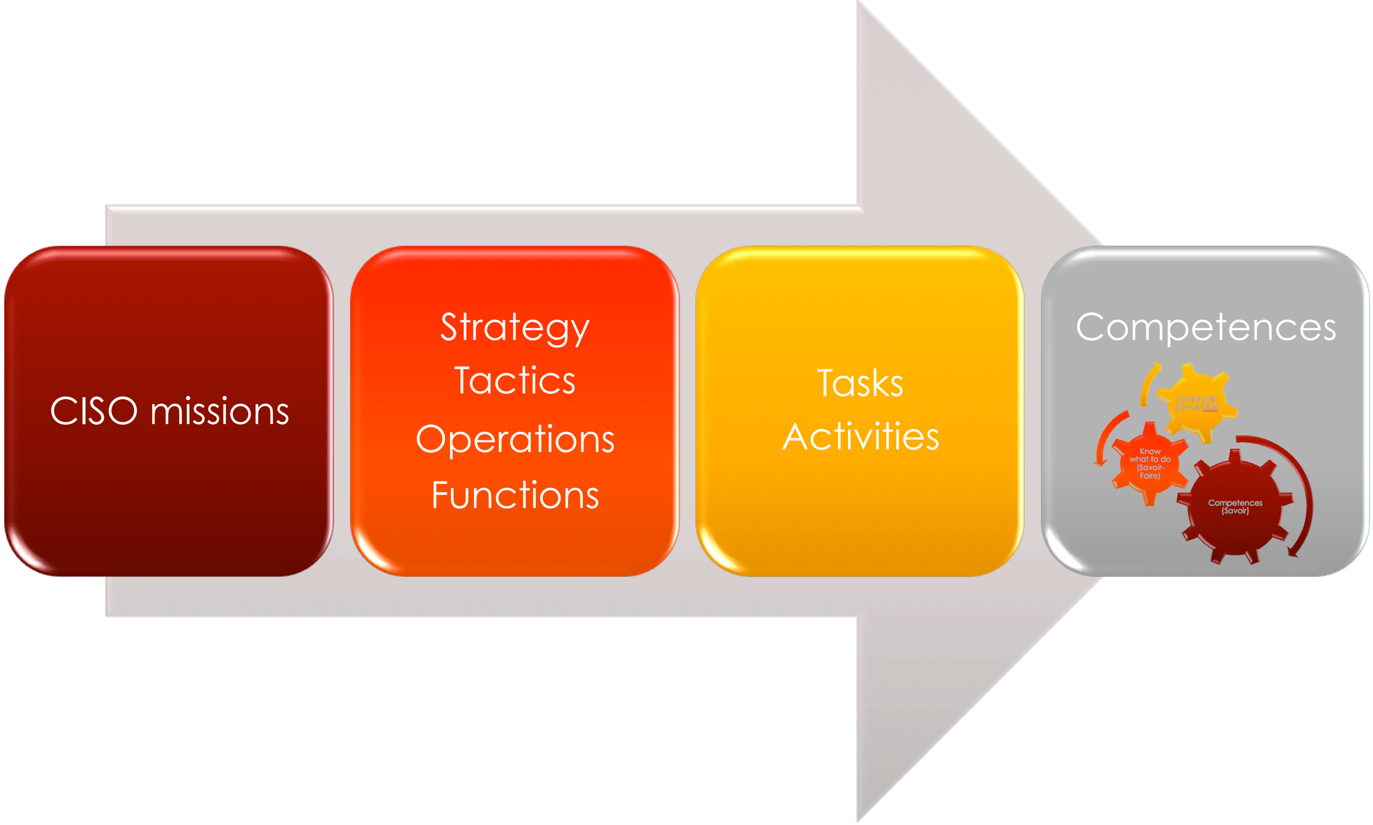
“Hacker” vs (C)ISO

“White board game”

This is the true story of Frank Abagnale, alias Frank Williams, alias Robert Conrad, Frank Adams, and Robert Monjo—
for five years the world's most
hunted forger, fraudulent check writer,
impostor, and con man extraordinaire.

CISO – full job description





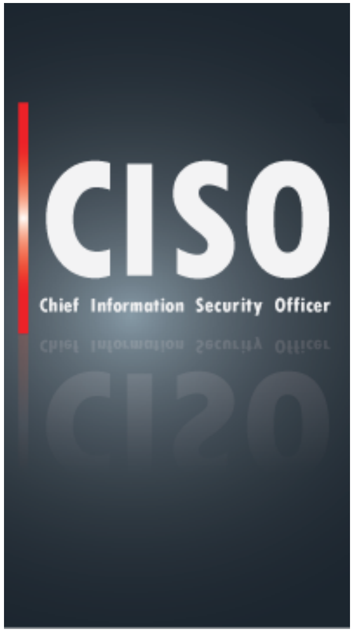
CISO missions

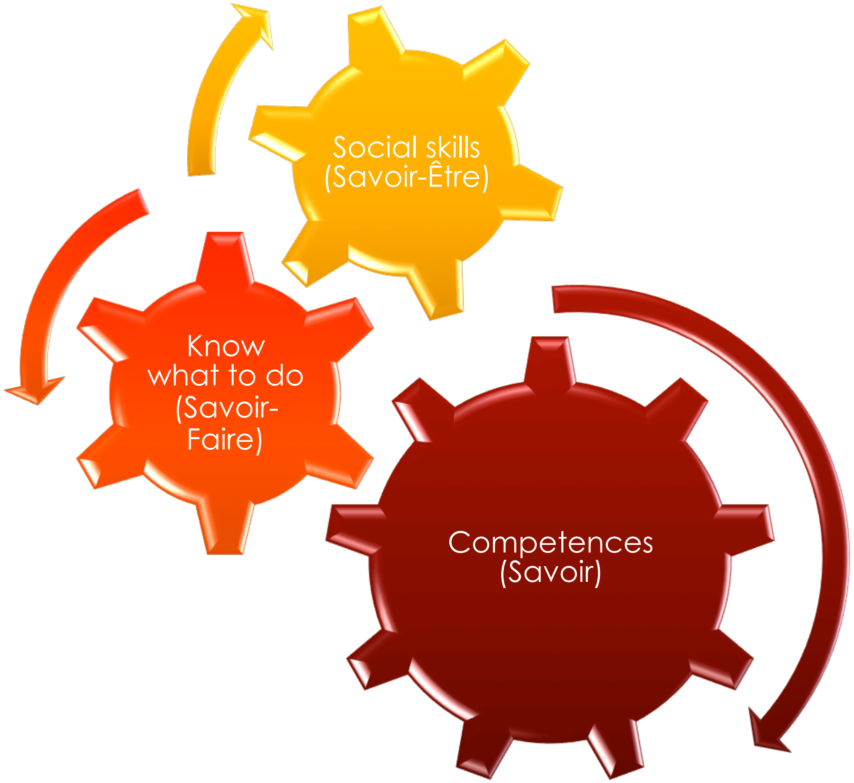
Strategy
Tactics
Operations
Functions

Tasks
Activities

Competences

CISO – full job description

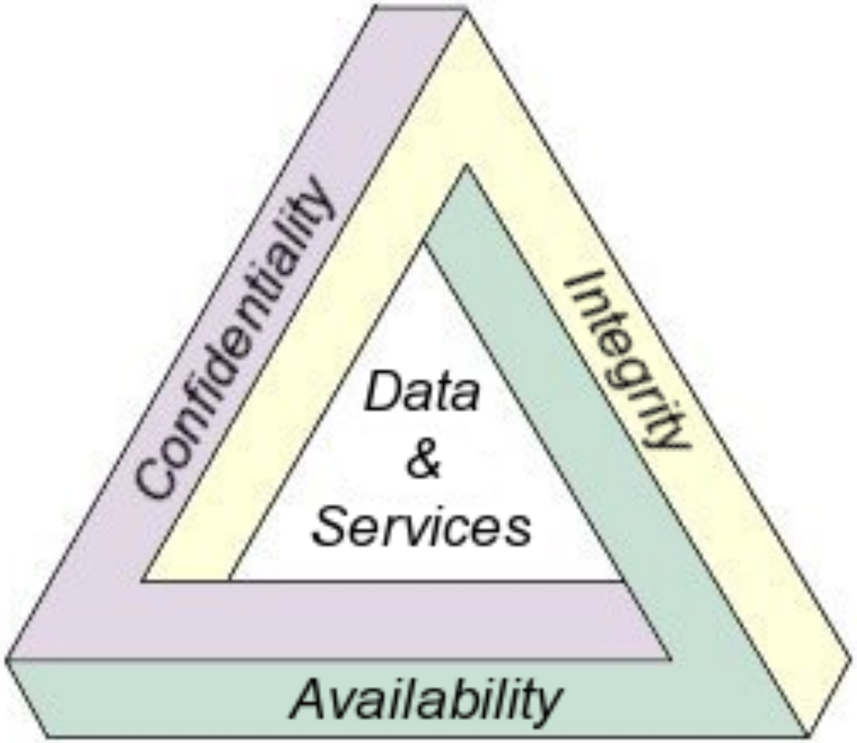




Key information security principles

Information attributes to address, protect

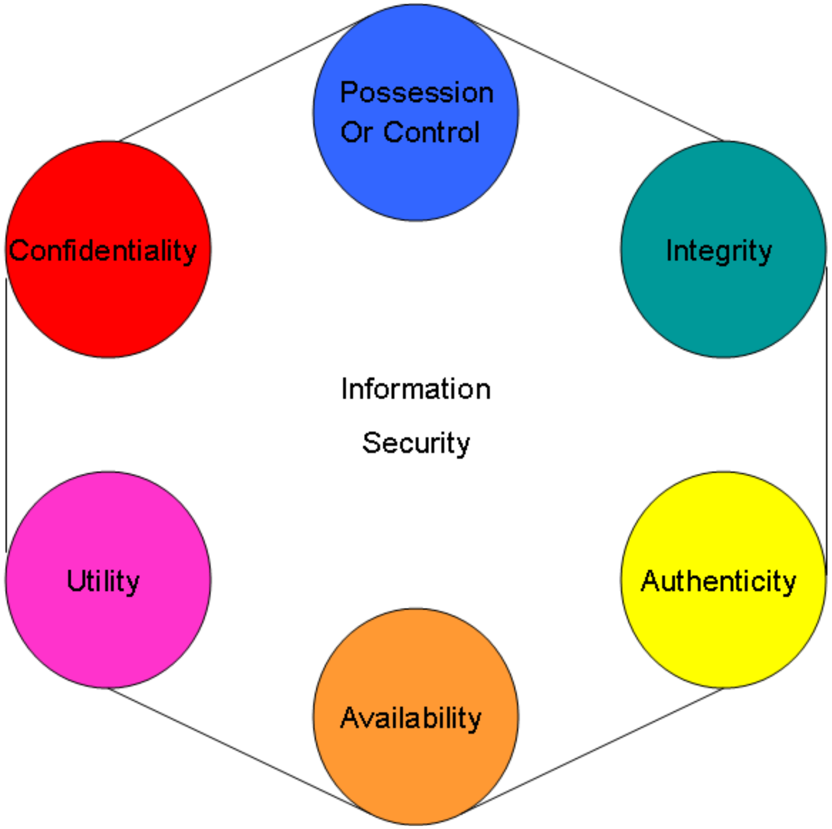
CIA triad (the static model)



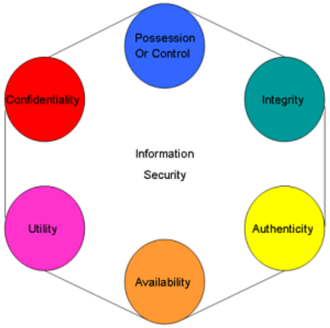
A process view of things

- Authentication(confidentiality)(who are you, are you allowed to use/read)
- Authorization (integrity) (what are you allowed to do, modify)
- Availability (is the data accessible)
- Authenticity (is the data intact)
- Non-repudiation (cannot deny action)
- *”Admissibility” (the state or quality of being admissible or allowable)*

Parkerian Hexad



Parkerian Hexad - explained

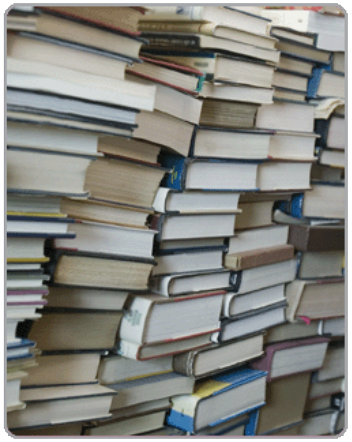


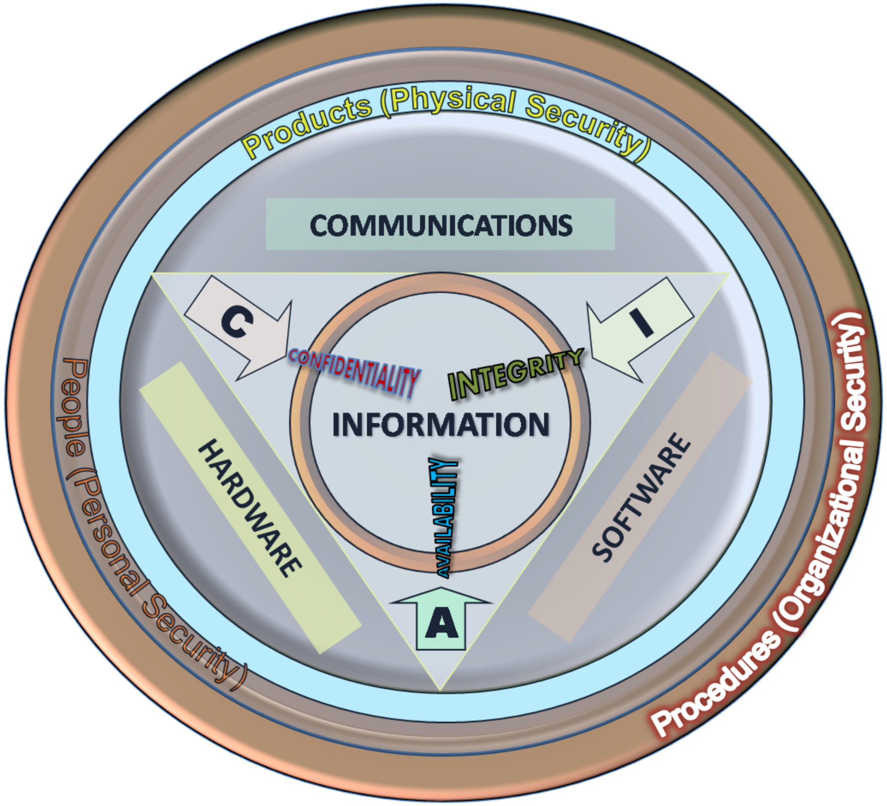
- Possession or Control
  - Suppose a thief were to steal a sealed envelope containing a bank debit card and (foolishly) its personal identification number. Even if the thief did not open that envelope, the victim of the theft would legitimately be concerned that (s)he could do so at any time without the control of the owner. That situation illustrates a loss of control or possession of information but does not involve the breach of confidentiality.
- Authenticity
  - refers to correct labeling or attribution of information. For example, if a criminal forges e-mail headers to make it look as if an innocent person is sending threatening e-mail messages, there has been no breach of confidentiality (the thief uses his or her own e-mail account), possession (no information has been taken out of the control of the victim), or integrity (the e-mail messages are exactly as intended by the criminal). What is breached is authenticity: the e-mail is incorrectly attributed to someone else. Similarly, misusing a field in a database to store information that is incorrectly labeled is a breach of authenticity; e.g., storing a merchant's tax code in a field labeled as the merchant's ZIP code would violate the authenticity of the information.
- Utility
  - means usefulness. For example, suppose someone encrypted data on disk to prevent unauthorized access or undetected modifica- tions – and then lost the decryption key: that would be a breach of util- ity. The data would be confidential, controlled, integral, authentic, and available – they just wouldn't be useful in that form. Similarly, conver- sion of salary data from one currency into an inappropriate currency would be a breach of utility, as would the storage of data in a format in- appropriate for a specific computer architecture; e.g., EBCDIC instead of ASCII or 9-track magnetic tape instead of DVD-ROM. A tabular representation of data substituted for a graph could be described as a breach of utility if the substitution made it more difficult to interpret the data. Utility is often confused with availability because breaches such as those described in these examples may also require time to work around the change in data format or presentation. However, the concept of usefulness is distinct from that of availability.

The CISO’s toolbox

Risk Assessment, Information Security Policy, ISMS

Formalize information security




Products (Physical Security)
COMMUNICATIONS
C
I
CONFIDENTIALITY
INTEGRITY
INFORMATION
HARDWARE
SOFTWARE
AVAILABILITY
A
People (Personal Security)
Procedures (Organizational Security)

Information security vocabulary

- **Risk** combination of the probability of an event and its consequence. NOTE: The term ”risk” is generally used only when there is at least the possibility of negative consequences
- **Risk treatment** process of selection and implementation of options to modify risk. NOTE: Risk treatment options can include avoiding, reducing, transferring or retaining risk.
- **Residual risk** risk remaining after risk treatment
- **ISMS** that part of the overall management system, based on a business risk approach, to establish, implement, operate, monitor, review, maintain and improve information security
- **Information security policy** A policy approved by the management that demonstrates support for, and commitment to information security.

Risk Assessment (ISO/IEC 27005)

- **Risk assessment** overall process of risk analysis and risk evaluation
- The risk equation:

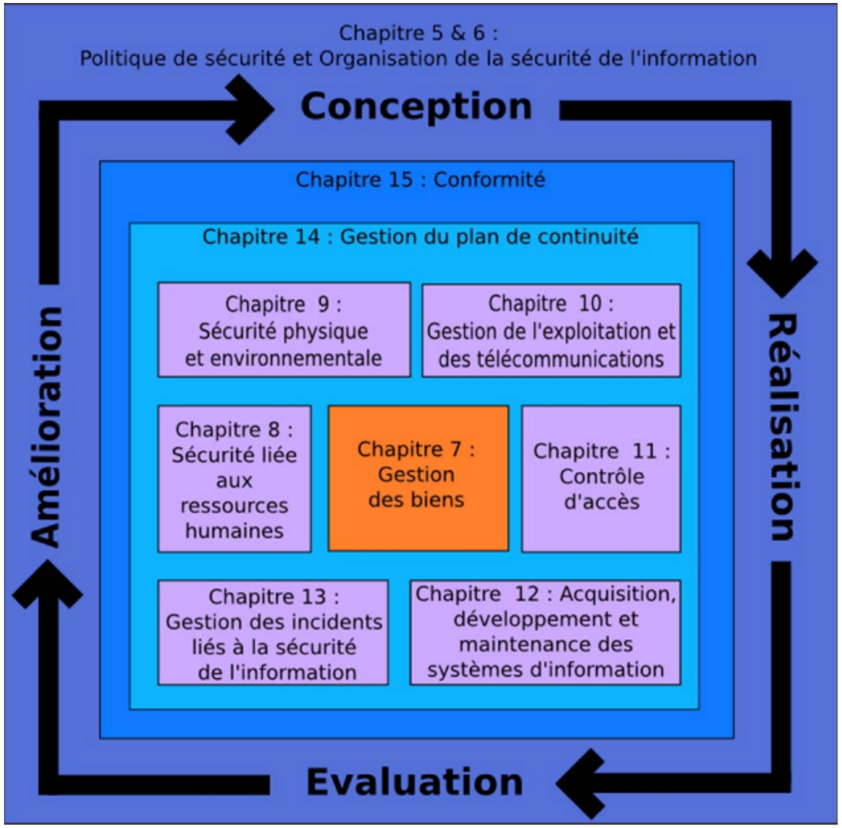
  Risk = Vulnerability * Threat * Impact

- **Threat** a potential source of an incident that may result in adverse changes to an asset, a group of assets or an organization
- **Vulnerability** weakness in an information system, system security procedures, internal controls, or implementation that could be exploited or triggered by a threat
- **Impact**: adverse change to the level of business objectives achieved

Risk Assessment (ISO/IEC 27005)

- **Asset**: anything that has value to the organization, there are many types of assets, including:
  - (a) information
  - (b) software assets
  - (c) physical assets
  - (d) people, and their qualifications, skills, and experience
  - (e) intangibles, such as reputation and image.
- **Attack** attempt that results in breaching the security policy by destroying, exposing, altering, disabling or gaining unauthorized access to assets

Information Security Policy (ISO/IEC 27002)



Chapitre 5 & 6 :
Politique de sécurité et Organisation de la sécurité de l'information

Conception

Réalisation

Evaluation

Amélioration

Chapitre 15 : Conformité

Chapitre 14 : Gestion du plan de continuité

Chapitre 9 : Sécurité physique et environnementale

Chapitre 10 : Gestion de l'exploitation et des télécommunications

Chapitre 8 : Sécurité liée aux ressources humaines

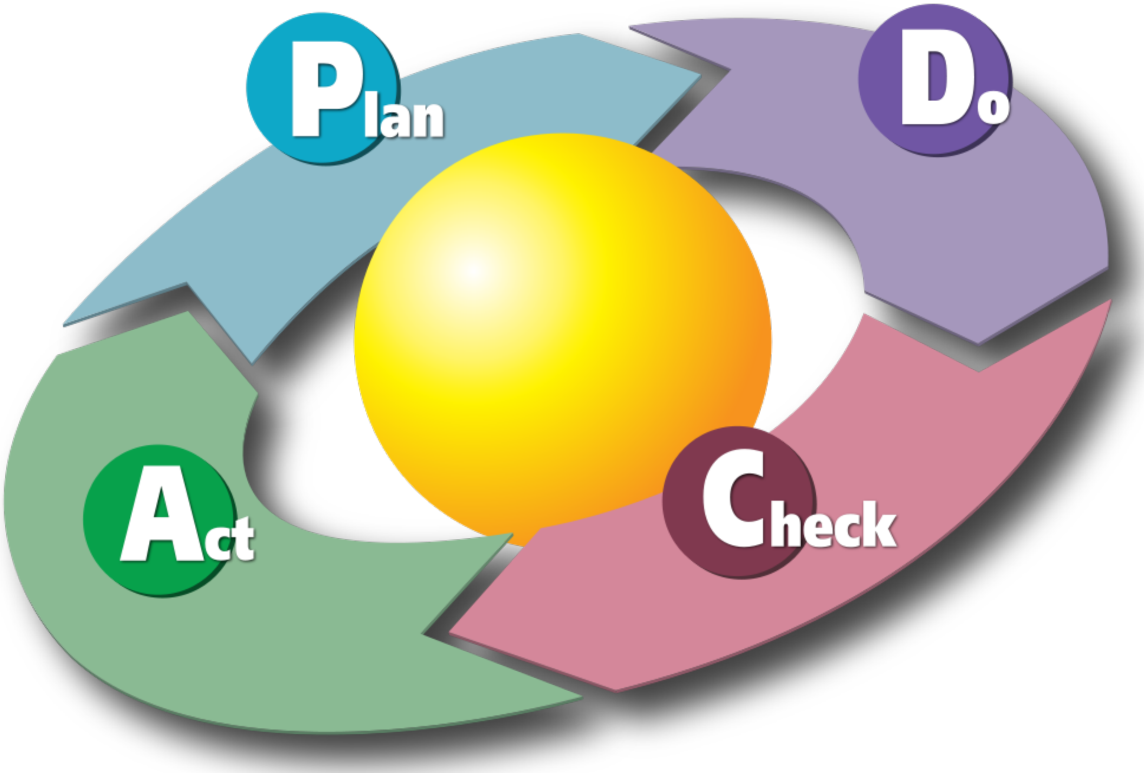
Chapitre 7 : Gestion des biens

Chapitre 11 : Contrôle d'accès

Chapitre 13 : Gestion des incidents liés à la sécurité de l'information

Chapitre 12 : Acquisition, développement et maintenance des systèmes d'information

ISMS
Information Security Management System
(ISO/IEC 27001)

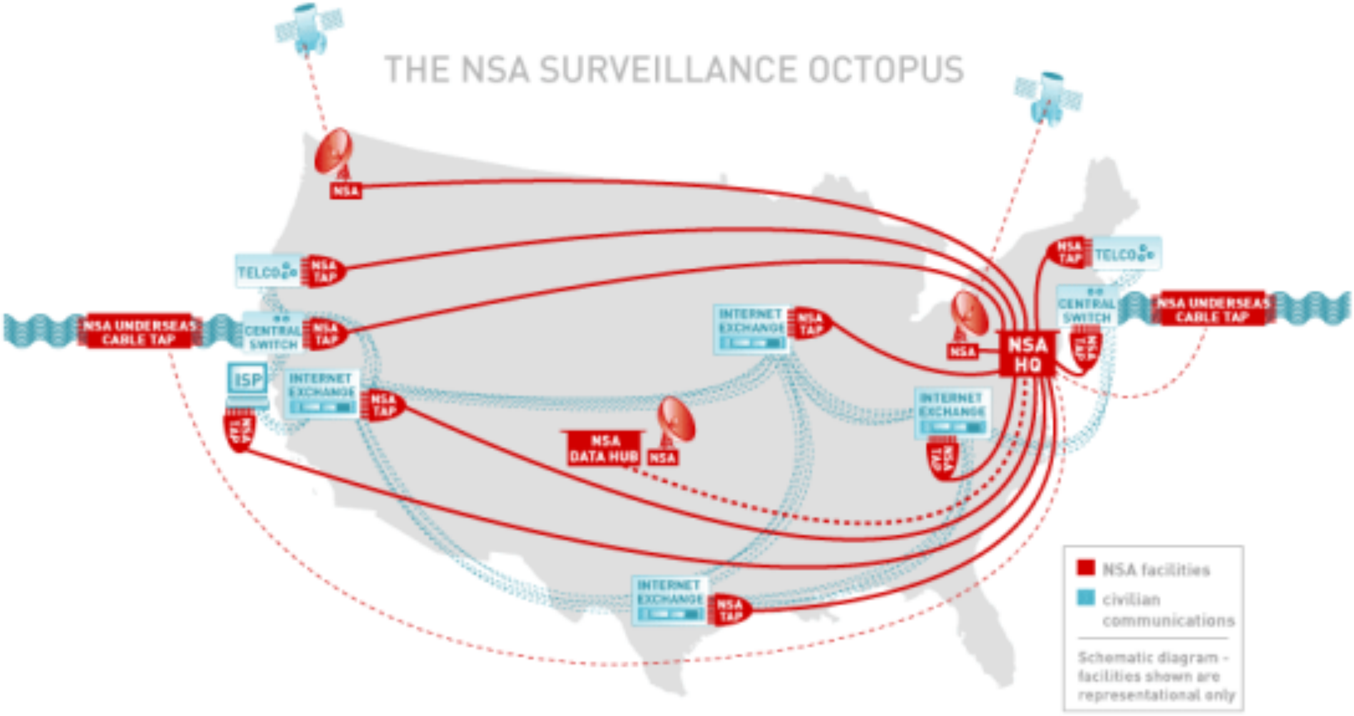


Background & references

NSA
National Security Agency

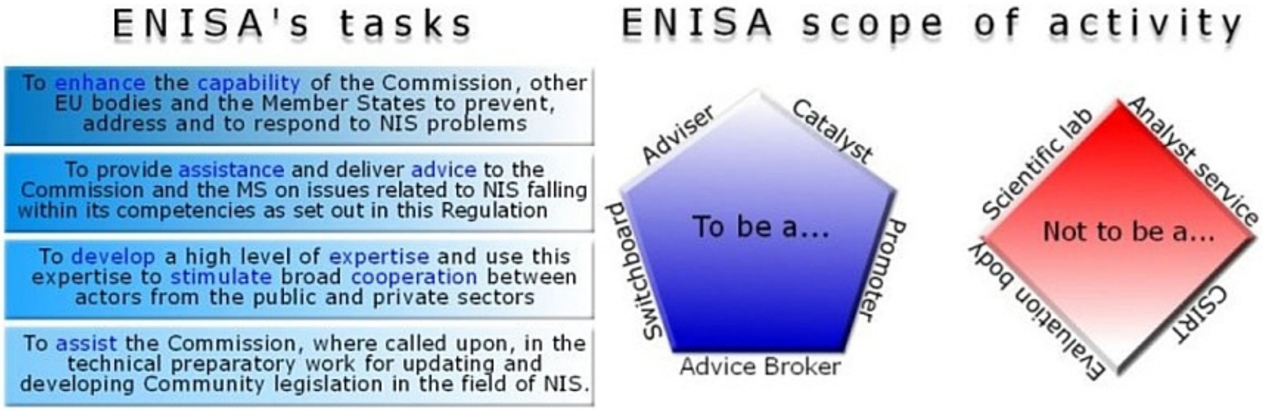
”The ability to understand the secret communications of our foreign adversaries while protecting our own communications – a capability in which the United States leads the world – gives our nation a unique advantage.”

The NSA “octopus”



ENISA

European Network and Information Security Agency



ENISA's tasks

To enhance the capability of the Commission, other EU bodies and the Member States to prevent, address and to respond to NIS problems

To provide assistance and deliver advice to the Commission and the MS on issues related to NIS falling within its competencies as set out in this Regulation

To develop a high level of expertise and use this expertise to stimulate broad cooperation between actors from the public and private sectors

To assist the Commission, where called upon, in the technical preparatory work for updating and developing Community legislation in the field of NIS.

ENISA scope of activity

CCDCOE
Cooperative Cyber Defence Centre of Excellence

- The main agenda of the facility is to:
  - **Improve** cyber defence **interoperability** within the NATO Network Enabled Capability (NNEC) environment,
  - **design** the doctrine and concept development and their validation,
  - enhance information security and cyber defence **education, awareness, and training**,
  - provide cyber defence support for **experimentation** (including on-site) for experimentation,
  - analyzing the **legal aspects** of cyber defence.

- The centre has also other responsibilities which include:
  - contribution to development of Cyber Defense Center **practices and standards** with NATO, PfP, NATO candidates and non-NATO nations,
  - contribution to development of NATO **security policies** related to cyber defence its definition of scope and responsibility of military in cyber defence,
  - carrying out cyber defence-focused **training, awareness campaigns**, workshops, and courses,
  - developing and conducting cyber defence-focused **exercises** and its ability to provide CD exercise support,
  - providing cyber defence SMEs to NATO and its ability in cyber defence **testing and validating.**

CCDCOE

Cooperative Cyber Defence
Centre of Excellence
Tallinn, Estonia

ANSSI

Agence nationale de la sécurité des systèmes d'information

- Elle a notamment pour mission de :
  - **détecter et réagir** au plus tôt en cas d'attaque informatique, grâce à un centre de détection chargé de la surveillance permanente des réseaux sensibles et de la mise en œuvre de mécanismes de défense adaptés aux attaques ;
  - **prévenir la menace**, en contribuant au développement d'une offre de produits de très haute sécurité ainsi que de produits et services de confiance pour les administrations et les acteurs économiques ;
  - jouer un rôle de **conseil** et de soutien aux **administrations** et aux **opérateurs d'importance vitale** ;
  - **informer** régulièrement le public sur les menaces, notamment par le biais du site Internet gouvernemental de la sécurité informatique, lancé en 2008, qui a vocation à être le portail Internet de référence en matière de sécurité des systèmes d'informations.
- S'agissant des **produits et des réseaux de sécurité**, elle est chargée :
  - de **développer et d'acquérir** les produits essentiels à la protection des réseaux interministériels les plus sensibles de l'État ;
  - de **mettre en œuvre** les moyens gouvernementaux de commandement et de liaison en matière de défense et de sécurité nationale, notamment le réseau Rimbaud et l'intranet Isis ;
  - de **délivrer des labels** aux produits de sécurité.

LU cyber security strategy

1. Protect operational infrastructures and systems of communication and information processing
2. Modernize the legal framework
3. Develop national and international cooperation
4. Inform, educate and raise awareness about risks
5. Establish binding standards and norms

Cyber Security Board