67. Додаток 59. Критерії оцінювання компетентності фахівців за кваліфікацією «Аудитор систем менеджменту інформаційної безпеки (ДСТУ ISO/IEC 27001:2015 (ISO/IEC 27001:2013; Cor 1:2014, IDT)»

Ф-55-75
Додаток 59 до ДП ОСП-18

Критерії оцінювання компетентності фахівців за кваліфікацією
«Аудитор систем менеджменту інформаційної безпеки»
(ДСТУ ISO/IEC 27001:2015 (ISO/IEC 27001:2013; Cor 1:2014, IDT))

Особистісні характеристики

Аудитор систем менеджменту інформаційної безпеки (ДСТУ ISO/IEC 27001:2015 (ISO/IEC 27001:2013; COR 1:2014, IDT)) повинен ознайомитися з Кодексом професійної поведінки і декларувати в заяві на сертифікацію, що він цілком і твердо буде дотримувати положень цього документа.

Аудитор повинен бути здатним діяти у відповідності з принципами, сформульованими в ДСТУ ISO 19011:2012, ISO 19011:2011, ISO 19011:2018.

Аудитор повинен демонструвати професійну поведінку під час здійснення аудиторської діяльності, бути:

- Етичним, тобто порядним, чесним. Правдивим, щирим і тактовним
- Об`єктивним, тобто готовим розглядати альтернативні ідеї чи точки зору
- Дипломатичним, тобто тактовним при роботі з людьми
- Уважним, тобто активно спостерігати за фізичним оточенням та діяльністю
- Проникливим, тобто усвідомлювати та бути здатним зрозуміти ситуацію
- Гнучким, тобто швидко адаптовуватися до різних ситуацій
- Наполегливим, тобто непохитно фокусуватися на досягненні цілей
- Рішучим, тобто робити своєчасні висновки на основі логічних міркувань та аналізу
- Впевненим у собі, тобто діяти незалежно, ефективно взаємодіяти з іншими
- Здатним діяти відповідально і етично, навіть якщо такі дії не завжди популярні, а іноді можуть викликати незгоду чи конфронтацію
- Відкритим для вдосконалення, тобто брати уроки з ситуацій, прагнути до досягнення найкращих результатів аудиту
- Шанобливим до культури організації , що проходить аудит
- Сумісним та товариським, тобто ефективно взаємодіяти з іншими, враховуючи членів аудиторської команди та тих, що проходять аудит

Аудитор має бути здатним:

- Добре розбиратися в людях
- Перейматися проблемами тих, хто проходить аудит
- Висловлювати, переконувати і аргументувати, орієнтуючи на переваги
- Спілкуватись на застосовуваній мові усно і письмово
- Залишатись витриманим та цілеспрямованим навіть складних ситуаціях
- В достатній мірі посилатись на факти при звертанні до осіб на різних рівнях організації
- Взаємодіяти в процесно-орієнтованому стилі
- Попереджати і належним чином розбиратись з конфліктами
- В достатній мірі подавати результати
- Готувати та проводити наради
- Аудитор повинен бути добре організованим, тобто демонструвати ефективний менеджмент часу, вибір пріоритетів, планування та результативність

Напрям думок і філософія поведінки мають бути спрямовані на наступне:

- Переваги для осіб, та організацій, що проходять аудит (наприклад, з точки зору співвідношення витрати/переваги від власної діяльності)
- Розглядання вимог споживачів
- Успіх та стійкий розвиток компанії
- Підвищення цінності компанії (наприклад, фінансової чи етичної цінності)
- Можливості та ризики для організації (наприклад, виявлення та зниження ризиків; просування інновацій та кращої практики)
- Постійне вдосконалення (наприклад, стимулювання та просування постійного вдосконалення процесів)
- Просування і підтримка процесів навчання, розповсюдження інновацій (know-how)
- Моніторинг змін
- Мислення в термінах загального контексту всіх бізнес-процесів і всієї ланки процесів
- Застосування принципів PDCA
- Підвищення обов`язків
- Приклади для наслідування

Вимоги до спеціалізованої підготовки

Обсяг підготовки - 40 академічних годин.

Код		
	A	Розуміти і вміти пояснити
	B	На додаток до А, уміти вибирати відповідні методи і застосовувати їх
	C	На додаток до А і В, розробляти й інтегрувати відповідні методи й інтерпретувати результати

Зміст спеціалізованої підготовки

1	**Системи менеджменту інформаційної безпеки**	
1.1	Вимоги стандарту ISO/IEC 27001 в останній редакції.	**C**
1.2	Впровадження та супровід систем менеджменту інформаційної безпеки (СМЯ) з урахуванням нормативних вимог і процесного підходу	**B**
1.3	Розуміння та володіння (практичний досвід) використання заходів безпеки, що наведені в додатку А стандарту ДСТУ ISO/IEC 27001:2015 (ISO/IEC 27001:2013; COR 1:2014, IDT)	**A**
1.4	Методи для визначення ризиків та можливостей.	**B**
1.5	Методи і прийоми, пов'язані з системою менеджменту інформаційної безпеки	**B**
1.6	Термінологія, принципи менеджменту інформаційної безпеки та їх застосування	**B**
1.7	Технологія модерації. Загальне уявлення про процеси керування динамікою групової роботи	**B**
1.8	Теорії мотивації (наприклад, Маслоу, Херсберга та ін.)	**B**
1.9	Знання, пов'язані з конкретною галуззю (термінологія відповідної галузі економіки, технічні характеристики, що відносяться до процесів та продукції, включаючи послуги та кращі практики галузі), можливі особливості відповідних галузях промисловості	**C**
1.10	Застосовні стандарти у відповідній галузі економіки	**B**
2	**Аудит**	
2.1	Стандарти ДСТУ ISO 19011:2012, ISO 19011:2011, ISO 19011:2018.	**C**
2.2	Класифікації аудитів (різні класифікації, цілі, відмінності, визначення)	**C**
2.3	Роль і відповідальність Аудитора і Головного Аудитора в аудиторській групі (компетенції, особисті якості, вміння та ноу-хау, підготовка та	**B**

	інформування, ноу-хау головного аудитора)	
2.4	Принципи, порядок та методи аудиту (принципи аудиторської діяльності, управління програмами аудиту, управління аудитом, невідповідності);	**B**
2.5	Документи та інша інформація, пов'язана з системами менеджменту (застосування систем менеджменту, пов'язаних з різними організаціями, взаємодії між різними компонентами системи менеджменту, стандарти на системи управління, законодавство, правила та інші застосовні вимоги, що мають відношення предмету аудиту).	**C**
2.6	Особливості аудиту третьої сторони, стандарти ДСТУ ISO/IEC 17021-1:2017, ISO/IEC 17021-1:2015, ISO/IEC TS 17021-3:2017.	**B**

Вимоги до процесу оцінювання професійних характеристик

Загальні знання і навички	Загальні знання і навички на рівні, який можна звичайно досягти, одержавши **вищу освіту**.
Спеціальні знання і навички	Компетентність проводити перевірки відповідності систем управління якістю вимогам ДСТУ ISO/IEC 27001:2015, ISO/IEC 27001:2015. Спеціальні знання і навички можуть бути досягнуті шляхом: **1. Спеціальної програми навчання з менеджменту інформаційної безпеки**. **<u>Зміст навчальної програми</u>:** цілі і задачі навчання повинні охоплювати знання і навички визначені вище. <u>Тривалість і методи</u>: 40 ак. годин (по 45 хв.). навчання в аудиторіях (або 24 години у випадку розширення галузей економіки, додаткове навчання за пунктами 1.9. та 1.10. спеціальної підготовки). Для претендента, який має кваліфікацію Аудитора або Головного аудитора з іншої системи менеджменту, необхідно пройти навчання тривалістю 24 години за пунктами 1.1. - 1.10. спеціальної підготовки). Альтернативні форми навчання (наприклад, самонавчання, електронне навчання), можуть бути визначені в навчальній програмі, якщо відповідають цілям навчання, але не більше ніж на 40% загального обсягу навчальних годин. Альтернативні форми навчання можуть бути застосовані, якщо виконуються наступні умови: Ø Форма навчання підходить для цілей навчання. Ø Будь-яка форма навчання повинна бути зазначена в навчальному плані навчального закладу. Виконання навчального плану повинне бути документально підтверджено навчальною установою. **2. Аудиторської практики** Виконання аудиторської діяльності **не менше 4 повних аудитів системи менеджменту інформаційної безпеки чи аудитів бізнес - процесів, загальною тривалістю не менш 20 днів (з них не менше 12 днів на місці) протягом 3 останніх років перед сертифікацією в якості аудитора - стажиста під керівництвом і управлінням кваліфікованого аудитора з компетенціями Головного Аудитора.** Головний аудитор (у команді аудиту) повинен бути професійно кваліфікований в органі з сертифікації / сертифікований органом з сертифікації персоналу у відповідній галузі промисловості. Для розширення галузей економіки **необхідна участь у 10 аудитах у відповідній галузі економіки за участю технічного спеціаліста у відповідній галузі економіки або продемонструвати досвід роботи у**

	відповідному секторі економіки щонайменше 3 роки.
Вимоги до освіти та практичного досвіду	· Кандидати на одержання сертифіката за кваліфікацією «Аудитор систем менеджменту інформаційної безпеки» повинні мати **вищу освіту, що відноситься до відповідної галузі економіки**. Аудитор систем менеджменту інформаційної безпеки Органу сертифікації персоналу Української асоціації якості (ОСП УАЯ) повинен мати не менше **5 років робочого досвіду для бакалаврів і 4 років для магістрів, з них не менш ніж 3 роки у відповідній галузі економіки**, на професійних чи технічних посадах, залучених у розслідування і рішення проблем у взаємодії з іншими керівниками, професіоналами, експертами, клієнтами і/чи зацікавленими сторонами, а також співробітників, що залучаються у керування групами, у робочих ситуаціях. Якщо кандидат займався консалтингом у відповідній галузі економіки, то необхідні роки роботи у цій галузі можуть бути еквівалентні особисто розробленим і доведеним до сертифікації як мінімум **шести відповідних систем менеджменту.** · Аудитор систем менеджменту інформаційної безпеки ОСП УАЯ повинен мати, принаймні, **2 роки практичного досвіду роботи у сфері менеджменту інформаційної безпеки або захисту інформації.** · **Практичний досвід роботи в ІТ 3 роки** · Особистісні характеристики (поведінка, напрям думок) повинні відповідати, визначеним вище і бути продемонстровані шляхом підписання **Кодексу професійної поведінки ОСП УАЯ**.