Аналіз рівня освіти та підготовки фахівців з управління IT та інформаційної безпеки в Україні

Валентин Сисоєв, CISM

1. Мета

Метою дослідження є аналіз рівня освіти та підготовки фахівців з управління IT та інформаційної безпеки в Україні. Для цього порівняємо вимоги до знань, умінь та навиків, що вимагає ISACA для спеціалістів із Управління IT (CGEIT) та інформаційної безпеки (CISM), із вимогами до знань, умінь та навиків, які ставляться перед фахівцями при підготовці в українських ВУЗах.

2. Аналіз рівня освіти та підготовки фахівців із управління IT

2.1 Вимоги до знань, умінь та навиків спеціалістів IT, яких готують ВУЗи України

Згідно Постанови Кабінету міністрів України № 787 від 27.08.2010 р. "Про затвердження переліку спеціальностей, за якими здійснюється підготовка фахівців у вищих навчальних закладах за освітньо-кваліфікаційними рівнями спеціаліста і магістра" та наказу Міністерства освіти і науки України № 1067 від 09.11.2010 р. з 2011/2012 навчального року вводиться в дію перелік спеціальностей, за якими здійснюється підготовка фахівців у ВУЗах України за освітньо-кваліфікаційними рівнями спеціаліста і магістра.
Згідно даного переліку спеціальностей, підготовка фахівців з IT у вищих навчальних закладах України здійснюється за наступними спеціальностями:

Найменування	Напрям підготовки	Код	Найменування спеціальності спеціаліста
Інформаційні технології	комп'ютерні науки	6.050101	інформаційні управляючі системи та технології (за галузями)
			інформаційні технології проектування
			системне проектування
			системи штучного інтелекту
			комп'ютерний еколого-економічний моніторинг
	комп'ютерна інженерія	6.050102	комп'ютерні системи та мережі
			системне програмування
			спеціалізовані комп'ютерні системи
	програмна інженерія	6.050103	програмне забезпечення систем
			інженерія програмного забезпечення

Освітньо-кваліфікаційна характеристика

Освітньо-кваліфікаційна характеристика випускника вищого навчального закладу (ОКХ) є галузевим нормативним документом, в якому узагальнюється зміст вищої освіти, тобто відображаються цілі вищої освіти та професійної підготовки, визначається місце фахівця в структурі галузей економіки держави і вимоги до його компетентності, інших соціально важливих властивостей та якостей.

Зокрема, ОКХ встановлює:

- Компетенції соціально-особистісні:
- Загальнонаукові компетенції
- Інструментальні компетенції
- Професійні компетенції
- Виробничі функції, типові задачі діяльності, уміння та компетенції, якими повинен володіти випускники вищого навчального закладу

Проаналізуємо, які вимоги ставляться до знань, умінь та навичок, якими повинен володіти випускник ВУЗу по кожному напрямку підготовки «Інформаційні технології», відповідно до ОКХ.

2.1.1 Напрям підготовки 6.050101 "Комп'ютерні науки"

Уміння та навички з предметної області

1. Обґрунтування проектних рішень з питань розробки комп'ютерних інформаційних систем і технологій
2. Дослідження та впровадження технологій пошуку та менеджменту інформації
3. Створення математичних моделей об'єктів та процесів автоматизації в комп'ютерних інформаційних системах при рішенні організаційно-економічних та конструкторсько-технологічних: задач
4. Аналіз предметних областей і їх формалізація при створенні автоматизованих систем.
5. Розробка математичних моделей компонентів і об'єктів проектування на мікро- і макрорівні їх опису.
6. Розробка імітаційної моделі для моделюючої системи та прийняття рішень.
7. Дослідження ефективності алгоритмів, що застосовуються.
8. Дослідження ефективності програм, що застосовуються.
9. Дослідження ефективності баз знань і баз даних.
10. Виконання проектних робіт на стадії обстеження об'єкта управління.
11. Розробка концепції комп'ютеризованої системи і концептуальної моделі для моделюючої системи
12. Техніко-економічного обґрунтування розробки комп'ютерних інформаційних систем і технологій.
13. Розробка технічного завдання на створення комп'ютерних інформаційних систем.
14. Розробка ескізного проекту комп'ютерних інформаційних систем і технологій.
15. Виконання робіт з технічного і робочого проектування комп'ютерних інформаційних систем і технологій.
16. Проектування імітаційних моделей
17. Розробка програмних засобів реалізації імітаційних моделей
18. Розробка та використання систем імітаційного моделювання
19. Проектування технічного забезпечення комп'ютерних інформаційних систем і технологій.
20. Проектування мікропроцесорних систем та їх елементів для комп'ютеризованих інформаційних систем і технологій.
21. Проектування мікропроцесорних систем та їх елементів для комп'ютеризованих інформаційних систем і технологій
22. Вибір, використання, адаптація периферійних технічних засобів, засобів телеобробки і передачі даних до потреб користувача
23. Експертний аналіз способів розгортання нових високопродуктивних мереж
24. Проектування топології, логічної і фізичної структури локальних комп'ютерних мереж
25. Участь у проектування програмних компонентів локальних комп'ютерних мереж
26. Проектування інформаційних вузлів мережі Internet.
27. Проектування інформаційного забезпечення комп'ютерних інформаційних систем і технологій
28. Розробка баз даних
29. Розробка прикладних процесів управління базами даних
30. Проектування запитів до баз даних
31. Проектування і розробка баз знань
32. Розробка прикладного програмного забезпечення комп'ютерних інформаційних систем і технологій
33. Розробка прикладного програмного забезпечення комп'ютерних інформаційних систем і технологій
34. Аналіз витрат і трудомісткості розробки програмної системи
35. Розробка та відлагодження програмного інтерфейсу, візуальних компонент програмного забезпечення комп'ютерних інформаційних систем і технологій
36. Розробка лінгвістичного програмного забезпечення

37. Проектування систем штучного інтелекту
38. Приймати участь у конструюванні окремих блоків обчислювальних технічних систем
39. Оформлення документації на різних стадіях проектування комп'ютерних інформаційних систем і технологій.
40. Розробка документації на різні види забезпечення комп'ютерних інформаційних систем і технологій
41. Розробка документації на програмну систему
42. Супроводження системного програмного забезпечення
43. Адміністрування баз даних
44. Супроводження прикладного програмного забезпечення комп'ютерних інформаційних систем і технологій.
45. Супроводження прикладного програмного забезпечення комп'ютерних інформаційних систем і технологій
46. Управління комп'ютерними мережами
47. Обслуговування апаратних засобів розподілених комп'ютерних мереж, систем телекомунікацій, комп'ютерних інформаційних систем і технологій.
48. Експлуатація баз даних
49. Експлуатація і супроводження комп'ютерних мереж
50. Аналіз ринку застосування комп'ютерних інформаційних систем і технологій
51. Експлуатація комп'ютерів
52. Установка системного програмного забезпечення
53. Експлуатація прикладних програм і пристроїв комп'ютерних інформаційних технологій
54. Формування вихідних документів по задачах автоматизованої обробки даних
55. Створення таблиць баз даних
56. Гарантійне обслуговування програмного забезпечення.
57. Діагностика технічних засобів розподілених комп'ютерних мереж, систем телекомунікацій, комп'ютерних інформаційних систем і технологій.
58. Контроль цілісності даних
59. Контроль працездатності системного і прикладного програмного забезпечення
60. Організація робіт по розробці розподілених і локальних комп'ютерних мереж.
61. Організація робіт по створенню інформаційного і програмного забезпечення комп'ютерних інформаційних систем і технологій
62. Організація робіт по підготовці персоналу до експлуатації систем

Знання з предметної області:

1. методології розроблення та застосування інформаційних комп'ютерних систем і технологій аналітичного та управлінського характеру, орієнтованих на формування і прийняття рішень, інструментальні засоби створення і підтримки таких систем;
2. узагальнені та спеціалізовані мови програмування;
3. основні принципи та алгоритми обробки інформації, сучасні інформаційні технології, теорія алгоритмів та математична логіка;
4. сучасні методи математичного моделювання в науці, техніці, промисловості, моделювання та дослідження технічних, економічних, екологічних та соціальних систем;
5. проведення обчислювальних експериментів із використанням комп'ютерної техніки, сучасних інформаційних технологій;
6. основи теорії оптимального керування та застосовувати методи оптимізації для розв'язування задач математичного програмування, методи прийняття рішень в організаційних системах;
7. базові уявлення про архітектуру сучасних обчислювальних систем, інформаційних і комп'ютерних мереж;
8. системне та прикладне програмне забезпечення управління базами даних та інформаційними системами;

9. методи і засоби роботи з даними і знаннями, методи математичного, логіко-семантичного, об'єктного та імітаційного моделювання, технології системного, кластерного та факторного аналізу;
10. проектування, реалізація, тестування, впровадження, супровід та експлуатація програмних засобів в комп'ютерних системах та мережах.

2.1.2 Напрям підготовки 6.050102 "Комп'ютерна інженерія"

Уміння та навички з предметної області

1. Математичні перетворення та розрахунки
2. Розрахунки фізичних параметрів ТО
3. Розробка документації
4. Розрахунки електричних кіл
5. Розрахунки імовірнісних та статистичних характеристик ТО
6. Аналіз та синтез дискретних об'єктів
7. Чисельні розрахунки
8. Кодування інформації
9. Розробка електронних схем
10. Синтез комбінаційних схем
11. Розробка архітектури комп'ютера
12. Розробка типового вузла і пристрою
13. Управління периферійними пристроями
14. Розробка програми
15. Розробка системних програм
16. Організація обчислювальних процесів
17. Автоматизація проектування ТО
18. Розробка паралельних або розподілених комп'ютерних систем
19. Розробка комп'ютерних мереж
20. Моделювання
21. Програмування для ПРКС
22. Робота з базами даних
23. Захист інформації
24. Експлуатація та діагностування ТО

Знання з предметної області:

1. Знати математичні перетворення та розрахунки, які необхідні для розробки та використання технічного об'єкту (ТО) та програмного об'єкту (ПО) і які потребують застосування основних понять, законів і методів математичного аналізу, та інших розділів вищої математики.
2. Знати теоретичні основи постановки та формалізації задач аналізу характеристик комп'ютерних засобів та наступний їх розв'язок методами теорії ймовірностей, методами математичної статистики, методами теорії випадкових процесів та ін..
3. Знати теоретичні основи побудови лінійних та нелінійних схем перетворення інформації з застосуванням операційних підсилювачів з врахуванням заданої точності та частотних властивостей.
4. Знати теорію абстрактного та структурного синтезу синхронних та асинхронних автоматів, застосовуючи різні методи та способи мінімізації функцій збудження та виходів, а також уникнення збоїв за умов використання для побудови схеми автомата заданого елементного базису, в тому числі інтегральних схем, що програмуються.
5. Знати принципи побудови архітектури процесора, визначення системи команд, структур даних, способів адресації, алгоритмів функціонування комп'ютера при виконанні різних команд та режимів, враховуючи розподіл функцій обробки інформації між апаратними і програмними

компонентами, цільові функції проектування, та критерії ефективності з використанням мов різного рівня для опису апаратних і програмних засобів.

6. Знати принципи побудови та функціонування пам'яті комп'ютера з урахуванням ієрархічного принципу її побудови і розподілу адресного простору між компонентами системи, визначення алгоритмів обміну даними на всіх рівнях. Знати алгоритми обміну інформацією процесора з зовнішніми пристроями в режимах програмного опитування готовності, переривань і прямого доступу до пам'яті при різних способах організації комутаційної системи комп'ютера, визначати вимоги до проектування периферійних пристроїв.
7. Знати принципи розробки функціональних і принципових схем типових вузлів комп'ютера (регістра, лічильника, шифратора, дешифратора, мультиплексора, суматора, компаратора та іншого) у заданому елементному базисі, оптимізації схемних та структурних рішень по заданій критеріальній сукупності (складності, швидкодії, надійності, відмовостійкості, тощо).
8. Знати принципи і методи розробки мікроалгоритмів і схем комутаційних систем для взаємодії різних пристроїв комп'ютерів із врахуванням обранного принципу побудови апаратних, мікропрограмних та програмних засобів, режимів роботи комп'ютера, в тому числі із зовнішніми пристроями.
9. Знати принципи і методи визначення множини еквівалентних алгоритмів, що забезпечують вирішення задачі, застосовуючи процедурні або об'єктно-орієнтовані технології програмування , та обрати для кодування алгоритм за критеріями часової та (або) ємнісної складності.
10. Знати принципи розробки резидентних програми реалізації функцій операційних систем типу UNIX або Windows з використанням системи переривань.
11. Знати основні підходи до розробки архітектури комп'ютерних мереж, використовуючи поняття еталонної моделі взаємодії відкритих систем та системи передачі даних на фізичному рівні (середовище передачі, канали передачі, цифрові мережі передачі даних).
12. Знати засоби забезпечення надійності функціонування комп'ютерних систем та мереж, виконувати розрахунки параметрів надійності комп'ютерних систем та мереж.

2.1.3 Напрям підготовки 6.050103 «Програмна інженерія»

Уміння та навички з предметної області

1. здатність здійснювати аналіз вимог, розробляти специфікацію програмних вимог, виконувати їхню верифікацію та атестацію;
2. здатність моделювати різні аспекти системи, для якої створюється програмне забезпечення;
3. здатність розробляти алгоритми та структури даних для програмних продуктів;
4. здатність проектувати компоненти архітектури програмного продукту
5. здатність аналізувати, проектувати та прототипувати людино-машинний інтерфейс
6. володіння основами конструювання програмного забезпечення
7. володіння основами методів та технологій об'єктно-орієнтованого програмування
8. здатність приймати участь у проектуванні та реалізації баз даних
9. здатність застосовувати та створювати компоненти багаторазового використання
10. здатність забезпечувати захищеність програм і даних від несанкціонованих дій
11. здатність застосовувати професійно профільовані знання в галузі загальноосвітніх дисциплін у процесі розв'язання професійних задач, побудови математичних моделей;
12. здатність проведення ділових перемов з бізнес-партнерами
13. використовувати Інтернет ресурси для рішення експериментальних і практичних завдань у галузі професійної діяльності;
14. здатність аргументовано переконувати колег у правильності пропонованого рішення, вміти донести до інших свою позицію;
15. дотримання професійної етики програмної інженерії

Знання з предметної області:

1. сучасні уявлення про основи інженерії вимог до програмного забезпечення;

2. базові уявлення про основи моделювання програмного забезпечення , типи моделей , основні концепції уніфікованої мови моделювання UML;
3. сучасні уявлення про структуру та архітектуру програмного забезпечення, методи проектування програмного забезпечення;
4. базові уявлення про сучасні психологічні принципи людино-машинної взаємодій , засоби розробки людино-машинного інтерфейсу;
5. сучасні уявлення про інформаційні моделі та системи , реляційні та розподілені бази даних , мови запитів до баз даних;
6. типові процеси програмної інженерії, здатність їх впровадження і управління ними;
7. базові уявлення про сучасні стандарти та процеси управління якістю програмного забезпечення

2.2 Вимоги до знань, умінь та навичок спеціалістів з управління IT, відповідно до ISACA (Certified in the Governance of Enterprise IT)

Проаналізуємо, які вимоги ставляться до знань, умінь та навиків, якими повинен володіти Certified in the Governance of Enterprise IT.
Ці вимоги до умінь та компетенцій спеціалістів з управління IT є результатом великого дослідження і опитування експертів з предметних областей IT з усього світу. Також буди використані дослідження, проведені IT Governance Institute і COBIT 4.1.

Ці уміння та навики спрямовані на виконання завдань, що виконуються особами, пов'язаними з управлінням IT, та знання, необхідні для виконання цих завдань. Вони також призначені для використання в якості визначення ролей і відповідальностей спеціалістів з управління IT.

2.2.1 Модель Управління IT

Визначати, встановлювати та підтримувати модель управління IT (керівництво, організаційну структуру і процеси) щоб: забезпечити відповідність із корпоративним управлінням, контролювати бізнес-інформації та інформаційно-технологічне середовище шляхом здійснення належної практики, а також забезпечити відповідності зовнішнім вимогам.

Уміння та навички з предметної області

1. Визначте вимоги та цілі управління IT на підприємстві, із врахуванням цінності, філософії, стилю управління, обізнаності,організації структури, стандартів і політик.
2. Гарантувати, що структура управління IT існує і заснована на всеосяжних і повторюваних IT-процесах і моделі управління, що відповідає структурі управління підприємством.
3. Створити відповідні структури управління, такі, як Інвестиційний Комітет, Комітет IT стратегії, Керівний комітет з інформаційних технологій, Комітет із перегляду IT інфраструктури, Комітет з потреб бізнесу та Комітет з IT аудиту.
4. Ensure that the enterprise and IT governance frameworks enable the enterprise to achieve optimal value for the enterprise.
5. Confirm that the IT governance framework ensures compliance with applicable external requirements and ethical statements that are aligned with, and confirm delivery of, the enterprise's goals, strategies and objectives.
6. Obtain independent assurance that IT conforms with relevant external requirements; contractual terms; organizational policies, plans and procedures; generally accepted practices; and the effective and efficient practice of IT.
7. Apply IT best practices to enable the business to achieve optimal value from implementation of IT services and IT-enabled business solutions.
8. Ensure the establishment of a framework for IT governance monitoring (considering cost/benefits analyses of controls, return on investment for continuous monitoring, etc.), an approach to track all IT governance issues and remedial actions to closure, and a lessons-learned process.

9. Ensure that appropriate roles, responsibilities and accountabilities are established and enforced for information requirements, data and system ownership, IT processes, and benefits and value realization.
10. Report IT governance status and issues, and effect transparency in reporting.
11. Establish a communications plan to continuously market, communicate and reinforce the need and value of IT governance across the enterprise.

Knowledge Statements

1. Knowledge of how to effect organizational, process and cultural change by translating objectives into actions
2. Knowledge of the components of an enterprise governance framework
3. Knowledge of how to direct, manage and report on IT governance activities at the enterprise level and collaborating with enterprise governance as appropriate
4. Knowledge of business drivers for the use of IT industry practices, standards and frameworks.
5. Knowledge of how accountability is established for information requirements, data and system ownership, and IT processes
6. Knowledge of COBIT, Val IT and related products.
7. Knowledge of the scope, objective and benefits of IT practices, standards and frameworks, such as ITIL, CMMI, PRINCE2, PMBOK, TOGAF, ISO 17799/27000 series, and the IT Balanced Scorecard
8. Knowledge of scope, objective and benefits of continuous process improvement, such as Six Sigma, Total Quality Management and the Balanced Scorecard
9. Knowledge of IT governance implementation practices
10. Knowledge of how IT practices, standards and frameworks relate to, and complement, each other
11. Knowledge of the process of selection, customization and integration of IT practices, standards and frameworks, as relevant for the enterprise
12. Knowledge of how to align the application of IT practices, standards and frameworks to the needs and culture of the enterprise
13. Knowledge of assurance methodologies and techniques
14. Knowledge of marketing and communications methods and techniques
15. Knowledge of how to utilize mission, vision, guiding principles, critical success factors, etc., in setting the direction for IT governance across the enterprise
16. Knowledge of the impact of cultural changes and the need to choose the correct time and way to achieve the desirable results, considering different but possible scenarios

2.2.2 Відповідність стратегії

Гарантувати, що IT направлене на підтримку та досягнення бізнес цілей через інтеграцію стратегії IT із стратегічними планами бізнесу; забезпечити відповідність IT послуг із операціями організації для оптимізації бізнес-процесів.

Tasks

1. Define and implement a strategic planning framework, requiring and facilitating collaborative and integrated business and IT management planning.
2. Actively support/promote and participate in IT management planning by employing best practice enterprise architecture (EA) frameworks.
3. Ensure that appropriate policies and procedures are in place, understood and followed to support IT and business strategic alignment.
4. Identify and take action on barriers to strategic alignment.
5. Ensure that effective communication and engagement exists between business and IT management regarding shared strategic initiatives and performance.
6. Ensure business and IT goals cascade down through the enterprise into clear roles, responsibilities and actions.

7. Assist senior management by aligning IT initiatives with business objectives and facilitating prioritization of business strategies that optimally achieve business objectives.
8. Identify and monitor the interdependencies of strategic initiatives and their impact on value delivery and risk.
9. Ensure that the strategic planning process is adequately documented, transparent and meets stakeholder needs.
10. Maintain and update the IT management plans, artifacts and standards for the enterprise.
11. Monitor, evaluate and report on the effectiveness of the alignment of IT and enterprise strategic initiatives.
12. Monitor and assess current and future technologies and provide advice on the costs, risks and opportunities that they bring.

Knowledge Statements

1. Knowledge of the enterprise's mission, objectives, culture, economic and business environment, key business processes, and how they are supported by IT
2. Knowledge of how an enterprise's structure, operational frameworks, systems, resources, internal and external stakeholder relationships, and culture can impact the enterprise's ability to achieve sufficient strategic alignment
3. Knowledge of the strategic planning process and techniques
4. Knowledge of enterprise architecture components, principles and frameworks, and their implementation.
5. Knowledge of how to map strategy to specific, enabling business processes and IT dashboard/balanced scorecard principles to monitor key goal and performance metrics
6. Knowledge of benchmarking planned vs. actual strategic performance
7. Knowledge of scope, objectives and benefits of investment programs
8. Knowledge of portfolio, program and project management techniques
9. Knowledge of linking enterprise business strategy with related best practices and selling the value proposition to key stakeholders
10. Knowledge of how procedures, monitoring and updating of the IT strategy are impacted and implemented by changes in business strategy
11. Knowledge of current and future technology direction to support the business by creation of technological infrastructure plan and architecture board that sets and manages what technology can deliver to achieve business objectives

2.2.3 Цінність

Забезпечити виконання функцій управління якістю як IT-фахівцями так і менеджментом: інвестиції, «влиті» в проекти з IT досягають прогнозованих результатів і вимірні цінності для бізнесу як для особистого так і колективного блага. Необхідні рішення і сервіси виконуються вчасно і в рамках бюджету, та IT - сервіс і інші IT-активи продовжують мати вагомий внесок у бізнес.

Tasks

1. Ensure that business takes ownership and accountability for business cases, business transformation, organizational change, business process operation and benefit realization for all IT-enabled business investments.
2. Ensure that all IT-enabled investments are managed as a portfolio of investments.
3. Ensure that all IT-enabled investments are managed as programs and include the full scope of activities and expenditures that are required to achieve business value.
4. Ensure that all IT-enabled investments are managed through their full economic life cycle so that value is optimized.
5. Recognize that different categories of investments need to be evaluated and managed differently.
6. Ensure that all IT solutions are developed and maintained effectively and efficiently through the development life cycle to deliver the required capabilities.
7. Ensure that all IT services are delivered to the business with the right service levels.

8. Ensure that IT services enable the business to create the required business value using assets (people, applications, infrastructure and information) to deliver the appropriate capabilities at optimal cost.
9. Define and monitor appropriate metrics for the measurement of solution and service delivery against objectives and for the measurement of benefits realized, and respond to changes and deviations.
10. Engage all stakeholders and assign appropriate accountability for delivery of business and IT capabilities and realization of benefits.
11. Ensure that IT investments, solutions and services are aligned with the enterprise strategies and architecture

Knowledge Statements

1. Knowledge of value governance practices
2. Knowledge of IT investment management practices and processes
3. Knowledge of business case development and monitoring, portfolio program and project management practices
4. Knowledge of managing and reporting the status of IT investments
5. Knowledge of IT investment processes, funding models and investment life cycle management, including benefits management
6. Knowledge of cost optimization
7. Knowledge of solution delivery processes and practices (systems development life cycle)
8. Knowledge of service delivery practices and processes
9. Knowledge of enterprise, information and IT architecture techniques and frameworks

2.2.4 Управління Ризиками

Гарантувати, що процес управління ризиками є невід'ємною частиною управління підприємством для ідентифікації, оцінки, пом'якшення, управління та моніторингу бізнес ризиків, пов'язаних із IT.

Tasks

1. Ensure that IT risk identification, assessment, mitigation, management, communication and monitoring strategies are integrated into business strategic and tactical planning processes.
2. Align the IT risk management processes with the enterprise business risk management framework (where this exists).
3. Ensure a consistent application of the risk management framework across the enterprise IT environment.
4. Ensure that risk assessment and management is included throughout the information life cycle.
5. Define risk management strategies, and prioritize responses to identified risks to maintain risk levels within the appetite of the enterprise.
6. Ensure that risk management strategies are adopted to mitigate risk and to manage to acceptable residual risk levels.
7. Implement timely reporting on risk events and responses to appropriate levels of management (including the use of key risk indicators, as appropriate).
8. Establish monitoring processes and practices to ensure the completeness and effectiveness of established risk management processes

Knowledge Statements

1. Knowledge of the context of risk management at the strategic, portfolio, program, project and operations level
2. Knowledge of risk management frameworks and standards (e.g., COSO ERM, MoR, OCTAVE, ISO31000, AS/NZ 4360:2004)
3. Knowledge of the enterprise's business objectives
4. Knowledge of the enterprise's risk management framework (including the risk classification model used to support risk identification and assessment)
5. Knowledge of the enterprise's external business environment

6. Knowledge of the enterprise's internal environment
7. Knowledge of how the enterprise defines and executes business strategies to achieve its goals and objectives
8. Knowledge of how to map business process down to IT process to understand dependencies and root cause
9. Knowledge of the enterprise's risk appetite
10. Knowledge of the enterprise's IT resources (applications, information, infrastructure and people)
11. Knowledge of the threats, vulnerabilities and opportunities inherent in the enterprise's use of IT
12. Knowledge of the types of business risks, exposures and threats that can be addressed using IT resources
13. Knowledge of quantitative and qualitative methods to determine sensitivity, criticality and maturity of IT-related contributions to business success
14. Knowledge of quantitative and qualitative methods (including enterprise-specific descriptive measurement scales, IT-related asset valuation methods and probability, use of both audit and stream data types, and impact and loss expectancy models/techniques) to assess IT risks
15. Knowledge of methods to discover more rare, but high-impact risk types, such as process analysis techniques
16. Knowledge of risk mitigation strategies in relation to the use of IT in the enterprise
17. Knowledge of risk management techniques that can be applied to affect enterprise risk management, particularly as they relate to IT-related activities
18. Knowledge of methods to effectively manage and report the status of identified risks

2.2.5 Управління Ресурсами

Гарантувати, що IT володіє достатніми, компетентними і здібними ресурсами для виконання поточних і майбутніх стратегічних цілей і йти в ногу з потребами бізнесу за рахунок оптимізації інвестицій, використання та розподілу IT активів.

Tasks

1. Ensure that the requirements for trained resources with the requisite skill sets are understood and are assessed appropriately.
2. Ensure the existence of appropriate policies for the training and development of all staff to help meet enterprise requirements and personal/professional growth.
3. Develop and facilitate the maintenance of systems to record the resources available and potentially available to the enterprise.
4. Undertake gap analyses to determine shortfalls against requirements to ensure that the business and IT resources (people, application, information, infrastructure) are able to meet strategic objectives.
5. Effectively and efficiently ensure clear, consistent and enforceable human resource allocation to investment programs and services.
6. Ensure that sourcing strategies are based on the effective use of existing resources and the identification of those that need be acquired.
7. Ensure that people, hardware, software and infrastructure procurement policies exist to effectively and efficiently fulfill resource requirements.
8. Through periodic assessment of the training requirements for human resources, ensure that sufficient, competent and capable human resources are available to execute the current and future strategic objectives and that they are kept up to date with constantly evolving technology.
9. Ensure integration of resource identification, classification, allocation and periodic evaluation processes into the business's strategic and tactical planning and operations.
10. Ensure that the IT infrastructure is standardized; economies of scale are achieved, wherever possible; and interoperability exists, where required, to support the agility needs of the enterprise.
11. Ensure that IT assets are managed and protected through their economic life cycle and are aligned with current and long-term business operations requirements to support cost-effective achievement of business objectives

Knowledge Statements

1. Knowledge of corporate business and IT resources (people, applications, infrastructure and information)
2. Knowledge of an enterprise's business and IT resources and acquisition processes (people, application, software, hardware, facilities and outsourced services)
3. Knowledge of the skill and technology mixes required to meet the enterprise's business objectives
4. Knowledge of human resource management processes and optimization practices needed to meet established technical and business proficiency, competency, and capability requirements
5. Knowledge of outsourcing and offshoring processes that may be employed to meet investment program and operation and service level agreements
6. Knowledge of the strengths and weaknesses inherent within the enterprise's human and technical business and IT resources and how to identify trainers with the requisite skill sets to maintain work competency and proficiency
7. Knowledge of enterprise business strategies
8. Knowledge of business and IT resource planning and strategic and tactical planning methods, techniques and processes
9. Knowledge of quantitative and qualitative methods used to determine and evaluate business and IT resource utilization and the availability of these resources to effectively meet enterprise objectives
10. Knowledge of methods for monitoring and reporting on business and IT resource performance

2.2.6 Вимірювання Продуктивності

Гарантувати, що IT цілі/завдання і заходи створені у співпраці з ключовими зацікавленими сторонами і можуть вимірюватися, відслідковуватися та оцінюватися.

Tasks

1. Establish the enterprise's strategic IT objectives, with the board of directors and executive leadership team, categorized into four areas: financial (business contribution), customer (user orientation), internal process (operational excellence), learning and growth (future orientation), or whatever areas are appropriate for the enterprise.
2. Establish outcome and performance measures, supported by metrics, and targets that assess progress toward the achievement of enterprise and IT objectives and the business strategy.
3. Evaluate IT process performance, track IT investment portfolio performance, and measure IT service delivery through the use of outcome measures and performance drivers.
4. Use maturity models and other assessment techniques to evaluate and report on the health of the enterprise's performance level.
5. Use continuous performance measurement to identify, prioritize, initiate and manage improvement initiatives and/or appropriate management action.
6. Report relevant portfolio, program and IT performance to relevant stakeholders in an appropriate, timely and accurate manner.

Knowledge Statements

1. Knowledge of the enterprise's business objectives
2. Knowledge of strategy mapping and balanced scorecard principles
3. Knowledge of the scope, objectives and benefits of commonly used IT maturity models, including their maturity attributes
4. Knowledge of data collection techniques for performance measurement
5. Knowledge of continuous improvement methodologies
6. Knowledge of IT governance implementation practices
7. Knowledge of characteristics of, and selection criteria for, measures and metrics
8. Knowledge of outcome measures and performance drivers

9. Knowledge of accepted practices in performance measurement (e.g., maturity models) and effective industry benchmarking techniques
10. Knowledge of tools and techniques that facilitate measurements, good communications and organizational change
11. Knowledge of automated monitoring tools and techniques
12. Knowledge of root cause analysis techniques
13. Knowledge of life cycle cost-benefit analysis techniques
14. Knowledge of evaluating and monitoring IT performance and value governance

2.3 Висновки

Проаналізувавши та порівнявши вимоги до вмінь та навиків спеціалістів IT, які готуються ВУЗами України із вимогами, які ставляться перед спеціалістами з управління IT, можна зробити наступні висновки:

- освіта в Україні направлена на підготовку сугубо технічних IT спеціалістів із великим уклоном на програмування та розробку IT систем
- технічний рівень випускників ВУЗів України на досить високому рівні, особливо це стосується спеціалістів із програмування та комп'ютерних систем
- основні спеціальні навчальні дисципліни направленні на навчання сугубо технічних навиків, і зовсім не розглядають такі навики як: лідерство, управління ресурсами, персоналом, бізнес процесами і т.д.
- ні один із напрямків підготовки IT спеціалістів у ВУЗах України не готує спеціалістів із управління IT
- вимоги до вмінь та навиків, що ставляться перед випускниками ВУЗів України по напряму підготовки IT абсолютно не відповідають навикам, що необхідні для управління IT
- тобто, навіть не розглядаючи предмети, що викладаються у ВУЗах, рівень підготовки викладачів, рівень студентів, а аналізуючи лише завдання, які ставлять ВУЗи перед випускниками, - очевидно, що випускники ВУЗів не мають знань, умінь та навиків, необхідних для управління IT

3. Аналіз рівня освіти та підготовки фахівців із управління інформаційною безпекою

3.1 Вимоги до знань, умінь та навиків спеціалістів інформаційної безпеки, яких готують ВУЗи України

Згідно Постанови Кабінету міністрів України № 787 від 27.08.2010 р. "Про затвердження переліку спеціальностей, за якими здійснюється підготовка фахівців у вищих навчальних закладах за освітньо-кваліфікаційними рівнями спеціаліста і магістра" та наказу Міністерства освіти і науки України № 1067 від 09.11.2010 р. з 2011/2012 навчального року вводиться в дію перелік спеціальностей, за якими здійснюється підготовка фахівців у ВУЗах України за освітньо-кваліфікаційними рівнями спеціаліста і магістра.
Згідно даного переліку спеціальностей, підготовка фахівців з інформаційної безпеки у вищих навчальних закладах України здійснюється за наступними спеціальностями:

Найменування	Напрям підготовки	Код	Найменування спеціальності спеціаліста
Інформаційна безпека	безпека інформаційних і комунікаційних систем	6.170101	безпека інформаційних і комунікаційних систем
			безпека державних інформаційних ресурсів
	системи технічного захисту інформації	6.170102	системи технічного захисту інформації, автоматизація її обробки
	управління інформаційною безпекою	6.170103	управління інформаційною безпекою
			адміністративний менеджмент у сфері захисту інформації

Проаналізуємо, які вимоги ставляться до знань, умінь та навичок, якими повинен володіти випускник ВУЗу по кожному напрямку підготовки «Інформаційна безпека» відповідно до ОКХ.

3.1.1 Напрям підготовки 6.170101 «Безпека інформаційних і комунікаційних систем»

Уміння та навички з предметної області

1. Супровід розробки та дослідження спеціальних технічних і програмно апаратних засобів захисту і обробки інформації в інформаційно комунікаційних системах
2. Дослідження архітектури комп'ютера
3. Управління периферійними пристроями
4. Організація обчислювальних процесів
5. Робота з базами даних
6. Організація аналізу загроз та захищеності для інформації в інформаційно комунікаційних системах
7. Розрахунки електричних кіл
8. Розрахунки імовірнісних та статистичних характеристик ТО
9. Аналіз та синтез дискретних об'єктів
10. Чисельні розрахунки
11. Розробка електронних схем
12. Розробка програм
13. Розробка комплексних систем захисту інформації
14. Розробка інформаційно комунікаційних систем та мереж
15. Забезпечення захищеності інформаційно комунікаційних систем і технологій
16. Забезпечення безпеки інформації в інформаційно комунікаційних системах та мереж ах
17. Розробка документації
18. Забезпечення організаційного захисту інформації

19. Забезпечення правового захисту інформації
20. Організація робіт по створенню КСЗІ та КТЗІ
21. Забезпечення організаційного захисту інформації
22. Забезпечення заходів та засобів охорони праці в установах (на підприємствах)
23. Забезпечення протипожежної безпеки та охорони довкілля в організаціях (на підприємствах)
24. Управління інформаційною безпекою
25. Користування комп'ютерними системами та використання комп'ютерних інформаційних технологій
26. Передача інформації
27. Кодування інформації
28. Забезпечення криптографічного захисту інформації
29. Забезпечення технічного захисту інформації
30. Проведення атестації технічних засобів та інформаційних ресурсів
31. Забезпечення контролю надання допусків до інформаційних ресурсів
32. Атестація, сертифікація та контроль робото спроможності систем і комплексів
33. Забезпечення інформаційної безпеки
34. Математичні перетворення та розрахунки
35. Розрахунки фізичних параметрів ТО

Знання з предметної області

1. знати основні положення захисту інформаційних ресурсів та баз даних інформаційно-комунікаційних систем на базі спеціальних програмних і технічних засобів захисту інформації з урахуванням вимог системи нормативно-правових і організаційних заходів;
2. знати управління доступом до інформаційно-комунікаційної системи та її послуг на основі положень політики безпеки організації на базі програмних та програмно-апаратних комплексів;
3. забезпечення цілісності і конфіденційності баз даних та інформаційних потоків в інформаційно-комунікаційних системах на основі положень політики безпеки організації на базі програмних та програмно-апаратних комплексів;
4. знати управління доступом до інформаційних ресурсів та баз даних в інформаційно-комунікаційних системах, в тому числі до програмних бібліотек та додатків;
5. основні способи впровадження і супроводження системного, об'єктно-орієнтованого та прикладного програмного забезпечення інформаційно-комунікаційних систем та аналіз його ефективності;
6. забезпечення цілісності та конфіденційності системного, об'єктно-орієнтованого та прикладного програмного забезпечення при його впровадженні, використанні чи обміні;
7. Знати основні положення по розробленню, впровадженню, дослідженню ефективності, супроводженню засобів та комплексів технічного захисту інформації в інформаційно-комунікаційних системах;
8. знати методи розроблення окремих складових, впровадження, супроводження та дослідження ефективності комплексних систем захисту інформації;
9. знати способи обстежень об'єкта інформаційної діяльності, автоматизованої системи та атестації засобів захисту інформаційних ресурсів з визначенням оцінки захищеності інформаційно-комунікаційних систем та їх ресурсів на базі використання спеціальних технічних засобів;

3.1.2 Напрям підготовки 6.170102 «Системи технічного захисту інформації»

Уміння та навички з предметної області

1. Дослідження у сфері забезпечення інформаційної безпеки
2. Розробка переліків (специфікацій) для проекту технічних засобів захисту інформації
3. Здійснювати розробку і проектування об'єктів, пристроїв і систем технічного захисту інформації
4. Організаційні механізми забезпечення інформаційної безпеки

5. Організація виконання завдань професійної діяльності
6. Підготовка та прийняття управлінських рішень
7. Управління системою забезпечення інформаційної безпеки
8. Забезпечення функціонування засобів систем технічного захисту інформації
9. Виконання діагностичних робіт із засобами та комплексами систем технічного захисту інформації
10. Забезпечення функціонування технічних систем внутрішньо об'єктового контролю та перепускного режиму
11. Проведення атестації технічних засобів та інформаційних ресурсів
12. Забезпечення контролю надання допусків до інформаційних ресурсів
13. Прогнозування стану інформаційної безпеки підприємства і визначення впливу ефективності задіяних заходів і засобів ТЗІ
14. Забезпечення ефективної експлуатації засобів системи технічного захисту інформації
15. Виконання ремонтних робіт із засобами та комплексами систем технічного захисту інформації

Знання з предметної області

1. знати основні положення нормативних документів по системах технічного захисту інформації;
2. вимоги до керівництва підрозділом підприємства, що відповідає за забезпечення інформаційної безпеки на підприємстві;
3. знати проектний менеджмент;
4. менеджмент безпеки трудових ресурсів;
5. маркетинг продуктів та послуг інформаційної безпеки;
6. основні загрози безпеці інформації;
7. управління інцидентами інформаційної безпеки;
8. знати забезпечення нормативної якості надання послуг технічного захисту інформації.

3.1.3 Напрям підготовки 6.170103 «Управління інформаційною безпекою»

Уміння та навички з предметної області

1. вміти розробляти системи управління інформаційною безпекою;
2. розроблення комплексних систем захисту інформації;
3. вміти розробляти заходи та технічні засобів захисту інформаційних ресурсів та баз даних обмеженого доступу;
4. розроблення модулів або компонентів програмних засобів захисту інформації з обмеженим доступом;
5. розроблення модулів або компонентів криптографічних засобів захисту інформації з обмеженим доступом;
6. вміти використовувати спеціалізовані захищені бази даних для накопичення та обробки інформації з обмеженим доступом;
7. аналізувати та формувати специфікацію вимог безпеки інформаційних систем.
8. вміти проводити аудит і сертифікацію (атестацію) систем, підсистем інформаційної безпеки та систем управління інформаційною безпекою;
9. вміти проводити експертизу комплексних систем захисту інформації;
10. вміти впроваджувати та випробувати СУІБ, КСЗІ;
11. вміти здійснювати підтримку та обслуговування СУІБ, КСЗІ;
12. вміти впроваджувати вимоги нормативно-технічної документації;
13. здійснювати організаційно-розпорядче документування інформації;
14. вміти організовувати захищений електронний документообіг, а також документообіг документів, що містять інформацію із обмеженим доступом;
15. вміти впроваджувати програмні системи автоматизованої обробки та захисту інформації з обмеженим доступом.

Знання з предметної області

1. знати основні положення нормативних документів по управлінню внутрішньою інформаційною безпекою;
2. знати аспекти управління неперервністю діяльності підприємства;
3. вимоги до керівництва підрозділом підприємства, що відповідає за забезпечення інформаційної безпеки на підприємстві;
4. знати проектний менеджмент;
5. менеджмент безпеки трудових ресурсів;
6. маркетинг продуктів та послуг інформаційної безпеки;
7. основні загрози та управління технічною вразливістю;
8. управління інцидентами інформаційної безпеки;
9. знати забезпечення нормативної якості надання послуг управління інформаційною безпекою.
10. управління розподілом та сертифікацією криптографічних ключів.

3.2 Вимоги до знань, умінь та навичок спеціалістів з управління інформаційною безпекою, відповідно до ISACA (Certified Information Security Manager)

3.2.1. Information Security Governance

Tasks

T1.1	Develop an information security strategy aligned with business goals and objectives.
T1.2	Align information security strategy with corporate governance.
T1.3	Develop business cases justifying investment in information security.
T1.4	Identify current and potential legal and regulatory requirements affecting information security.
T1.5	Identify drivers affecting the organization (e.g., technology, business environment, risk tolerance, geographic location) and their impact on information security.
T1.6	Obtain senior management commitment to information security.
T1.7	Define roles and responsibilities for information security throughout the organization.
T1.8	Establish internal and external reporting and communication channels that support information security.

Knowledge Statements

KS1.1	Knowledge of business goals and objectives
KS1.2	Knowledge of information security concepts
KS1.3	Knowledge of the components that comprise an information security strategy (e.g., processes, people, technologies, architectures)
KS1.4	Knowledge of the relationship between information security and business functions
KS1.5	Knowledge of the scope and charter of information security governance
KS1.6	Knowledge of concepts of corporate and information security governance
KS1.7	Knowledge of methods of integrating information security governance into the overall enterprise governance framework
KS1.8	Knowledge of budgetary planning strategies and reporting methods
KS1.9	Knowledge of methodologies for business case development
KS1.10	Knowledge of the types and impact of internal and external drivers (e.g., technology, business environment, risk tolerance) that may affect organizations and information security
KS1.11	Knowledge of regulatory requirements and their potential business impact from an information

security standpoint

KS1.12 Knowledge of common liability management strategies and insurance options (e.g., crime or fidelity insurance, business interruptions)

KS1.13 Knowledge of third-party relationships and their impact on information security (e.g., mergers and acquisitions, partnerships, outsourcing)

KS1.14 Knowledge of methods used to obtain senior management commitment to information security

KS1.15 Knowledge of the establishment and operation of an information security steering group

KS1.16 Knowledge of information security management roles, responsibilities and general organizational structures

KS1.17 Knowledge of approaches for linking policies to enterprise business objectives

KS1.18 Knowledge of generally accepted international standards for information security management

KS1.19 Knowledge of centralized and distributed methods of coordinating information security activities

KS1.20 Knowledge of methods for establishing reporting and communication channels throughout an organization

3.2.2. Information Risk Management

Tasks

T2.1 Establish a process for information asset classification and ownership.

T2.2 Implement a systematic and structured information risk assessment process.

T2.3 Ensure that business impact assessments are conducted periodically.

T2.4 Ensure that threat and vulnerability evaluations are performed on an ongoing basis.

T2.5 Identify and periodically evaluate information security controls and countermeasures to mitigate risk to acceptable levels.

T2.6 Integrate risk, threat and vulnerability identification and management into life cycle processes (e.g., project management, development, procurement and employment life cycles)

T2.7 Report significant changes in information risk to appropriate levels of management for acceptance on both a periodic and event-driven basis.

Knowledge Statements

KS2.1 Knowledge of required components for establishing an information classification schema consistent with business objectives (including the identification of assets)

KS2.2 Knowledge of the components of information ownership schema (including drivers of the schema, such as roles and responsibilities)

KS2.3 Knowledge of information threats, vulnerabilities and exposures

KS2.4 Knowledge of information resource valuation methodologies

KS2.5 Knowledge of risk assessment and analysis methodologies (including measurability, repeatability and documentation)

KS2.6 Knowledge of the factors used to determine risk reporting frequency and requirements

KS2.7 Knowledge of quantitative and qualitative methods used to determine sensitivity and criticality of information resources and the impact of adverse events on the business

KS2.8 Knowledge of baseline modeling and its relationship to risk-based assessments of control requirements

KS2.9 Knowledge of security controls and countermeasures

KS2.10 Knowledge of methods of analyzing the effectiveness of information security controls and countermeasures

KS2.11 Knowledge of risk mitigation strategies used in defining security requirements for information resources

KS2.12 Knowledge of gap analysis to assess the current state against generally accepted standards of good practice for information security management

KS2.13 Knowledge of cost-benefit analysis techniques for mitigating risks to acceptable levels

KS2.14 Knowledge of life cycle-based risk management principles and practices

3.2.3. Information Security Program Development

Tasks

T3.1 Develop and maintain plans to implement the information security strategy.

T3.2 Specify the activities to be performed within the information security program.

T3.3 Ensure alignment between the information security program and other assurance functions (e.g., physical, human resources (HR), quality, IT).

T3.4 Identify internal and external resources (e.g., finances, people, equipment, systems) required to execute the information security program.

T3.5 Ensure the development of information security architectures (e.g., people, processes, technology).

T3.6 Establish, communicate and maintain information security policies that support the security strategy.

T3.7 Design and develop a program for information security awareness, training and education.

T3.8 Ensure the development, communication, and maintenance of standards, procedures and other documentation (e.g., guidelines, baselines, codes of conduct) that support information security policies.

T3.9 Integrate information security requirements into the organization's processes (e.g., change control, mergers and acquisitions) and life cycle activities (e.g., development, employment, procurement).

T3.10 Develop a process to integrate information security controls into contracts (e.g., with joint ventures, outsourced providers, business partners, customers, third parties).

T3.11 Establish metrics to evaluate the effectiveness of the information security program.

Knowledge Statements

KS3.1 Knowledge of methods to interpret strategies into manageable and maintainable plans for implementing information security

KS3.2 Knowledge of the activities required within an information security program

KS3.3 Knowledge of methods for managing the implementation of the information security program

KS3.4 Knowledge of planning, designing, developing, testing and implementing information security controls

KS3.5 Knowledge of methods to align information security program requirements with those of other assurance functions (e.g., physical, HR quality, IT)

KS3.6 Knowledge of how to identify internal and external resources and skills requirements (e.g., finances, people, equipment, systems)

KS3.7 Knowledge of resource and skills acquisition (e.g., project budgeting, employment of contract staff, equipment purchase)

KS3.8 Knowledge of information security architectures (e.g., logical architectures and physical architectures) and their deployment

KS3.9 Knowledge of security technologies and controls (e.g., cryptographic techniques, access controls, monitoring tools)

KS3.10 Knowledge of the process for developing information security policies that meet and support enterprise business objectives

KS3.11 Knowledge of content for information security awareness, training and education across the enterprise (e.g., general security awareness, writing secure code, operating system controls)

KS3.12 Knowledge of methods to identify activities to close the gap between proficiency levels and skill requirements

KS3.13 Knowledge of activities to foster a positive security culture and behavior

KS3.14 Knowledge of the uses of and differences between policies, standards, procedures, guidelines and other documentation

KS3.15 Knowledge of the process for linking policies to enterprise business objectives

KS3.16 Knowledge of methods to develop, implement, communicate and maintain information security policies, standards, procedures, guidelines and other documentation

KS3.17 Knowledge of integrating information security requirements into organizational processes (e.g., change control, mergers and acquisition)

KS3.18 Knowledge of life cycle methodologies and activities (e.g., development, employment, procurement)

KS3.19 Knowledge of processes for incorporating security requirements into contracts (e.g., with joint ventures, outsourced providers, business partners, customers, third parties).

KS3.20 Knowledge of methods and techniques to manage third-party risks (e.g., service level agreements, contracts, due diligence, suppliers, subcontractors)

KS3.21 Knowledge of the design, development and implementation of information security metrics

KS3.22 Knowledge of certifying and accrediting the compliance of business applications and infrastructure to business needs

KS3.23 Methods for ongoing evaluation of the effectiveness and applicability of information security controls (e.g., vulnerability testing, assessment tools)

KS3.24 Knowledge of methods of tracking and measuring the effectiveness and currency of information security awareness, training and education

KS3.25 Knowledge of methods of sustaining the information security program (e.g., succession planning, allocation of jobs, documentation of the program)

3.2.4 Information Security Program Management

Tasks

T4.1 Manage internal and external resources (e.g., finances, people, equipment, systems) required executing the information security program.

T4.2 Ensure that processes and procedures are performed in compliance with the organization's information security policies and standards.

T4.3 Ensure the performance of contractually agreed (e.g., with joint ventures, outsourced providers, business partners, customers, third parties) information security controls.

T4.4 Ensure that information security is an integral part of the systems development process and acquisition processes.

T4.5 Ensure that information security is maintained throughout the organization's processes (e.g., change control, mergers and acquisitions) and life cycle activities (e.g., development, employment procurement).

T4.6 Provide information security advice and guidance (e.g., risk analysis, control selection) in the organization.

T4.7 Provide information security awareness, training and education to stakeholders (e.g., business process owners, users, information technology).

T4.8 Monitor, measure, test and report on the effectiveness and efficiency of information security controls and compliance with information security policies.

T4.9 Ensure that noncompliance issues and other variances are resolved in a timely manner

Knowledge Statements

KS4.1 Knowledge of interpreting and implementing information security policies

KS4.2 Knowledge of information security administrative processes and procedures (e.g., access controls, identity management, remote access)

KS4.3 Knowledge of methods for implementing and managing the enterprise's information security program in agreement with third parties (e.g., trade partners, contractors, joint venture partners, outsourcing providers)

KS4.4 Knowledge of methods for managing the information security program through security service providers

KS4.5 Knowledge of information-security-related contract provisions (e.g., right to audit, confidentiality, nondisclosure)

KS4.6 Knowledge of methods to define and monitor security requirements in service level agreements (SLAs)

KS4.7 Knowledge of methods and approaches to providing continuous monitoring of security activities in the enterprise's infrastructure and business applications

KS4.8 Knowledge of management metrics to validate the information security program investment (e.g., data collection, periodic review, key performance indicators)

KS4.9 Knowledge of methods of testing the effectiveness and applicability of information security controls (e.g., penetration testing, password cracking, social engineering, assessment tools)

KS4.10 Knowledge of change and configuration management activities

KS4.11 Knowledge of the advantages/disadvantages of using internal/external assurance providers to perform information security reviews

KS4.12 Knowledge of due diligence activities, reviews and related standards for managing and controlling access to information

KS4.13 Knowledge of external vulnerability, reporting sources for information on potential impacts on information security in applications and infrastructure

KS4.14 Knowledge of events affecting security baselines that may require risk reassessments and changes to information security program elements

KS4.15 Knowledge of information security problem management practices

KS4.16 Knowledge of reporting requirements of systems and infrastructure security status

KS4.17 Knowledge of general line management techniques including budgeting (e.g., estimating, quantifying, trade-offs), staff management (e.g., motivating, appraising, objective setting) and facilities (e.g., obtaining and using equipment)

3.2.5 Incident Management and Response

Tasks

T5.1	Develop and implement processes for detecting, identifying, analyzing and responding to information security incidents.
T5.2	Establish escalation and communication processes and lines of authority.
T5.3	Develop plans to respond to and document information security incidents.
T5.4	Establish the capability to investigate information security incidents (e.g., forensics, evidence collection and preservation, log analysis, interviewing)
T5.5	Develop a process to communicate with internal parties and external organizations (e.g., media, law enforcement, customers)
T5.6	Integrate information security incident response plans with the organization's disaster recovery (DR) and business continuity plan.
T5.7	Organize, train, and equip teams to respond to information security incidents.
T5.8	Periodically test and refine information security incident response plans.
T5.9	Manage the response to information security incidents.
T5.10	Conduct reviews to identify causes of information security incidents, develop corrective actions and reassess risk.

Knowledge Statements

KS5.1	Knowledge of the components of an incident response capability
KS5.2	Knowledge of disaster recovery planning and business continuity planning
KS5.3	Knowledge of information incident management practices
KS5.4	Knowledge of disaster recovery testing for infrastructure and critical business applications
KS5.5	Knowledge of events that trigger incident response
KS5.6	Knowledge of containing damage
KS5.7	Knowledge of notification and escalation processes for effective security management
KS5.8	Knowledge of the role of individuals in identifying and managing security incidents
KS5.9	Knowledge of crisis communications
KS5.10	Knowledge of methods of identifying business resources essential to recovery
KS5.11	Knowledge of the types and sources of tools and equipment required to adequately equip incident response teams
KS5.12	Knowledge of forensic requirements for collecting and presenting evidence (e.g., admissibility, quality and completeness of evidence, chain of custody)
KS5.13	Knowledge used to document incidents and subsequent actions
KS5.14	Knowledge of internal and external reporting requirements
KS5.15	Knowledge of postincident review practices and investigative methods to identify causes and determine corrective actions
KS5.16	Knowledge of techniques for quantifying damages, costs and other business impacts arising from security incidents
KS5.17	Knowledge of the recovery time objective (RTO) and its relationship to business continuity and contingency planning objectives and processes

3.3 Висновки

Проаналізувавши та порівнявши вимоги до вмінь та навиків спеціалістів із інформаційної безпеки, які готуються ВУЗами України із вимогами, які ставляться перед спеціалістами з управління інформаційною безпекою, можна зробити наступні висновки:

- освіта в Україні направлена на підготовку сугубо технічних спеціалістів із великим уклоном на технічні засоби захисту інформації та криптографію.
- основні спеціальні навчальні дисципліни направленні на навчання сугубо технічних навиків, і зовсім не розглядають такі навики як: лідерство, управління ресурсами, персоналом, бізнес процесами, ризиками і т.д.
- вимоги до вмінь та навиків, що ставляться перед випускниками ВУЗів України по напряму підготовки інформаційна безпека абсолютно не відповідають навикам, що необхідні для управління інформаційною безпекою.
- тобто, навіть не розглядаючи предмети, що викладаються у ВУЗах, рівень підготовки викладачів, рівень студентів, а аналізуючи лише завдання, які ставлять ВУЗи перед випускниками, - очевидно, що випускники ВУЗів не мають знань, умінь та навиків, необхідних для управління інформаційною безпекою.