دورة خبير معتمد في إدارة المخاطر وضوابط نظم المعلومات
(CRISC) – ISACA

****دورة تدريبية وامتحان****

****(20)ساعة****

ما الفرق الذي تقدمه شهادةCRISC ؟

شهادة **معتمد في إدارة مخاطر وضوابط نظم المعلومات** (CRISC) تُظهر خبرتك في إدارة مخاطر تكنولوجيا المعلومات. من خلال اتباع نهج استباقي، ستتعلم كيفية تعزيز مرونة وديمومة الأعمال في مؤسستك، وتقديم قيمة لأصحاب المصلحة، وتحسين إدارة المخاطر عبر المؤسسة. كحامل لشهادة CRISC ، ستكون مستعدًا لمواجهة التكنولوجيا الناشئة، بما في ذلك تقييم مخاطر الذكاء الاصطناعي وأفضل الممارسات العامة لإدارة المخاطر والتخفيف منها فيما يتعلق بحوكمة وأخلاقيات بيانات الذكاء الاصطناعي.

كيف تستفيد منها؟

تجمع الشهادة مجموعة المعارف والمهارات التي يحتاجها صاحب العمل، ومن خلال الاطلاع على محاور الشهادة نلاحظ بأنها تعني وقريبة جدا من تخصصات كلية إدارة الأعمال وكلية تكنولوجيا المعلومات، حيث تركز موايعها على ما يلي:

1. **حوكمة تكنولوجيا المعلومات المؤسسية**
2. **تقييم مخاطر تكنولوجيا المعلومات**
3. **الاستجابة للإبلاغ عن المخاطر**
4. **تكنولوجيا المعلومات والأمن السيبراني**

لماذا تحصل على شهادة CRISC ؟

- شهادة CRISC من ISACA معترف بها عالميًا.
- شهادة CRISC تمنحك المصداقية للتقدم في حياتك المهنية.
- شهادة CRISC تثبت لأصحاب العمل أنك قادر على إضافة قيمة لمؤسستهم.
- مطلوبة للعديد من المنظمات والوكالات الحكومية
- متطلبات الحصول على الشهادة تؤكد لصاحب العمل وجهة التوظيف أن حاملها يجمع بين المعارف والخبرة العملية.

منظمة (ISACA) مانحة الشهادة:

الوصول العالمي والتأثير

لأكثر من 50 عامًا، ساعدت ISACA الأفراد والمؤسسات في جميع أنحاء العالم على تطوير مساراتهم المهنية، وتحويل مؤسساتهم، وبناء عالم رقمي أكثر ثقة وأخلاقية.

ISACAهي جمعية مهنية عالمية ومنظمة تعليمية تضم 185,000 عضو يعملون في مجالات التكنولوجيا الرقمية مثل أمن المعلومات، والحوكمة، وإدارة المخاطر، والخصوصية، والجودة. مع وجودها في 188 دولة و225 فرعًا حول العالم، تُعترف بـ ISACA في جميع أنحاء العالم لتوجيهاتها، وشهاداتها، وتعليمها، وتدريبها، ومجتمعها. لخدمة مجتمعها المهني في جميع أنحاء العالم، أنشأت ISACA ثلاثة مكاتب في أمريكا الشمالية، وأوروبا، والصين.

مجالات العمل والتوظيف:

شهادة **معتمد في إدارة مخاطر وضوابط نظم المعلومات** (CRISC)تُعد واحدة من الشهادات الرائدة في مجال إدارة مخاطر تكنولوجيا المعلومات، وهي تفتح أبوابًا واسعة لحامليها للعمل في العديد من المجالات والوظائف المتعلقة بإدارة المخاطر، والأمن السيبراني، وحوكمة تكنولوجيا المعلومات. فيما يلي بعض المجالات والوظائف التي يمكن لحامل شهادة CRISC العمل فيها:

1. مدير إدارة المخاطر(Risk Manager)
   - مسؤول عن تحديد وتقييم وإدارة المخاطر التي تواجه المؤسسة، خاصة تلك المتعلقة بتكنولوجيا المعلومات.
   - تطوير استراتيجيات للتخفيف من المخاطر وضمان الامتثال للوائح والمعايير.

2. مدير أمن المعلومات(Information Security Manager)
   - يشرف على حماية أنظمة المعلومات والبيانات من التهديدات الداخلية والخارجية.
   - يضمن تطبيق أفضل الممارسات الأمنية والسياسات لحماية أصول المعلومات.

3. مدير حوكمة تكنولوجيا المعلومات(IT Governance Manager)
   - مسؤول عن ضمان أن أنظمة تكنولوجيا المعلومات تتماشى مع أهداف الأعمال وتلتزم بالمعايير التنظيمية.
   - يعمل على تحسين عمليات الحوكمة داخل المؤسسة.

4. محلل مخاطر تكنولوجيا المعلومات(IT Risk Analyst)
   - يقوم بتحليل وتقييم المخاطر المرتبطة بأنظمة تكنولوجيا المعلومات.
   - يقدم توصيات لتحسين إدارة المخاطر وضمان استمرارية الأعمال.

5. مدير ضوابط نظم المعلومات (Information Systems Control Manager)
- مسؤول عن تصميم وتنفيذ ضوابط نظم المعلومات لضمان فعالية وكفاءة العمليات.
- يراقب الامتثال للضوابط الداخلية والخارجية.

6. مستشار إدارة المخاطر (Risk Management Consultant)
- يعمل كخبير خارجي لتقديم المشورة للمؤسسات حول أفضل الممارسات في إدارة المخاطر.
- يساعد في تطوير استراتيجيات إدارة المخاطر وتحسين العمليات.

7. مدير استمرارية الأعمال (Business Continuity Manager)
- مسؤول عن ضمان استمرارية الأعمال في حالة حدوث كوارث أو أزمات.
- يطور خطط استمرارية الأعمال واختبارها بشكل دوري.

8. مدير الامتثال (Compliance Manager)
- يضمن أن المؤسسة تلتزم باللوائح والقوانين المحلية والدولية المتعلقة بتكنولوجيا المعلومات وإدارة المخاطر.
- يقوم بمراجعة وتقييم عمليات الامتثال بشكل منتظم.

9. محلل أمن المعلومات (Information Security Analyst)
- يراقب أنظمة المعلومات للكشف عن التهديدات الأمنية والاستجابة لها.
- يقوم بتطوير وتنفيذ إجراءات أمنية لحماية البيانات والأنظمة.

10. مدير مشاريع إدارة المخاطر (Risk Management Project Manager)
- يدير مشاريع متعلقة بإدارة المخاطر، مثل تنفيذ أنظمة إدارة المخاطر أو تحسين العمليات الحالية.
- يضمن أن المشاريع تُنفذ في الوقت المحدد وبالميزانية المقررة.

11. مدير أمن الذكاء الاصطناعي (AI Security Manager)
- مع التطور السريع لتكنولوجيا الذكاء الاصطناعي، يمكن لحامل شهادة CRISC العمل في مجال إدارة مخاطر الذكاء الاصطناعي.
- يضمن أن أنظمة الذكاء الاصطناعي آمنة وتلتزم بالمعايير الأخلاقية والقانونية.

12. مدير حوكمة البيانات (Data Governance Manager)
- مسؤول عن إدارة سياسات وإجراءات حوكمة البيانات داخل المؤسسة.
- يضمن أن البيانات تُدار بشكل آمن وفعال وفقًا للمعايير التنظيمية.

13. مدير الخصوصية (Privacy Manager)
- يركز على حماية خصوصية البيانات الشخصية داخل المؤسسة.
- يضمن الامتثال للقوانين المتعلقة بالخصوصية مثل GDPR.

14. مدير عمليات الأمن (Security Operations Manager)
- يشرف على عمليات الأمن اليومية، بما في ذلك مراقبة التهديدات والاستجابة للحوادث الأمنية.
- يضمن أن الفرق الأمنية تعمل بشكل فعال لحماية المؤسسة.

15. مدير تقييم المخاطر (Risk Assessment Manager)
- مسؤول عن إجراء تقييمات دورية للمخاطر التي تواجه المؤسسة.
- يقدم تقارير مفصلة عن المخاطر المحتملة ويوصي بإجراءات التخفيف.

16. مدير ضمان المعلومات (Information Assurance Manager)
- يركز على ضمان أن أنظمة المعلومات تعمل بشكل آمن وفعال.
- يضمن أن المؤسسة تلتزم بمعايير أمن المعلومات.

17. مدير أمن السحابة (Cloud Security Manager)
- مع الانتشار الواسع للحوسبة السحابية، يمكن لحامل شهادة CRISC العمل في مجال أمن السحابة.
- يضمن أن البيانات والأنظمة السحابية محمية من التهديدات.

18. مدير أمن الشبكات (Network Security Manager)
- مسؤول عن حماية شبكات المؤسسة من التهديدات الإلكترونية.
- يشرف على تصميم وتنفيذ إجراءات أمن الشبكات.

19. مدير أمن التطبيقات (Application Security Manager)
- يركز على تأمين التطبيقات البرمجية ضد الثغرات الأمنية.
- يضمن أن التطبيقات تُطور وتُنفذ وفقًا لأفضل الممارسات الأمنية.

20. مدير أمن البنية التحتية (Infrastructure Security Manager)
- مسؤول عن تأمين البنية التحتية لتكنولوجيا المعلومات، بما في ذلك الخوادم وقواعد البيانات.
- يضمن أن البنية التحتية محمية من التهديدات الداخلية والخارجية.

21. مدير أمن الأجهزة الطرفية (Endpoint Security Manager)
- يركز على تأمين الأجهزة الطرفية مثل أجهزة الكمبيوتر والأجهزة المحمولة.
- يضمن أن هذه الأجهزة محمية من البرمجيات الخبيثة والتهديدات الأخرى.

22. مدير أمن الهوية والوصول (Identity and Access Management Manager)
- مسؤول عن إدارة هويات المستخدمين والتحكم في الوصول إلى الأنظمة والبيانات.
- يضمن أن الوصول يتم بشكل آمن ووفقًا لسياسات المؤسسة.

23. مدير أمن البيانات (Data Security Manager)
- يركز على حماية البيانات الحساسة داخل المؤسسة.
- يضمن أن البيانات محمية من الوصول غير المصرح به والاختراقات.

24. مدير أمن العمليات(Operational Security Manager)
- مسؤول عن تأمين العمليات اليومية للمؤسسة.
- يضمن أن العمليات تتم بشكل آمن وفعال.

25. مدير أمن التكنولوجيا التشغيلية(Operational Technology Security Manager)
- يركز على تأمين الأنظمة التشغيلية مثل أنظمة التحكم الصناعي.
- يضمن أن هذه الأنظمة محمية من التهديدات الإلكترونية.

26. مدير أمن إنترنت الأشياء(IoT Security Manager)
- مع تزايد استخدام إنترنت الأشياء، يمكن لحامل شهادة CRISC العمل في مجال أمن إنترنت الأشياء.
- يضمن أن أجهزة إنترنت الأشياء محمية من التهديدات.

27. مدير أمن السلسلة الكتلية(Blockchain Security Manager)
- يركز على تأمين أنظمة السلسلة الكتلية.(Blockchain)
- يضمن أن هذه الأنظمة محمية من التهديدات الإلكترونية.

28. مدير أمن الذكاء الاصطناعي(AI Security Manager)
- يركز على تأمين أنظمة الذكاء الاصطناعي.
- يضمن أن هذه الأنظمة محمية من التهديدات الإلكترونية.

29. مدير أمن البيانات الضخمة(Big Data Security Manager)
- يركز على تأمين أنظمة البيانات الضخمة.
- يضمن أن هذه الأنظمة محمية من التهديدات الإلكترونية.