CGRC® – Certified in Governance Risk and Compliance (E-Learning)

ISC2

- **Nível:** Avançado
- **Duração:** h

Sobre o curso

O curso Certified in Governance, Risk and Compliance (CGRC) oferece uma compreensão e revisão abrangente dos conhecimentos necessários à autorização e manutenção de sistemas de informação como parte do Risk Management Framework (RMF) do NIST.

O presente curso de formação ajudará os participantes a rever e atualizar os seus conhecimentos, ao mesmo tempo que identificam as áreas que necessitam de estudar para o exame CGRC. O conteúdo programático encontra-se alinhado com os sete domínios do Common Body of Knowledge (CBK®) do CGRC da ISC2, abordando-os de forma abrangente.

O material oficial do curso foi desenvolvido pela ISC2, criadora do CBK do curso de certificação CGRC, garantindo que a formação é relevante e se encontra atualizada. Os formadores da ISC2 são especialistas de segurança certificados, possuidores da certificação CGRC, e que realizaram uma formação intensiva para estarem autorizados a ensinar o conteúdo da ISC2.

Destinatários

O curso destina-se a todos os interessados em obter a certificação CGRC. A realização do curso e a, consequente, obtenção da certificação CGRC é ideal para profissionais de TI, de segurança da informação e de garantia da informação, bem como a outros profissionais que utilizam o RMF no governo federal, em cargos militares e civis, em governos locais e em organizações do sector privado. Os cargos incluem:

- ISSOs, ISSMs e outros profissionais de segurança da informação/garantia da informação focados em questões de avaliação e de autorização (C&A) da segurança e de monitorização contínua.
- Executivos que devem autorizar a execução do processo de Authority to Operate (ATO).
- Inspetores gerais (IGs) e auditores que executam revisões independentes.
- Gestores de programas que desenvolvem ou mantêm sistemas de TI.
- Profissionais de TI interessados em melhorar a cibersegurança e em aprender mais sobre a importância da gestão de riscos de cibersegurança ao longo do ciclo de vida.

Objetivos

Após a conclusão deste curso, os participantes deverão ser capazes de:

- Identificar e descrever as fases e as tarefas associados ao Risk Management Framework (RMF) do NIST.
- Aplicar elementos comuns de outros frameworks de gestão de riscos e utilizar, em simultâneo, o RMF como guia.
- Descrever as funções associadas ao RMF e como as mesmas são atribuídas a determinadas tarefas do RMF.
- Realizar tarefas no processo de RMF com base na atribuição de uma ou mais funções do RMF.
- Explicar a gestão de riscos organizacional e como a mesma tem por base o RMF.

Condições

Para particulares
• 10% do valor total pago no ato da inscrição; restante valor até 7 dias antes do início do curso.
• Formandos não residentes em Portugal: pagamento de 50% no ato da inscrição; restante valor até 7 dias antes do início do curso.
• Possibilidade de beneficiar do Cheque Formação+Digital até 750€ (conforme elegibilidade).
• Isenção de IVA para particulares.
Para empresas
• Empresas nacionais: pagamento a 30 dias, contra fatura (acresce IVA à taxa legal em vigor).
• Empresas da UE e fora da UE: valores isentos de IVA e pagamento a pronto.

Pré-requisitos

A frequência no curso de certificação CGRC requer um mínimo de dois anos de experiência profissional cumulativa, remunerada e a tempo inteiro num ou mais dos sete domínios do Common Body of Knowledge (CBK) do CGRC.

Metodologia

A Formação Oficial ISC2 Online Self-Paced CGRC constitui uma forma inovadora de preparação para a certificação que utiliza inteligência artificial para personalizar o teu percurso de aprendizagem. Identifica as áreas que exigem foco adicional e orienta-te na preparação para o exame de forma verdadeiramente personalizada.

Estuda de forma mais inteligente com estas principais vantagens:

- **Instrução personalizada** – O conteúdo, o ritmo e a dificuldade adaptam-se ao teu nível de conhecimento, velocidade de aprendizagem e nível de confiança.

- **Maior envolvimento** – Feedback imediato e conteúdo dinâmico permitem-te aprender a um nível adequado.
- **Poupança de tempo** – O tempo de formação é otimizado ao focar-se nas áreas que exigem maior revisão.
- **Melhores resultados de aprendizagem** – A plataforma identifica as áreas que exigem revisão adicional e disponibiliza suporte direcionado para maximizar a tua compreensão do conteúdo.

A formação Certified in Governance, Risk, and Compliance (CGRC) tira partido do poder da inteligência artificial, orientando os formandos numa experiência de aprendizagem ao seu ritmo, adaptada às suas necessidades. Abrange os conhecimentos e competências necessários para desenhar, desenvolver e gerir a postura global de segurança de uma organização.

O exame incluído no curso é presencial e realiza-se num centro Pearson VUE Select, em Lisboa.

Programa

- Preparação
- Categorização
- Seleção
- Implementação
- Avaliação
- Autorização
- Monitorização
- Informação sobre a Certificação CGRC

Capítulo 1: Preparação (10 Módulos)

- Explicar o propósito e o valor da fase de preparação.
- Identificar referências associadas à fase de preparação.
- Identificar outras frameworks de gestão de risco e a relação das mesmas com as tarefas do RMF.
- Identificar regulamentos relevantes nas áreas de segurança e privacidade.
- Listar as referências, os processos e os resultados que definem as tarefas:
    - RMF Task P-1: Risk Management Roles
    - RMF Task P-2: Risk Management Strategy
    - RMF Task P-3: Risk Assessment – Organization
    - RMF Task P-14: Risk Assessment – System
    - RMF Task P-4: Organizationally Tailored Control Baselines and Cybersecurity Framework Profiles
    - RMF Task P-5: Common Control Identification
    - RMF Task P-6: Impact-Level Prioritization
    - RMF Task P-7: Continuous Monitoring Strategy – Organization
    - RMF Task P-8: Mission or Business Focus
    - RMF Task P-9: System Stakeholders
    - RMF Task P-10: Asset Identification
    - RMF Task P-11: Authorization Boundary

    - RMF Task P-12: Information Types
    - RMF Task P-13: Information Life Cycle
    - RMF Task P-15: Requirements Definition
    - RMF Task P-16: Enterprise Architecture
    - RMF Task P-17: Requirements Allocation
    - RMF Task P-18: System Registration
- Completar as tarefas da fase de Preparação selecionadas no sistema de exemplo.

Capítulo 2: Categorização (5 Módulos)

- Explicar o propósito e o valor da fase de categorização.
- Identificar referências associadas à fase de categorização.
- Listar as referências, os processos e os resultados que definem a tarefa RMF Task C-1: System Description.
- Descrever a arquitetura de um sistema.
- Descrever o propósito e a funcionalidade de um sistema de informação.
- Descrever e documentar as características de um sistema.
- Listar as referências, os processos e os resultados que definem a tarefa RMF Task C-2: Security Categorization.
- Categorizar um sistema de informação.
- Listar as referências, os processos e os resultados que definem a tarefa RMF Task C-3: Security Categorization Review and Approval.
- Descrever o processo de revisão e aprovação da categorização de segurança.
- Categorizar os sistemas de exemplo.

Capítulo 3: Seleção (7 Módulos)

- Explicar o propósito e o valor da fase de seleção e da alocação do controlo.
- Identificar referências associadas à fase de seleção.
- Relacionar a Declaração de Aplicabilidade da norma ISO 27001 com o RMF do NIST.
- Listar as referências, os processos e os resultados que definem a tarefa RMF Task S-1: Control Selection.
- Listar as referências, os processos e os resultados que definem a tarefa RMF Task S-2: Control Tailoring.
- Selecionar as linhas de base do controlo de segurança apropriadas de acordo com a orientação organizacional.
- Ajustar os controlos de um sistema dentro de um ambiente operacional específico.
- Listar as referências, os processos e os resultados que definem a tarefa RMF Task S-3: Control Allocation.
- Listar as referências, os processos e os resultados que definem a tarefa RMF Task S-4: Documentation of Planned Control Implementations.
- Alocar os controlos de segurança e privacidade no sistema e no ambiente operacional.
- Documentar os controlos do sistema e do ambiente operacional existentes em planos de segurança e privacidade.
- Listar as referências, os processos e os resultados que definem a tarefa RMF Task S-5: Continuous Monitoring Strategy – System.
- Desenvolver e implementar uma estratégia ao nível do sistema para monitorizar a eficácia dos controlos, e que seja consistente e suplemente a estratégia organizacional de monitorização contínua.
- Listar as referências, os processos e os resultados que definem a tarefa RMF Task S-6: Plan Review and

Approval.
- Rever e aprovar os planos de segurança e privacidade do sistema e do ambiente operacional.
- Alocar os controlos de segurança no sistema de exemplo.
- Ajustar os controlos de segurança do sistema de exemplo.
- Elaborar um plano de monitorização contínua para o sistema de exemplo.

Capítulo 4: Implementação (5 Módulos)

- Explicar o propósito e o valor da fase de implementação
- Identificar referências associadas à fase de implementação
- Listar as referências, os processos e os resultados que definem a tarefa RMF Task I-1: Control Implementation
- Identificar as orientações adequadas à implementação de frameworks de controlo
- Integrar os requisitos de privacidade com a implementação do sistema
- Listar as referências, os processos e os resultados que definem a tarefa RMF Task I-2: Update Control Implementation Information
- Atualizar a estratégia de monitorização contínua
- Atualizar o plano de implementação de controlo

Capítulo 5: Avaliação (6 Módulos)

- Explicar o propósito e o valor da fase de avaliação.
- Identificar referências associadas à fase de avaliação.
- Compreender e identificar os elementos comuns do processo NIST que estão incluídos noutras frameworks e processos.
- Listar as referências, os processos e os resultados que definem a tarefa RMF Task A-1: Assessor Selection.
- Listar as referências, os processos e os resultados que definem a tarefa RMF Task A-2: Assessment Plan.
- Listar as referências, os processos e os resultados que definem a tarefa RMF Task A-3: Control Assessment.
- Listar as referências, os processos e os resultados que definem a tarefa RMF Task A-4: Assessment Reports.
- Listar as referências, os processos e os resultados que definem a tarefa RMF Task A-5: Remediation Actions.
- Listar as referências, os processos e os resultados que definem a tarefa RMF Task A-6: Plan of Action and Milestones.
- Desenvolver um plano de avaliação para os controlos identificados no sistema de exemplo.
- Desenvolver um plano de remediação para controlos não satisfeitos no sistema de exemplo.

Capítulo 6: Autorização (6 Módulos)

- Explicar o propósito e o valor da fase de autorização.
- Identificar referências associadas à fase de autorização.
- Relacionar aprovações de sistema aos conceitos aplicados no RMF do NIST.
- Listar as referências, os processos e os resultados que definem a tarefa RMF Task R-1: Authorization Package.
- Listar as referências, os processos e os resultados que definem a tarefa RMF Task R-2: Risk Analysis and

Determination.
- Listar as referências, os processos e os resultados que definem a tarefa RMF Task R-3: Risk Response.
- Listar as referências, os processos e os resultados que definem a tarefa RMF Task R-4: Authorization Decision.
- Listar as referências, os processos e os resultados que definem a tarefa RMF Task R-5: Authorization Reporting.
- Desenvolver uma ferramenta de determinação de risco para o sistema de exemplo no nível de risco do sistema.
- Autorizar o funcionamento do sistema.
- Determinar os elementos apropriados ao documento de decisão de autorização do sistema de exemplo.

Capítulo 7: Monitorização (8 Módulos)

- Explicar o propósito e o valor da fase de monitorização.
- Identificar referências associadas à fase de monitorização.
- Listar as referências, os processos e os resultados que definem a tarefa RMF Task M-1: System and Environment Changes.
- Integrar a gestão de riscos de cibersegurança com a gestão da mudança organizacional.
- Listar as referências, os processos e os resultados que definem a tarefa RMF Task M-2: Ongoing Assessments.
- Monitorizar os riscos associados à cadeia de fornecimento.
- Listar as referências, os processos e os resultados que definem a tarefa RMF Task M-3: Ongoing Risk Response.
- Compreender os elementos de comunicação associados a um evento cibernético.
- Listar as referências, os processos e os resultados que definem a tarefa RMF Task M-4: Authorization Package Updates.
- Listar as referências, os processos e os resultados que definem a tarefa RMF Task M-5: Security and Privacy Reporting.
- Listar as referências, os processos e os resultados que definem a tarefa RMF Task M-6: Ongoing Authorization.
- Listar as referências, os processos e os resultados que definem a tarefa RMF Task M-7: System Disposal.
- Discutir as atividades da fase de Monitorização no sistema de exemplo.

Capítulo 8: Informação sobre a Certificação CGRC

Neste capítulo são abordadas informações importantes sobre os requisitos de experiência necessários à certificação CGRC, bem como políticas e procedimentos do exame ISC2.