

Master en Management de la Sécurité des Systèmes d'Information

Semester 1

	Vorlesung (UE)	Übung (UE)	ECTS
<p>Module 1 : Understanding Organisations & Management (Compréhension des organisations et du management) : Ce module est le premier module d'introduction au contexte de la sécurité de l'information en entreprise. Les matières sont abordées en lien constant avec la sécurité de l'information. But : Préciser les éléments de contexte internes à l'entreprise dans lesquels va s'exercer le métier de responsable de la sécurité de l'information. Objectifs : Familiariser les étudiants avec les composantes, les mécanismes et les propriétés des organisations de tout type d'une part et de certains métiers de support abordés sous l'angle général de la gestion d'autre part. Améliorer, pour le domaine de la sécurité de l'information, la performance des étudiants dans l'intégration de leurs pratiques et l'atteinte de leurs objectifs dans les organisations. Ouvrir aux étudiants des domaines connexes et leurs outils de gestion mis au service de leur métier.</p>			9
<p>1.1 Organisational Theory and Change (Théorie des organisations et du changement)</p>	16		2
<p>Module 2 : Regulatory Frameworks (Cadres réglementaires) : Ce module est le second module d'introduction au contexte de la sécurité de l'information en entreprise. Les matières sont abordées en lien constant avec la sécurité de l'information. But : Préciser les éléments du cadre réglementaire et contextuel dans lequel va s'exercer le métier de responsable de la sécurité de l'information. Objectifs : Familiariser les étudiants avec les aspects réglementaires et répressifs Familiariser les étudiants avec des secteurs d'activités particuliers Faire prendre conscience aux étudiants des évolutions et des spécificités qui vont être induites sur leurs pratiques professionnelles</p>			7
<p>2.1 Legal and Regulatory Aspects (Aspect légaux et réglementaires)</p>	24		3
<p>Module 3 : Information Security Management (Gestion de la sécurité de l'information) : Ce module est le premier des deux modules centraux de la formation. Ces matières sont une partie émergente du cœur de métier actuel de la sécurité de l'information. But : Installer le contenu organisationnel nécessaire pour gérer une sécurité de l'information moderne en entreprise. Objectifs : Familiariser les étudiants avec les méthodes et outils nécessaires à la gestion de la sécurité de l'information Maîtriser les caractéristiques, les propriétés et les diverses utilisations possibles de ces fonctionnalités (politique de sécurité, conformité aux référentiels de sécurité, continuité de service) Déployer les grandes fonctionnalités de la sécurité de l'information en rapport avec sa gestion (ISMS, normes applicables)</p>			10
<p>3.1 Information Security Management System - IMS (Systèmes de Management de la Sécurité de l'Information - SMSI)</p>	16		2
<p>Module 3 : Information Security Management (Gestion de la sécurité de l'information) : Ce module est le premier des deux modules centraux de la formation. Ces matières sont une partie émergente du cœur de métier actuel de la sécurité de l'information. But : Installer le contenu organisationnel nécessaire pour gérer une sécurité de l'information moderne en entreprise. Objectifs : Familiariser les étudiants avec les méthodes et outils nécessaires à la gestion de la</p>			10

Master en Management de la Sécurité des Systèmes d'Information

	Vorlesung (UE)	Übung (UE)	ECTS
sécurité de l'information Maitriser les caractéristiques, les propriétés et les diverses utilisations possibles de ces fonctionnalités (politique de sécurité, conformité aux référentiels de sécurité, continuité de service) Déployer les grandes fonctionnalités de la sécurité de l'information en rapport avec sa gestion (ISMS, normes applicables)			
3.2 Risk Analysis and Management (Analyse et gestion de risques)	16		2
<p>Module 3 : Information Security Management (Gestion de la sécurité de l'information) : Ce module est le premier des deux modules centraux de la formation. Ces matières sont une partie émergente du cœur de métier actuel de la sécurité de l'information. But : Installer le contenu organisationnel nécessaire pour gérer une sécurité de l'information moderne en entreprise. Objectifs : Familiariser les étudiants avec les méthodes et outils nécessaires à la gestion de la sécurité de l'information Maitriser les caractéristiques, les propriétés et les diverses utilisations possibles de ces fonctionnalités (politique de sécurité, conformité aux référentiels de sécurité, continuité de service) Déployer les grandes fonctionnalités de la sécurité de l'information en rapport avec sa gestion (ISMS, normes applicables)</p>			10
3.3 Risk Analysis Practices (Pratiques d'analyse de risques)	8		1
<p>Module 4 : Technical Aspects (Aspects techniques) : Ce module est le second des deux modules centraux de la formation. Ces matières font parties du cœur de métier historique de la sécurité de l'information. But : Permettre aux étudiants de disposer des connaissances pour comprendre les différentes couches techniques devant être sécurisées dans un système d'information. Objectifs : Il s'agit de savoir traduire en termes techniques les analyses produites par le module de gestion de la sécurité. Parmi les compétences à acquérir, le module comprend un cours sur les technologies et les composants de sécurité (Technologie de la sécurité) dont se servent la majorité des solutions de sécurité (chiffrement, gestion des clés). Un second cours permet d'avoir la vision des différentes couches techniques (réseau/communication, traitement et persistance) impliquées dans un système d'information ouvert sur Internet, avec un accent mis sur les vulnérabilités propres à chacune de ces couches. Un troisième cours permet de comprendre et de décortiquer les attaques récentes, afin de mieux appréhender les parades possibles. : Familiariser les étudiants avec les principes, les propriétés et les mécanismes de la sécurité de l'information et les technologies associés. Donner une vue générale et des références sur un plan technique de la sécurité de l'information Approfondir les parties importantes et les fondamentaux du domaine</p>			12
4.1 Information Security 1 (Technologies de la sécurité 1)	16		2
<p>Module 6 : Professional Part (Volet professionnel) : Ce module représente à lui seul le volet professionnel de la formation qu'il encadre au tout début et en toute fin du cycle de deux années. Les activités sont centrées sur la sécurité de l'information, l'exercice de la responsabilité de la sécurité de l'information et la professionnalisation des pratiques. But : Préparer par la pratique l'étudiant à l'exercice de la responsabilité de la sécurité de l'information et de la profession associée. Objectifs : Réaliser une synthèse démonstrative de toutes les compétences apportées par les enseignements que l'étudiant a suivis dans les modules précédents en lui faisant réaliser un projet professionnel. Familiariser l'étudiant avec les réalités et la professionnalisation des pratiques du</p>			18

Master en Management de la Sécurité des Systèmes d'Information

	Vorlesung (UE)	Übung (UE)	ECTS
métier de responsable de la sécurité de l'information. Étudier le métier de responsable de la sécurité de l'information. Réaliser une application de ce métier à travers un projet professionnel.			
6.1 Working in Information Security Management (Le métier de responsable de la sécurité de l'information)	8		1

Semester 2

	Vorlesung (UE)	Übung (UE)	ECTS
Module 1 : Understanding Organisations & Management (Compréhension des organisations et du management) : Ce module est le premier module d'introduction au contexte de la sécurité de l'information en entreprise. Les matières sont abordées en lien constant avec la sécurité de l'information. But : Préciser les éléments de contexte internes à l'entreprise dans lesquels va s'exercer le métier de responsable de la sécurité de l'information. Objectifs : Familiariser les étudiants avec les composantes, les mécanismes et les propriétés des organisations de tout type d'une part et de certains métiers de support abordés sous l'angle général de la gestion d'autre part. Améliorer, pour le domaine de la sécurité de l'information, la performance des étudiants dans l'intégration de leurs pratiques et l'atteinte de leurs objectifs dans les organisations. Ouvrir aux étudiants des domaines connexes et leurs outils de gestion mis au service de leur métier.			
1.2. Architecture and Business Strategy (Architecture et stratégie des entreprises)	24		3

Module 1 : Understanding Organisations & Management (Compréhension des organisations et du management) : Ce module est le premier module d'introduction au contexte de la sécurité de l'information en entreprise. Les matières sont abordées en lien constant avec la sécurité de l'information. But : Préciser les éléments de contexte internes à l'entreprise dans lesquels va s'exercer le métier de responsable de la sécurité de l'information. Objectifs : Familiariser les étudiants avec les composantes, les mécanismes et les propriétés des organisations de tout type d'une part et de certains métiers de support abordés sous l'angle général de la gestion d'autre part. Améliorer, pour le domaine de la sécurité de l'information, la performance des étudiants dans l'intégration de leurs pratiques et l'atteinte de leurs objectifs dans les organisations. Ouvrir aux étudiants des domaines connexes et leurs outils de gestion mis au service de leur métier.			
--	--	--	--

1.3 Financial Management (Gestion financière)	8		1
Module 1 : Understanding Organisations & Management (Compréhension des organisations et du management) : Ce module est le premier module d'introduction au contexte de la sécurité de l'information en entreprise. Les matières sont abordées en lien constant avec la sécurité de l'information. But : Préciser les éléments de contexte internes à l'entreprise dans lesquels va s'exercer le métier de responsable de la sécurité de l'information. Objectifs : Familiariser les étudiants avec les composantes, les mécanismes et les propriétés des organisations de tout type d'une part et de certains métiers de support abordés sous l'angle général de la gestion d'autre			

Master en Management de la Sécurité des Systèmes d'Information

	Vorlesung (UE)	Übung (UE)	ECTS
part. Améliorer, pour le domaine de la sécurité de l'information, la performance des étudiants dans l'intégration de leurs pratiques et l'atteinte de leurs objectifs dans les organisations. Ouvrir aux étudiants des domaines connexes et leurs outils de gestion mis au service de leur métier.			
1.5 IT Service Management (Gestion des services IT)	8		1
Module 2 : Regulatory Frameworks (Cadres réglementaires) : Ce module est le second module d'introduction au contexte de la sécurité de l'information en entreprise. Les matières sont abordées en lien constant avec la sécurité de l'information. But : Préciser les éléments du cadre réglementaire et contextuel dans lequel va s'exercer le métier de responsable de la sécurité de l'information. Objectifs : Familiariser les étudiants avec les aspects réglementaires et répressifs Familiariser les étudiants avec des secteurs d'activités particuliers Faire prendre conscience aux étudiants des évolutions et des spécificités qui vont être induites sur leurs pratiques professionnelles			7
2.2 Law Enforcement (Mise en application des dispositions légales)	16		2
Module 2 : Regulatory Frameworks (Cadres réglementaires) : Ce module est le second module d'introduction au contexte de la sécurité de l'information en entreprise. Les matières sont abordées en lien constant avec la sécurité de l'information. But : Préciser les éléments du cadre réglementaire et contextuel dans lequel va s'exercer le métier de responsable de la sécurité de l'information. Objectifs : Familiariser les étudiants avec les aspects réglementaires et répressifs Familiariser les étudiants avec des secteurs d'activités particuliers Faire prendre conscience aux étudiants des évolutions et des spécificités qui vont être induites sur leurs pratiques professionnelles			7
2.3 Special Businesses and Impacts (Spécificités du secteur financier)	12		2
Module 4 : Technical Aspects (Aspects techniques) : Ce module est le second des deux modules centraux de la formation. Ces matières font parties du cœur de métier historique de la sécurité de l'information. But : Permettre aux étudiants de disposer des connaissances pour comprendre les différentes couches techniques devant être sécurisées dans un système d'information. Objectifs : Il s'agit de savoir traduire en termes techniques les analyses produites par le module de gestion de la sécurité. Parmi les compétences à acquérir, le module comprend un cours sur les technologies et les composants de sécurité (Technologie de la sécurité) dont se servent la majorité des solutions de sécurité (chiffrement, gestion des clés). Un second cours permet d'avoir la vision des différentes couches techniques (réseau/communication, traitement et persistance) impliquées dans un système d'information ouvert sur Internet, avec un accent mis sur les vulnérabilités propres à chacune de ces couches. Un troisième cours permet de comprendre et de décortiquer les attaques récentes, afin de mieux appréhender les parades possibles. : Familiariser les étudiants avec les principes, les propriétés et les mécanismes de la sécurité de l'information et les technologies associés. Donner une vue générale et des références sur un plan technique de la sécurité de l'information Approfondir les parties importantes et les fondamentaux du domaine			12
4.2 Information Security Technologies 2 (Technologies de la sécurité 2)	20		2

Master en Management de la Sécurité des Systèmes d'Information

	Vorlesung (UE)	Übung (UE)	ECTS
4.3 Communication, Information Processing and Persistence 1 (Communication, traitement et persistance des informations 1)	16		2

Semester 3

	Vorlesung (UE)	Übung (UE)	ECTS
Module 1 : Understanding Organisations & Management (Compréhension des organisations et du management) : Ce module est le premier module d'introduction au contexte de la sécurité de l'information en entreprise. Les matières sont abordées en lien constant avec la sécurité de l'information. But : Préciser les éléments de contexte internes à l'entreprise dans lesquels va s'exercer le métier de responsable de la sécurité de l'information. Objectifs : Familiariser les étudiants avec les composantes, les mécanismes et les propriétés des organisations de tout type d'une part et de certains métiers de support abordés sous l'angle général de la gestion d'autre part. Améliorer, pour le domaine de la sécurité de l'information, la performance des étudiants dans l'intégration de leurs pratiques et l'atteinte de leurs objectifs dans les organisations. Ouvrir aux étudiants des domaines connexes et leurs outils de gestion mis au service de leur métier.			9
1.4 Project Management (Gestion des projets)	16		2
Module 3 : Information Security Management (Gestion de la sécurité de l'information) : Ce module est le premier des deux modules centraux de la formation. Ces matières sont une partie émergente du cœur de métier actuel de la sécurité de l'information. But : Installer le contenu organisationnel nécessaire pour gérer une sécurité de l'information moderne en entreprise. Objectifs : Familiariser les étudiants avec les méthodes et outils nécessaires à la gestion de la sécurité de l'information Maitriser les caractéristiques, les propriétés et les diverses utilisations possibles de ces fonctionnalités (politique de sécurité, conformité aux référentiels de sécurité, continuité de service) Déployer les grandes fonctionnalités de la sécurité de l'information en rapport avec sa gestion (ISMS, normes applicables)			10
3.4 Security Policy (Politique de sécurité)	16		2
Module 3 : Information Security Management (Gestion de la sécurité de l'information) : Ce module est le premier des deux modules centraux de la formation. Ces matières sont une partie émergente du cœur de métier actuel de la sécurité de l'information. But : Installer le contenu organisationnel nécessaire pour gérer une sécurité de l'information moderne en entreprise. Objectifs : Familiariser les étudiants avec les méthodes et outils nécessaires à la gestion de la sécurité de l'information Maitriser les caractéristiques, les propriétés et les diverses utilisations possibles de ces fonctionnalités (politique de sécurité, conformité aux référentiels de sécurité, continuité de service) Déployer les grandes fonctionnalités de la sécurité de l'information en rapport avec sa gestion (ISMS, normes applicables)			10
3.5 Compliance Assurance (Assurance de la conformité)	16		2

Master en Management de la Sécurité des Systèmes d'Information

	Vorlesung (UE)	Übung (UE)	ECTS
<p>Module 4 : Technical Aspects (Aspects techniques) : Ce module est le second des deux modules centraux de la formation. Ces matières font parties du cœur de métier historique de la sécurité de l'information. But : Permettre aux étudiants de disposer des connaissances pour comprendre les différentes couches techniques devant être sécurisées dans un système d'information. Objectifs : Il s'agit de savoir traduire en termes techniques les analyses produites par le module de gestion de la sécurité. Parmi les compétences à acquérir, le module comprend un cours sur les technologies et les composants de sécurité (Technologie de la sécurité) dont se servent la majorité des solutions de sécurité (chiffrement, gestion des clés). Un second cours permet d'avoir la vision des différentes couches techniques (réseau/communication, traitement et persistance) impliquées dans un système d'information ouvert sur Internet, avec un accent mis sur les vulnérabilités propres à chacune de ces couches. Un troisième cours permet de comprendre et de décortiquer les attaques récentes, afin de mieux appréhender les parades possibles. : Familiariser les étudiants avec les principes, les propriétés et les mécanismes de la sécurité de l'information et les technologies associés. Donner une vue générale et des références sur un plan technique de la sécurité de l'information Approfondir les parties importantes et les fondamentaux du domaine</p>			12
4.4 Communication, Information Processing and Persistence 2 (Communication, traitement et persistance des informations 2)	32		4
4.5 Threats, Attacks and Controls (Menaces, attaques et parades)	16		2
<p>Module 5 : Human Aspects (Aspects humains) : Objet : Ce module est le dernier module académique complétant la formation. Les matières sont abordées en lien constant avec la sécurité de l'information. But : Aborder et intégrer la dimension humaine pour exercer le métier de responsable de la sécurité de l'information. Objectifs : Familiariser les étudiants sur les caractéristiques de la composante humaine et de la communication en général Améliorer ses performances de communication et d'approches psychologiques Savoir communiquer les différents éléments de la sécurité de l'information dans son contexte professionnel Savoir appréhender l'impact du facteur humain sur la sécurité de l'information</p>			4
5.1 Human Risk (Risque humain)	16		2

Semester 4

	Vorlesung (UE)	Übung (UE)	ECTS
<p>Module 3 : Information Security Management (Gestion de la sécurité de l'information) : Ce module est le premier des deux modules centraux de la formation. Ces matières sont une partie émergente du cœur de métier actuel de la sécurité de l'information. But : Installer le contenu organisationnel nécessaire pour gérer une sécurité de l'information moderne en entreprise. Objectifs : Familiariser les étudiants avec les méthodes et outils nécessaires à la gestion de la sécurité de l'information Maitriser les caractéristiques, les propriétés et les diverses utilisations possibles de ces fonctionnalités (politique de sécurité, conformité aux référentiels de sécurité,</p>			10

Master en Management de la Sécurité des Systèmes d'Information

	Vorlesung (UE)	Übung (UE)	ECTS
continuité de service) Déployer les grandes fonctionnalités de la sécurité de l'information en rapport avec sa gestion (ISMS, normes applicables)			
3.6 Business Continuity Management (Gestion de la continuité)	8		1
Module 5 : Human Aspects (Aspects humains) : Objet : Ce module est le dernier module académique complétant la formation. Les matières sont abordées en lien constant avec la sécurité de l'information. But : Aborder et intégrer la dimension humaine pour exercer le métier de responsable de la sécurité de l'information. Objectifs : Familiariser les étudiants sur les caractéristiques de la composante humaine et de la communication en général Améliorer ses performances de communication et d'approches psychologiques Savoir communiquer les différents éléments de la sécurité de l'information dans son contexte professionnel Savoir appréhender l'impact du facteur humain sur la sécurité de l'information			4
5.2 Human Communication (Communication humaine)	16		2
Module 6 : Professional Part (Volet professionnel) : Ce module représente à lui seul le volet professionnel de la formation qu'il encadre au tout début et en toute fin du cycle de deux années. Les activités sont centrées sur la sécurité de l'information, l'exercice de la responsabilité de la sécurité de l'information et la professionnalisation des pratiques. But : Préparer par la pratique l'étudiant à l'exercice de la responsabilité de la sécurité de l'information et de la profession associée. Objectifs : Réaliser une synthèse démonstrative de toutes les compétences apportées par les enseignements que l'étudiant a suivis dans les modules précédents en lui faisant réaliser un projet professionnel. Familiariser l'étudiant avec les réalités et la professionnalisation des pratiques du métier de responsable de la sécurité de l'information. Étudier le métier de responsable de la sécurité de l'information. Réaliser une application de ce métier à travers un projet professionnel.			18
6.3 Professional Project (Projet professionnel)			14
6.2 Security Emerging Technologies	24		3

Master en Management de la Sécurité des Systèmes d'Information

Semester 1

1.1 Organisational Theory and Change (Théorie des organisations et du changement)

Modul:	Module 1 : Understanding Organisations & Management (Compréhension des organisations et du management) (Semester 1)
ECTS:	2
Objektiv:	<ul style="list-style-type: none">• Define the characteristics of the organizational context within which security management is deployed• Provide insight into the different components of the organization, their respective roles and their interrelations• Identify the organizational changes related to security management, and how to manage these as well as the socio organizational risks• Understand the challenges of security management in terms of sense-making within the organizations
Beschreibung:	<p>The course aims to develop your understanding of the organizational context. It focuses on the structure (organizational configurations), types of strategies and corporate culture that characterize an organization.</p> <p>Content :</p> <ul style="list-style-type: none">• Class 1: What is an organization ? Which configuration ?• Class 2: What is Corporate Strategy ? What are the links between Strategy, Information systems and the organizational structure ?• Class 3: What is change and how does it work ? What are the socio organizational risks related to security management ?
Modalitäten:	Lectures (12 hrs), personal work (38 hrs)
Sprache:	Anglais
Pflichtkurs:	Oui
Evaluation:	Group oral presentation and supporting documentation: Case study analysis of an organizational situation, using the theoretical frameworks seen in class.
Remark:	<p>Oral presentations, PowerPoint presentations, Videos, case studies</p> <ul style="list-style-type: none">• Pichault, F. (2013), Change management : Towards polyphony, Manager RH (Coll), De Boeck, 182p• Pichault, F., & Schoenaers, F. (2003), "HRM practices in a process of organizational change: A contextualist perspective", Applied Psychology, 52 (1), 120-143• K.Laudon & J.P. Laudon (2014) Management Information Systems, Global Edition, 13E, Pearson Education
Professor:	VALOGGIA Philippe

Master en Management de la Sécurité des Systèmes d'Information

2.1 Legal and Regulatory Aspects (Aspect légaux et réglementaires)

Modul:	Module 2 : Regulatory Frameworks (Cadres réglementaires) (Semester 1)
ECTS:	3
Objektiv:	Create good legal reflexes, enable students to identify / flag (for further analysis / resolution by management / legal counsels) potential legal or regulatory issues linked to their function / duties or information security in general.
Beschreibung:	<ul style="list-style-type: none">• General introduction (laws, regulations, courts)• IT law fundamentals• Liability principles• Contract law principles, pre-contractual arrangements• Study of usual IT contracts (development, license, maintenance, escrow)• Intellectual property basics• Criminal law and IT crime• Personal data protection law principles• Employee IT monitoring• IT investigations and inforensics rules• IT security statutory obligations• Forthcoming EU / Luxembourg rules
Modalitäten:	lectures (18 hrs), personal work (57 hrs)
Sprache:	Anglais
Pflichtkurs:	Oui
Evaluation:	Students are evaluated based on a paper they submit (response to case studies and questionnaire)
Remark:	Slides Relevant Luxembourg / EU laws (IT security, data protection, cybercrime)
Professor:	PIERRE-BEAUSSE Cyril

3.1 Information Security Management System - IMS (Systèmes de Management de la Sécurité de l'Information - SMSI)

Modul:	Module 3 : Information Security Management (Gestion de la sécurité de l'information) (Semester 1)
ECTS:	2
Objektiv:	<ul style="list-style-type: none">• To understand ISO/IEC 27001, its structure and its requirements• To have the same interpretation of the requirements and "speak the same language"• To have a first view on "how" to comply with the different requirements• To be able to define an action plan towards compliance

Master en Management de la Sécurité des Systèmes d'Information

Beschreibung:	<ul style="list-style-type: none">• The ISO/IEC 27001 standard<ul style="list-style-type: none">o Overview of the standard• ISMS establishment and management<ul style="list-style-type: none">o Definition of an ISMS establishment and management project• Context and objectives• Document management• Leadership<ul style="list-style-type: none">o Commitment, policy and roles & responsibilities• Performance evaluation<ul style="list-style-type: none">o Indicators, internal audit and management review• Improvement<ul style="list-style-type: none">o Nonconformity and corrective action and incident management• Risk management<ul style="list-style-type: none">o Risk assessmento Risk treatment• Information security policy(ies) and procedures• Conclusions and work plan
Sprache:	Anglais
Pflichtkurs:	Oui
Evaluation:	Written exam based on a questionnaire
Remark:	Slideshow in a PDF file ISO/IEC 27001. Information technology - Security techniques - Information security management systems - Requirements. International Organization for Standardization, Geneva, 2005. Management de la sécurité de l'information. Implémentation ISO 27001, Alexandre Fernandez-Toro, Eyrolles, 2012. N. Mayer, "A Cluster Approach to Security Improvement according to ISO/IEC 27001", 17th European Systems & Software Process Improvement and Innovation Conference (EUROSPI'10), Grenoble, France, September 2010. T. Valdevit, N. Mayer, and B. Barafort, "Tailoring ISO/IEC 27001 for SMEs: A Guide to Implement an Information Security Management System in Small Settings", 16th European Systems & Software Process Improvement and Innovation Conference (EUROSPI'09), Alcala, Spain, September 2009
Professor:	MAYER Nicolas

3.2 Risk Analysis and Management (Analyse et gestion de risques)

Modul:	Module 3 : Information Security Management (Gestion de la sécurité de l'information) (Semester 1)
ECTS:	2
Objektiv:	<ul style="list-style-type: none">• To introduce the concepts of risk regardless of context• To highlight the socio-cultural aspects of risk perception and its (empirical) assessment methods• To master the set of concepts related to Information System Security Risk Management (ISSRM)

Master en Management de la Sécurité des Systèmes d'Information

- To have the theoretical background to ease the understanding of risk management methods
- To understand the ISO/IEC 27005:2011 standard
- To have a pragmatic and ready-to-use view of the standard

- Beschreibung:**
- * Introduction to risk management
 - Perception of risk and risk management in general
 - Influence of socio-cultural risk perception
 - Empirical methods
 - Endogenous and exogenous threats
 - Illustration based on examples
 - * Introduction to information security risk management
 - * Outline of information security risk management concepts
 - Asset
 - Risk
 - Risk treatment
 - * Metrics of information security risk management
 - * The ISO/IEC 27005:2011 process and its underlying activities
 - Context establishment
 - Risk identification
 - Risk analysis
 - Risk evaluation
 - Risk treatment
 - Risk acceptance
 - Risk communication and consultation
 - Risk monitoring and review

Modalitäten: Lectures (12 hrs) ; personal work (38 hrs)

Sprache: Anglais

Pflichtkurs: Oui

Evaluation: Project on a case study

Remark: Slideshow in a PDF file

ISO/IEC 27005. Information technology - Security techniques - Information security risk management. International Organization for Standardization, Geneva, 2008.

Gestion des risques en sécurité de l'information - Mise en oeuvre de la norme ISO 27005, Anne Lupfer, Eyrolles, 2010

N. Mayer, "Model-based Management of Information System Security Risk", Presses universitaires de Namur, April 2009. ISBN: 978-2870376409.

E. Dubois, P. Heymans, N. Mayer, and R. Matulevicius, "A Systematic Approach to Define the Domain of Information System Security Risk Management", Book Chapter in: S. Nurcan et al. (eds.), "Intentional Perspectives on Information Systems Engineering", Springer-Verlag, 2010. ISBN: 978-3-642-12543-0.

Professor: MAYER Nicolas, HAGEN David

3.3 Risk Analysis Practices (Pratiques d'analyse de risques)

Modul: Module 3 : Information Security Management (Gestion de la sécurité de l'information)
(Semester 1)

Master en Management de la Sécurité des Systèmes d'Information

ECTS:	1
Sprache:	Anglais
Pflichtkurs:	Oui
Professor:	ALESSANDRONI Johann

4.1 Information Security 1 (Technologies de la sécurité 1)

Modul:	Module 4 : Technical Aspects (Aspects techniques) (Semester 1)
ECTS:	2
Objektiv:	<ul style="list-style-type: none">• Understand the basic concepts of modern cryptography such as: confidentiality, integrity and authentication, public and private key cryptography.• Study the principles of operation of basic cryptographic algorithms: block ciphers, stream ciphers, hash functions, message authentication codes, public-key encryption and digital signatures.• Become familiar with the most widely used cryptographic standards: AES, DES, SHA, RSA, DSA, etc. - Given certain security requirements, be able to propose solutions using current best practices and state-of-the-art cryptographic standards.
Beschreibung:	<p>The course teaches the fundamental security components used as building blocks in modern security technologies. The material is divided in two parts. One part covers the basics of public-key cryptography: public-key encryption, digital signatures, etc. The second part is dedicated to symmetric-key cryptography and discusses topics such as stream ciphers, block ciphers, hash functions and message authentication codes.</p> <p>A brief outline of the covered topics follows.</p> <ul style="list-style-type: none">• Overview of cryptography• Introduction to public-key cryptography• Public key encryption- Digital signatures• Introduction to symmetric-key cryptography• Block ciphers, stream ciphers• Hash functions, Message authentication codes• Real life applications
Sprache:	Anglais
Pflichtkurs:	Oui
Evaluation:	Written exam
Remark:	<ul style="list-style-type: none">• Lecture slides and lecture notes• William Stallings, Cryptography and Network Security (5th edition)• Keith M.Martin, Everyday Cryptography• Alfred Menezes, Scott Vanstone, Paul van Oorschot, The Handbook of Applied Cryptography : http://cacr.uwaterloo.ca/hac/
Professor:	CORON Jean-Sébastien, GROSZSCHÄDL Johann

Master en Management de la Sécurité des Systèmes d'Information

6.1 Working in Information Security Management (Le métier de responsable de la sécurité de l'information)

Modul:	Module 6 : Professional Part (Volet professionnel) (Semester 1)
ECTS:	1
Objektiv:	<ul style="list-style-type: none">• Provide a feedback on the field job of a Chief Information Security Officer• Provide practical tools and techniques in order to become efficient• Explain common threats in order to avoid professional mistakes
Beschreibung:	<ul style="list-style-type: none">• Introduction - Background & expenses as a CISO• CISO - Different pathways• CISO - The multiple facets• CISO - Strengths and obstacles• CISO - A 360° organizational cleverness• CISO - Good communication for effective awareness• CISO - Methods & Tools. The global paradigm & combination• CISO - The importance of Risk Management• CISO - An ordinary day• Conclusion - For a future Chief Information Security Officer
Sprache:	Anglais
Pflichtkurs:	Oui
Evaluation:	Evaluation based on a project
Professor:	MANS Rodolphe

Master en Management de la Sécurité des Systèmes d'Information

Semester 2

1.2. Architecture and Business Strategy (Architecture et stratégie des entreprises)

Modul:	Module 1 : Understanding Organisations & Management (Compréhension des organisations et du management) (Semester 2)
ECTS:	3
Objektiv:	<ul style="list-style-type: none">• Define the role of enterprise architecture as a means to bridge between an enterprise's business strategy and the transformation programmes aiming to realise/execute this strategy.• Identification of the two-way role, which this bridge (enterprise architecture) plays with regards to core qualities (such as flexibility, reliability, compliance, and information security). In other words, how enterprise architecture can be used to study/elaborate the consequences of strategic decisions, and how core design decisions may have strategic consequences. Such consequences will also be expressed in terms of security related risk analysis.• Provide insight into the different elements of enterprise architecture, and their respective roles, covering models, views, frameworks and principles.• Elaboration of this role for security in the context of information systems and their alignment with the business objectives of the company In doing so, we will also provide students with an insight into the state-of-the-art of the field of enterprise architecture with regards to security
Beschreibung:	<ul style="list-style-type: none">• Business strategy• Enterprise transformations• Enterprise architecture as a bridge between business strategy and enterprise transformation• Elements of enterprise architecture: models, views, frameworks and principles.• Security related risk analysis and business/IT alignment
Modalitäten:	Courses (18 hrs), personal work (57 hrs)
Sprache:	Anglais
Pflichtkurs:	Oui
Evaluation:	Exam based on a case study, as well as general insight related questions.
Remark:	This course is taught in English. The examination will also take place in English.
Professor:	PROPER Erik

1.3 Financial Management (Gestion financière)

Modul:	Module 1 : Understanding Organisations & Management (Compréhension des organisations et du management) (Semester 2)
ECTS:	1

Master en Management de la Sécurité des Systèmes d'Information

Objektiv:	<p>Students get familiar with two fundamental tools of financial management: financial accounting and management accounting as well as costing.</p> <ul style="list-style-type: none">• Understand fundamental concepts of financial accounting, especially the annual accounts (balance sheet, profit and loss accounts) as well as value adjustments and provisions. Any person who must manage investments and risks must be familiar with these concepts.• Understand some fundamentals of management accounting: cost analysis, budgeting and auditing
Beschreibung:	<ul style="list-style-type: none">• Fundamentals of financial accounting<ol style="list-style-type: none">a.Objectives and meansb.The balance sheet and the profit and loss accountsc.Value adjustments<ol style="list-style-type: none">i.Foreseeable value adjustmentsii.Unforeseeable value adjustmentsd.Provisionse.The legal context• Fundamentals of management accounting and auditing<ol style="list-style-type: none">a. Objectives and meansb. Determining the full cost<ol style="list-style-type: none">i. Direct and indirect costii. Cost centresiii. Costc Cost analysis and determination of margin<ol style="list-style-type: none">i. Structural cost and variable costii. Rational allocation of structural costiii. Variable cost and marginsd. Budgeting<ol style="list-style-type: none">i. Budget estimateii. Budget hierarchyiii. General budgete. Management control<ol style="list-style-type: none">i. Budget estimate and budget achievedii. The balanced scoreboard <p>The briefs to be elaborated should allow applying the learned concepts to security management for information systems.</p>
Sprache:	Anglais
Pflichtkurs:	Oui
Evaluation:	The assessment is based on the personal work, especially the practical exercises proposed by the teacher and the brief presenting one more case studies taken from the student's professional activity in the field of Security Management for Information Systems.
Remark:	SlidesFor those interested interested in deepening the subjects (not mandatory literature): Financial Accounting for Decision Makers, Dr. Peter Atrill, Eddie McLaney (authors), Pearson, 2013 (seventh edition) Financial Management for Decision Makers, Dr. Peter Atrill, Pearson, 2014 (seventh edition)
Professor:	FIORAZZO Raphaël

Master en Management de la Sécurité des Systèmes d'Information

1.5 IT Service Management (Gestion des services IT)

Modul:	Module 1 : Understanding Organisations & Management (Compréhension des organisations et du management) (Semester 2)
ECTS:	1
Objektiv:	<ul style="list-style-type: none">• Comprendre les concepts de Service IT et de Gestion des Services IT.• Présenter l'évolution des référentiels de gestion des Services IT jusqu'à aujourd'hui.• Comprendre le rôle de la gestion de la sécurité de l'information dans la gestion globale des Services IT.• Comprendre les apports de la gestion des Services IT pour la gestion de la Sécurité de l'information.
Beschreibung:	<ul style="list-style-type: none">• IT Service et IT Service Management : concepts et historique <p>·Les référentiels ITIL v2 et v3 (la dernière version)</p> <ul style="list-style-type: none">• Présentation de ITIL v2 et v3 (structure et processus)• Comparatif et évolution entre la v2 et la v3• La gestion de la sécurité de l'information dans ITIL v2 et v3• La gestion de la sécurité et ITIL : la réalité du terrain <p>·Le standard ISO 20000</p> <ul style="list-style-type: none">• Présentation du standard• Relations entre ITIL et ISO 20000• Relations entre ISO 20000 et ISO 27000• La gestion de la sécurité de l'information dans ISO 20000 <p>·Les apports de la gestion des services pour la gestion de la sécurité de l'information.</p>
Modalitäten:	cours magistraux (6 hrs) ; travaux personnels (19 hrs)
Sprache:	Anglais
Pflichtkurs:	Oui
Evaluation:	Evaluation : case study based homework
Remark:	Supports de cours en anglais, enseignement en français
Professor:	PICARD Michel

Master en Management de la Sécurité des Systèmes d'Information

2.2 Law Enforcement (Mise en application des dispositions légales)

Modul:	Module 2 : Regulatory Frameworks (Cadres réglementaires) (Semester 2)
ECTS:	2
Objektiv:	<ul style="list-style-type: none">• Students should get familiar with the legal and procedural environment of criminal investigations• Students should also become familiar with good practices and learn about the specific procedural difficulties encountered by law enforcement bodies during (computer) investigations• Students should eventually become familiar with the specific problems linked to gathering and reporting digital evidence
Beschreibung:	<p>Part I. Criminal procedure and investigations</p> <ol style="list-style-type: none">1. Law enforcement bodies2. General principles of criminal investigations3. Specific procedures<ul style="list-style-type: none">- Police investigation- Emergency procedure- Judicial examination- Access to telecommunication data- Legal interception4. Specific aspects of obtaining digital evidence5. International police cooperation6. Mutual legal assistance <p>Part II. Digital forensics</p> <ol style="list-style-type: none">1. Good practice2. Acquisition of numeric information3. Authentication of digital evidence4. Analysis of digital evidence and reporting5. Professional software6. Practical examples and visit

Master en Management de la Sécurité des Systèmes d'Information

Modalitäten:	For legal texts and official documents no translation is provided. References to these documents as well as quotations will be based on their original versions
Sprache:	Anglais
Pflichtkurs:	Oui
Evaluation:	Written exam (questionnaire) Short questions or multiple choice. No documentation is allowed. The questionnaire is based on the course contents and the course handouts.
Remark:	Handouts of powerpoint presentations Official texts and good practice guides are provided as PDF files.
Professor:	MOES René

2.3 Special Businesses and Impacts (Spécificités du secteur financier)

Modul:	Module 2 : Regulatory Frameworks (Cadres réglementaires) (Semester 2)
ECTS:	2
Sprache:	Anglais
Pflichtkurs:	Oui
Professor:	HAGEN David

4.2 Information Security Technologies 2 (Technologies de la sécurité 2)

Modul:	Module 4 : Technical Aspects (Aspects techniques) (Semester 2)
ECTS:	2
Objektiv:	The course is about the main fundamental security components/technologies that are basic blocks used in most of security solutions. A first part of the course is dedicated to cryptography and the second one is about secured platforms. This second part is about public key infrastructures and how to build secure component-based platforms
Beschreibung:	Content : A.PKI applications <ul style="list-style-type: none">• Public key infrastructure• Authentication protocols• Application to the financial sector• Case study B.Architectures the secure platforms <ul style="list-style-type: none">• Modern web architectures• The different technical levels for securing a platform• Implementation of a component-based system embedding security policies

Master en Management de la Sécurité des Systèmes d'Information

	<ul style="list-style-type: none">• Case study
Modalitäten:	Lectures (12hrs), personal work (36hrs)
Sprache:	Anglais
Pflichtkurs:	Oui
Evaluation:	Written exam
Professor:	JIMENEZ Matthieu, GIRARD Frédéric

4.3 Communication, Information Processing and Persistence 1 (Communication, traitement et persistances des informations 1)

Modul:	Module 4 : Technical Aspects (Aspects techniques) (Semester 2)
ECTS:	2
Objektiv:	<p>Information systems combine three dimensions that must be independently and globally secured from a systemic viewpoint; the communication aspect (classical and dynamic networks), treatments (software, business logic), and persistency (databases and data storage)</p> <p>Apprehend the different parameters impacting network and communication security.</p> <p>Understand the software layer and be familiar with the safe and secure design and deployment of software</p> <p>This course treats the technological means that are available or required to secure the communication between users over a hostile network</p>
Beschreibung:	<p>Introduction to computer networks and protocols</p> <p>ISO/OSI layered communication model</p> <p>Virtual private networks</p> <p>IPSec</p> <p>Firewalls</p> <p>Intrusion detection</p> <p>E-mail security</p> <p>Security protocols</p> <p>SSL/TLS</p> <p>Web security</p> <p>User authentication</p> <p>Viruses/malware (optional)</p> <p>RFID security (optional)</p>
Sprache:	Anglais
Pflichtkurs:	Oui
Evaluation:	Evaluation through practical work and questionnaires
Remark:	Lectures (12hrs), personal work (38hrs)
Professor:	MAUW Sjouke

Master en Management de la Sécurité des Systèmes d'Information

Semester 3

1.4 Project Management (Gestion des projets)

Modul:	Module 1 : Understanding Organisations & Management (Compréhension des organisations et du management) (Semester 3)
ECTS:	2
Objektiv:	<ul style="list-style-type: none">• Donner aux étudiants les clés pour comprendre l'intérêt du mode projet• Donner aux étudiants les capacités de décision d'activation et de choix des modalités du mode projet• Donner aux étudiants les fondamentaux conceptuels et pratiques leur permettant de mettre en œuvre le mode projet dans leur activités relatives à la sécurité de l'information
Course learning outcomes:	
Beschreibung:	<ul style="list-style-type: none">• Histoire de la gestion de projet• Pourquoi le mode projet• Les différents référentiels / méthode / certifications de gestion de projet à disposition• Exemple de contexte : Le référentiel projet GISSIP de la DCSSI (France)• Agile project Management : Theory and Planning Game
Modalitäten:	cours magistraux (12 hrs) ; travaux personnels (38 hrs)
Sprache:	Anglais
Pflichtkurs:	Oui
Evaluation:	Home exam
Professor:	PIRAUX Jean-Louis

3.4 Security Policy (Politique de sécurité)

Modul:	Module 3 : Information Security Management (Gestion de la sécurité de l'information) (Semester 3)
ECTS:	2
Sprache:	Anglais
Pflichtkurs:	Oui
Professor:	GIRARD Frédéric, STEICHEN Pascal

Master en Management de la Sécurité des Systèmes d'Information

3.5 Compliance Assurance (Assurance de la conformité)

Modul:	Module 3 : Information Security Management (Gestion de la sécurité de l'information) (Semester 3)
ECTS:	2
Sprache:	Anglais
Pflichtkurs:	Oui
Professor:	TERONI Mirko

4.4 Communication, Information Processing and Persistence 2 (Communication, traitement et persistance des informations 2)

Modul:	Module 4 : Technical Aspects (Aspects techniques) (Semester 3)
ECTS:	4
Objektiv:	<p>The course aims at presenting design techniques to develop a secure software integrating persistency. The course is two-fold : the first part is about modeling, development and testing of software (including security policies); the second one about secured databases. We thus introduce software engineering techniques for security.</p> <p>Modelling will be done with UML standard, that will be briefly presented, as well as the link with programming. The student will understand the main challenges for efficient implementation of a maintainable security policy (access control, XACML standard)</p>
Beschreibung:	<p>A.Design and validation for safety and security</p> <ol style="list-style-type: none">1. Design methods for designing software and architectures2. Security policies and their deployment3. Software functional testing4. Software security testing <p>B.Secured databases</p> <ol style="list-style-type: none">1. Architectures for persistency (databases, cloud, datacenters)2. Securing a database3. Performance, robustness and security testing of databases <p>Use case :</p> <p>A practical case will be (partly) implemented in Java (e.g. Auction system) or an Android application</p>
Sprache:	Anglais
Pflichtkurs:	Oui
Evaluation:	Evaluation via practical work and questionnaires
Remark:	Lectures (24hrs), personal work (72hrs)
Professor:	HABCHI Sarra, ACKERMAN Michel, LE TRAON Yves

Master en Management de la Sécurité des Systèmes d'Information

4.5 Threats, Attacks and Controls (Menaces, attaques et parades)

Modul:	Module 4 : Technical Aspects (Aspects techniques) (Semester 3)
ECTS:	2
Objektiv:	Understand common web vulnerabilities, their impact on security properties, and how to fix them, prevent them. Acquire the ability to exploit web vulnerabilities through tools or manually.
Beschreibung:	SQL Injection & other injection flaws in theory and in practice. Cross Site Scripting theory and practical exploitation. Common web application vulnerabilities. Web application auditing methodology. Self-teaching ressources and material.
Sprache:	Anglais
Pflichtkurs:	Oui
Evaluation:	Practical exam on real-world vulnerability discovery and exploitation
Remark:	Virtual machines, online ressources. Web applications Hacker Handbook, OWASP Top 10, OWASP Wiki
Professor:	STEICHEN Pascal, TABAN Raphaël

5.1 Human Risk (Risque humain)

Modul:	Module 5 : Human Aspects (Aspects humains) (Semester 3)
ECTS:	2
Objektiv:	Introduce and familiarise course participants with basic principles and properties of: <ul style="list-style-type: none">• Human information processing: What are the basic principles of human perception and cognition?• Human risk-taking behavior: Under which circumstances do people engage in risky behavior?• Persuasion and manipulation in social interactions: What are the best-known strategies in social engineering? How to identify social engineering attacks? How to avoid these attacks?
Beschreibung:	Theories and models of human information processing <ul style="list-style-type: none">• 'Basics': Human sensation and perception• 'Higher cognitive functions': thinking, remembering, problem-solving• 'Regulatory mechanisms': Emotion, motivation and their effects on behavior• 'Outcome': Human behavior Principles of social interaction <ul style="list-style-type: none">• Human behavior in groups• Leadership and the influences of authorities• 'Tit-for-tat': Reciprocity in interactions• Influence and persuasion in social interactions Social engineering: A novel social phenomenon in information security <ul style="list-style-type: none">• General aspects: Communication and elicitation

Master en Management de la Sécurité des Systèmes d'Information

- Methods: Interviews and interrogation
- Influence: persuasion, playing with limited attention
- Counteractive measures: identifying social engineering attacks, raising personal security awareness, learning how to respond properly

Sprache: Anglais

Pflichtkurs: Oui

Evaluation: Oral presentation of a selected topic from the field of human risks (small groups up to four students: 60%), written exam based on a questionnaire (individual: 40%)

Remark: Powerpoint presentations, video clips, handouts, group discussions

- Cialdini, R. (2001). Influence. Science and practice. Boston, MA: Pearson Education, Inc.
- Hadnagy, C. (2011). Social Engineering: The art of human hacking. Indianapolis, IN: John Wiley & Sons Ltd.
- Levine, R. (2003). The power of persuasion: how we're bought and sold. Hoboken, NJ: John Wiley & Sons.
- Wickens, C. D., Lee, J. D., Liu, Y., & Gordon Becker, S. E. (2004). An introduction to human factors engineering. Upper Saddle River, NJ: Pearson Education, Inc.

Professor: HAPP Christian

Master en Management de la Sécurité des Systèmes d'Information

Semester 4

3.6 Business Continuity Management (Gestion de la continuité)

Modul:	Module 3 : Information Security Management (Gestion de la sécurité de l'information) (Semester 4)
ECTS:	1
Sprache:	Anglais
Pflichtkurs:	Oui
Professor:	ALESSANDRONI Johann

5.2 Human Communication (Communication humaine)

Modul:	Module 5 : Human Aspects (Aspects humains) (Semester 4)
ECTS:	2
Sprache:	Anglais
Pflichtkurs:	Oui
Professor:	MANS Rodolphe, MAX Charles Joseph

6.3 Professional Project (Projet professionnel)

Modul:	Module 6 : Professional Part (Volet professionnel) (Semester 4)
ECTS:	14
Objektiv:	<ul style="list-style-type: none">• Travailler sur un projet au choix de l'étudiant et sous la direction d'un tuteur, qui est aussi un enseignant de la formation.• Rédiger un mémoire de Master en relation avec le projet professionnel affecté à l'étudiant par l'équipe pédagogique.• Comprendre l'intérêt des apports académiques dans les pratiques professionnelles• Se familiariser avec la mise en pratique des connaissances acquises • Exercer sur le terrain une responsabilité de la sécurité de l'information
Course learning outcomes:	1.
Beschreibung:	Sujet et contenu, à définir par l'étudiant et ses encadrants académiques et professionnels lors du lancement du projet

Master en Management de la Sécurité des Systèmes d'Information

Modalitäten:	Cours magistraux (0 hrs) ; travaux personnels (350 hrs minimum)
Sprache:	Anglais
Pflichtkurs:	Oui
Evaluation:	rapport de projet et défense oral
Remark:	L'étudiant est leader sur son projet professionnel et se conforme aux indications données dans le guide du projet professionnel Supports en anglais, projet au choix de l'étudiant, réunions intermédiaires et défense en anglais par défaut ou dans la langue commune
Professor:	LE TRAON Yves, MAYER Nicolas

6.2 Security Emerging Technologies

Modul:	Module 6 : Professional Part (Volet professionnel) (Semester 4)
ECTS:	3
Sprache:	Anglais
Pflichtkurs:	Oui
Professor:	BISSYANDE Tegawendé François d Assise, TANG Qiang, PIERRE-BEAUSSE Cyril