

42. Security and Quality of Information Systems

The **Risk Management Framework (RMF)** is a set of criteria that dictate how United States government IT systems must be architected, secured, and monitored. Originally developed by the Department of Defense (DoD), the RMF was adopted by the rest of the US federal information systems in 2010.

Today, the RMF is maintained by the **National Institute of Standards and Technology (NIST)**, and provides a solid foundation for any data security strategy. The RMF is a 6-step process to architect and engineer a data security process for new IT systems.



to assign a role to a system
to be consistent with sthg
risk assessment
to implement security controls
to remediate a weakness
to strike a balance between X and Y

attribuer/ assigner un rôle à un système
être cohérent par rapport à qqch
évaluation du risque
mettre en place/ exécuter les contrôles de sécurité
corriger une faiblesse
trouver un équilibre entre X et Y

Information security's primary focus is the balanced protection of the confidentiality, integrity and availability of data (also known as the **CIA triad**). Non-repudiation is really important too and has to be associated with the triad.

Data security refers to protective digital privacy measures that are applied to prevent unauthorized access to computers, databases and websites. Data security also protects data from corruption. Data security is an essential aspect of IT for organizations of every size and type. It includes data encryption, tokenization, and key management practices that protect data across all applications and platforms.

encryption
to secure data/ a network
a data security breach
to ensure privacy
to prevent tracking
reliability/ dependability
a leak of information
data confidentiality
data integrity
data availability

cryptage
sécuriser des données/ un réseau
faille de sécurité
garantir/ assurer la confidentialité
empêcher l'espionnage
fiabilité
fuite d'information
confidentialité des données
intégrité des données
disponibilité des données

INTERNET SECURITY

Crackers are individuals who break into computers or network systems. A cracker might be performing cracking for **malicious activities**, profit, for certain nonprofit intentions or causes, or just for a challenge. Some crackers break into a network system deliberately **to point out the flaws** involved in that network's security system. In most cases, crackers aim **to gain access to** confidential data, get hold of software applications for free, or carry out malicious damage to files.



to sabotage a system	saboter un système
to break into a computer	pénétrer/ s'introduire dans un ordinateur
to crack a code	casser un code
to carry out damage	causer des dommages/ dégâts
to commit a crime	perpétrer un crime
data theft	vol de données
to hack into a system	s'introduire dans un système (par effraction)

Black-hat hackers are the stereotypical illegal hacking groups often portrayed in popular culture, and are "the epitome of all that the public fears in a computer criminal". Black hat hackers break into secure networks to destroy, modify, or steal data, or to make the networks unusable for authorized network users.

dark web	darknet
cybercrime	cybercriminalité
a scam	arnaque
email fraud	courriel frauduleux
phishing	hameçonnage
cyberbullying	cyber harcèlement
cyberstalking	cyber prédation
piracy	piratage
copyright piracy	violation des droits d'auteur
computer hacking	piratage informatique

The term "**white hat**" in Internet slang refers to an ethical computer hacker, or a computer security expert, who specializes in **penetration testing** and in other testing methodologies that ensures the security of an organization's information systems. Ethical hacking is a term meant to imply a broader category than just penetration testing.

Chief Information Security Officer	
Chief Security Officer	
to identify vulnerabilities	repérer les failles
a security expert	spécialiste de la sécurité
an engineer	ingénieur
to put/ place at risk	mettre en danger
to foil a hacking attempt	déjouer une tentative de piratage

Malware (malicious software) is software that is specifically designed to disrupt, damage, or gain unauthorized access to a computer system.

a virus	virus
executable files	fichiers exécutables
to run an infected program	executer un programme corrompu
to spread/ to propagate	se répandre/ se propager
an attachment	pièce jointe
a worm	ver
a Trojan horse	cheval de Troie
a spyware	logiciel espion
a ransomware	rançongiciel
an adware	publiciel/ logiciel publicitaire

a security flaw	faille de sécurité
a denial-of-service attack	attaque par déni de service
a backdoor	porte dérobée
a botnet	réseau de zombies
to be embedded in	être intégré/ imbriqué dans
to collect stored data	collecter des données stockées

A **digital certificate** authenticates the Web credentials of the sender and lets the recipient of an encrypted message know that the data is from a trusted source (or a sender who claims to be one). A digital certificate is issued by a certification authority (CA). Digital certificates are used with signatures and message encryption. Digital certificates are also known as **public key certificates** or **identity certificates**.

authentication	authentification
an anti-virus software	logiciel anti-virus
a firewall	pare-feu
content filtering	filtrage de contenu
checksum	somme/ total de contrôle
a back-up copy	copie de sauvegarde
a cybercop	cyber-policier

Useful acronyms:

RMF Risk Management Framework
NIST National Institute of Standards and Technology
DES Data Encryption Standard
TOR The Onion Router

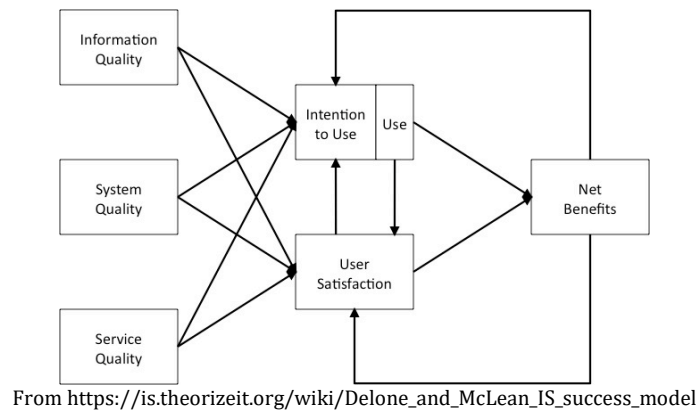
QUALITY

Many companies continually strive toward creating and maintaining quality products and processes. What is vitally important, but is often overlooked (*négligé*) in the literature, is that to achieve a quality organization, you must begin by emphasizing the importance of creating and maintaining quality data and information systems. Information pervades all activities of an organization, and without efforts to collect, store, and process data in a manner that ensures quality information, the organization's ability to promote total quality will be severely lessened.

to assess quality	évaluer la qualité
quality control	contrôle qualité
to comply with standards	se conformer à des normes
a user interface	interface utilisateur
to adjust a technology	ajuster une technologie

Information system quality is expected to have a strong impact on information **system effectiveness**. With proper business/IT alignment, an effective information system is an information system that successfully plays a central role in the fulfillment of strategic business goals like cost leadership, **increased profitability** or sustained growth.

A framework that explains the relationship between information system quality and information system effectiveness is the **DeLone and McLean (D&M) Model of IS Success** according to which, information system quality affects both the use of the information system (i.e. whether the information system is adopted by its intended users) and how satisfied the intended users are with this use.



user satisfaction
 user-friendliness
 usability
 accuracy
 practicality
 increased profitability

satisfaction de l'utilisateur
 convivialité/ ergonomie
 facilité d'utilisation
 précision
 aspect pratique
 rentabilité accrue

to meet a purpose
 to malfunction
 to fail

remplir un objectif
 dysfonctionner
 échouer

VOCABULARY EXERCISES

EXERCISE 1: Form 4 compound nouns with the following elements and translate them into French.
 digital/ divide/ engine/ identity/ provider/ search/ service/ theft

EXERCISE 2: Fill in the following sentences with the right preposition or particle.

1. It is necessary to assign a role ____ local education actors in the development of cluster and resource center activities.
2. Some offshore outsourcing initiatives are embedded ____ a broader restructuring strategy, while others aim to tackle a specific identified 'problem'.
3. Working outdoors at midday we were put ____ risk of severe sunburn.
4. A firm that specializes ____ the analysis of handwriting claims from a one-page writing sample that it can assess more than three hundred personality traits
5. Today's tech savvy criminals can hack ____ your computer system to gain access ____ sensitive information about you, your business and your customers.
6. Everyone has the right to point ____ flaws in the law and to work towards changing these laws - lawfully, of course.
7. Voluntary contributions are accepted provided they are consistent ____ the policies and objectives of the program.

EXERCISE 3: Fill in the following definitions with the right compound based on "access".

access control list (ACL)	access path	access point	access profile	access rights
network access				

1. **An** _____ is a device, such as a wireless router, that allows wireless devices to connect to a network. Most access points have built-in routers, while others must be connected to a router in order to provide _____.
2. An _____ defines the functions to which a specific user has access.

3. The permissions that are granted to a user, or to an application, to read, write and erase files in the computer are called _____. They can be tied to a particular client or server, to folders within that machine or to specific programs and data files.
4. An _____ specifies the path chosen by a database management system to retrieve the requested tuples from a relation.
5. An _____, with respect to a computer file system, is a list of permissions attached to an object. It specifies which users or system processes are granted access to objects, as well as what operations are allowed on given objects.

CORRECTION of the VOCABULARY EXERCISES

EXERCISE 1: Form 4 compound nouns with the following elements and translate them into French.

digital divide	fossé/ fracture numérique
search engine	moteur de recherche
identity theft	vol d'identité
service provider	fournisseur d'accès

EXERCISE 2: Fill in the following sentences with the right preposition or particle.

1. It is necessary to assign a role to local education actors in the development of cluster and resource center activities.
2. Some offshore outsourcing initiatives are embedded in a broader restructuring strategy, while others aim to tackle a specific identified 'problem'.
3. Working outdoors at midday we were put at risk of severe sunburn.
4. A firm that specializes in the analysis of handwriting claims from a one-page writing sample that it can assess more than three hundred personality traits
5. Today's tech savvy criminals can hack into your computer system to gain access to sensitive information about you, your business and your customers.
6. Everyone has the right to point out flaws in the law and to work towards changing these laws - lawfully, of course.
7. Voluntary contributions are accepted provided they are consistent with the policies and objectives of the program.

EXERCISE 3: Fill in the following definitions with the right compound based on "access".

access control list (ACL)	access path	access point	access profile	access rights
network access				

1. An **access point** is a device, such as a wireless router, that allows wireless devices to connect to a network. Most access points have built-in routers, while others must be connected to a router in order to provide **network access**.
2. An **access profile** defines the functions to which a specific user has access.
3. The permissions that are granted to a user, or to an application, to read, write and erase files in the computer are called **access rights**. They can be tied to a particular client or server, to folders within that machine or to specific programs and data files.
4. An **access path** specifies the path chosen by a database management system to retrieve the requested tuples from a relation.
5. An **access-control list (ACL)**, with respect to a computer file system, is a list of permissions attached to an object. An ACL specifies which users or system processes are granted access to objects, as well as what operations are allowed on given objects.

UNDERSTANDING

EXERCISE 1: About Risks.

Risk Management Frameworks

Organizations have faced, and will continue to face, multiple challenges with regards to information security and privacy, including the growing need to demonstrate compliance with multiple federal, state and industry requirements. However, given the general lack of definition and prescriptiveness of these requirements, organizations are left with the task of deciding what actions would be considered 'reasonable and appropriate' and what level of protection would be 'adequate' in the eyes of federal, state and industry regulators, business partners, customers, and other interested third parties. Implementing the right framework, processes and tools is the only efficient and effective way to manage information risk and compliance.

So, how can an organization determine 'reasonable and appropriate' safeguards to provide 'adequate' protection for sensitive information? Or stated another way, how can an organization select and implement a specific set of controls to manage information security and privacy-related risk at an acceptable level?

The textbook answer is through a comprehensive risk analysis that (1) includes threat and vulnerability assessments, information asset valuation, and the selection of a comprehensive set of information security and privacy controls that addresses the enumerated threat-vulnerability pairs (a process sometimes referred to as threat modeling), (2) is cost-effective, and (3) manages risk at a level deemed acceptable by the organization.

From a quantitative viewpoint, this process is virtually impossible for many—if not most—organizations to perform. For example, unless actuarial-type information is available, the likelihood a threat-source will successfully exploit one or more vulnerabilities cannot be calculated with any level of precision. In the case of a human actor, likelihood is also dependent on the motivation of the threat source and the difficulty or cost associated with exploiting one or more vulnerabilities to achieve the threat actor's objectives. As a result, it is similarly difficult to develop a valid business case for a specific risk response or treatment based on a return on investment. Organizations could take a semi- or quasi-quantitative approach or even a purely qualitative approach; however, it would still be difficult for an organization to develop a valid business case, particularly for a comprehensive set of risk responses.

An alternative approach is to rely on other organizations that do have the resources to develop a set of controls that addresses similar threats to similar technologies employed by their own organization. Risk management frameworks support a basic 4-step risk management process model:

Step 1 - _____

The objective of this step is to determine the risks to information and information assets that are specific to the organization. Risks can be identified through the analysis of regulations and legislative requirements, breach data for similar organizations in the industry, as well as an analysis of current architectures, technologies and market trends. The end result of this analysis should be a prioritized list of high-risk areas and an overall control strategy to minimize the risk to the organization from the use of sensitive or business critical information in terms of overall impact to the organization.

This step is supported by seven sub-processes, which range from the classification of information assets to the development of specific risk treatments. As indicated previously, this is one of the more problematic aspects of risk analysis that a control-based risk management framework will help an organization address.

Step 2 - _____

The next step is to determine a set of reasonable and appropriate safeguards an organization should implement to adequately manage information security risk. The end result should be a clear, consistent and detailed or prescriptive set of control recommendations that are customized for the organization.

A control-based risk management framework will provide a comprehensive control catalog derived from the seven sub-processes outlined earlier as well as specific criteria for the selection of a baseline set of controls, which is performed in this step.

Step 3 - _____

Controls are implemented through an organization's normal operational and capital budget and work processes with board-level and senior executive oversight using existing governance structures and

processes. A risk management framework will provide guidance and tools for implementation of the framework, including the controls specified earlier in step 2.

Step 4 - _____

The objective of this last step is to assess the efficacy of implemented controls and the general management of information security against the organization's baseline. The result of these assessment and reporting activities is a risk model that assesses internal controls and those of business associates based on well-defined risk factors. It should also provide common, easy-to-use tools that address requirements and risk without being burdensome, support third-party review and validation, and provide common reports on risk and compliance.

<https://hitrustalliance.net/documents/campaigns/HITRUST-RMF-Whitepaper-FM.pdf>, 2018

After reading the text, answer the following questions.

1. According to that document, who are the main stakeholders of a company concerned by the level of protection of the company's data?
2. What must a well-designed risk analysis include?
3. Why is it so difficult for organizations to carry out an effective risk analysis?
4. Give a title to each step of the risk management process model.

EXERCISE 2: About Data Security

"In July 2009, Amazon Kindle readers found life imitating art when their copy of Orwell's novel *1984* completely disappeared from their devices. In *1984*, the 'memory hole' is used to incinerate documents that are considered subversive or no longer wanted. Documents permanently disappear and history is rewritten.

It could almost have been an unfortunate prank but *1984* and Orwell's *Animal Farm* had actually been removed as the result of a dispute between Amazon and the publisher. Customers were angry, having paid for the e-book and assumed that it was therefore their property. A lawsuit filed by a high school student and one other person was settled out of court. In the settlement, Amazon stated that they would no longer erase books from people's Kindles, except in certain circumstances, including that '*a judicial or regulatory order requires such deletion or modification.*' Amazon offered customers a refund, gift certificate, or to restore the deleted books. In addition to being unable to sell or to lend our Kindle books, it seems we do not actually own them at all.

Although the Kindle incident was in response to a legal problem and was not intended maliciously, it serves to illustrate how straightforward it is to delete e-documents, and without hard copies, how simple it would be to completely eradicate any text viewed as undesirable or subversive. If you pick up the physical version of the book tomorrow and read it, you know with absolute certainty it will be the same as it was today but if you read anything on the Web today you cannot be certain that it will be the same when you read it tomorrow."

From *Big Data*, by Dawn E. Holmes, pp.90-91.

After reading the text, answer the following questions.

1. Sum up in your own words what Amazon did in 2009 and the reasons why they did it.
2. Explain why it is ironic.
3. What were the consequences of Amazon's action?
4. What conclusion does the author draw from the incident?

CORRECTION of the UNDERSTANDING PART

EXERCISE 1

1. According to that document, who are the main stakeholders of a company concerned by the level of protection of the company's data?

The main stakeholders mentioned in the document are: federal, state and industry regulators, business partners and customers.

2. What must a well-designed risk analysis include?

It must:

- evaluate the threats to the system and its vulnerability,
- inventory the information assets of the organization,
- opt for a comprehensive set of information security and privacy controls that addresses the threat-vulnerability pairs that are pointed out in the process,
- be cost-effective.

3. Why is it so difficult for organizations to carry out an effective risk analysis?

It is difficult for companies to assess the probability a threat-source will successfully exploit one or more vulnerabilities. Plus, if the threat is posed by a human actor, the probability of the threat will depend on the motivation of the source and the difficulty or cost associated with exploiting one or more vulnerabilities to achieve the threat actor's objectives. That is why it is not easy to develop a valid business case for a specific risk response.

4. Give a title to each step of the risk management process model.

- Step 1—Identify risks and define protection requirements
- Step 2—Specify controls
- Step 3—Implement and manage controls
- Step 4—Assess and report

For more info on RMFs:

<https://www.ncsc.gov.uk/collection/risk-management-collection>

<https://www.enisa.europa.eu/>

EXERCISE 2

1. Sum up in your own words what Amazon did in 2009 and the reasons why they did it.

In 2009 Amazon remotely deleted some digital editions of *1984* and *The Animal Farm* by G. Orwell from the Kindle devices of readers who had bought them.

An Amazon spokesman, Drew Herdener, said in an e-mail message that the books were added to the Kindle store by a company that did not have rights to them, using a self-service function. "When we were notified of this by the rights holder, we removed the illegal copies from our systems and from customers' devices."

2. Explain why it is ironic.

It is ironic because in George Orwell's *1984*, government censors erase all traces of news articles embarrassing to Big Brother by sending them down an incineration chute called the "memory hole." On that occasion, it was *1984* itself that was dropped down the memory hole — by Amazon.com.

3. What were the consequences of Amazon's action?

Some customers sued Amazon for damage. The company offered customers a refund, gift certificate, or to restore the deleted books. They also had to alter their systems so that in the future they would not remove books from customers' devices in these circumstances.

4. What conclusion does the author draw from the incident?

It illustrates how few rights you have when you buy an e-book from Amazon and also raises the question of the reliability of digital content over the years.