ISACA®
Confiança e Valor em Sistemas de Informação
São Paulo Chapter

Tendências e Certificações Profissionais da ISACA

ISACA Capítulo São Paulo

Fabio Penna Curto, CGEIT, CISM, Diretor
Cristiano Borges, Diretor ISACA SP
Carmen Ozores, Vice presidente – ISACA SP

Contato: info@isaca.org.br

ISACA®
Confiança e Valor em Sistemas de Informação
São Paulo Chapter

ISACA Internacional

ISACA Brasil !

Capítulo São Paulo, 2001
Capítulos RJ e DF, em 2009

Mais de 400 associados
Tendência de crescimento

Novas oportunidades de participação aos associados

- Mais de 86.000 profissionais associados em mais de 160 países
- ISACA , desde 1969 – mais de 40 Anos
- Líder global em conhecimento, certificações, network profissional, pesquisa e educação em:
  - ✓ Auditoria, Segurança e Controle
  - ✓ Governança em TI
  - ✓ Riscos e Compliance em TI
- Certificação CISA – mais de 30 anos
  - 73.000 profissionais CISA
- CISA - Prêmio SC magazine em 2009, como melhor programa de Certificação profissional

ISACA®
Confiança e Valor em Sistemas de Informação
São Paulo Chapter

Governança em TI e os objetivos estratégicos da organização

PROGRAMA

1. Conceitos de Governança de TI

   - O Modelo CobiT e frameworks relacionados

2. Importância do valor dos Investimentos em TI
   - Governança de TI alinhada aos objetivos de negócio

3. Competências requeridas dos Gestores em Governança
   - Governança em TI , Auditoria, Gestão de Segurança da Informação, Gestão de Riscos e Controles
   - Certificações profissionais

ISACA®
Confiança e Valor em Sistemas de Informação
São Paulo Chapter

O que é Governança de TI

Uma definição com base nas referências de melhores práticas

O ITGI (IT Governance Institute) define Governança em TI como:

"A responsabilidade dos executivos e do corpo de administração, que consiste em liderança, estruturas organizacionais e processos que asseguram que a TI corporativa sustenta e expande as estratégias e objetivos da organização."

ISACA®
Confiança e Valor em Sistemas de Informação
São Paulo Chapter

O que é Governança de TI

Uma definição com base em melhores práticas

- Esta definição de Governanca de TI trata de forma mais abrangente um conceito que tradicionalmente tinha um foco mais estreito somente nos domínios de TI – os serviços de TI, a infraestrutura de suporte e as organizações que fornecem aplicações, conectividade e informação.

- A definição do ITGI posiciona a governança de TI nao como uma disciplina isolada, mas como parte integrante da governança corporativa.

- A necessidade por governança no nível corporativo tem sido orientada principalmente pela demanda por transparência através dos riscos organizacionais e proteção do valor aos acionistas. Os grandes custos, riscos e oportunidades associados a TI exigem um foco da Governança dedicado à TI, porém integrado ao negócio.

ISACA®
Confiança e Valor em Sistemas de Informação
São Paulo Chapter

O que a Governança de TI deve prover ?

- Governança em TI essencialmente tem como preocupação dois principais resultados:

- A geração de valor para o negócio e mitigação dos riscos de TI

  – Ambos objetivos são promovidos pelo alinhamento estratégico de TI ao negócio e a disponibilidade dos recursos adequados.

  – A administração necessita para isso medir o desempenho dos processos e monitorar seu progresso em direção aos objetivos desejados

ISACA®
Confiança e Valor em Sistemas de Informação
São Paulo Chapter

O que a Governança de TI deve prover ?

Dentro desse contexto, a Governança de TI concentra seu foco em cinco áreas principais:

1. **Alinhamento estratégico**
2. **Geração de Valor *(value delivery)***
3. **Gestão do Risco *(risk management)***
4. **Gestão de Recursos**
5. **Mensuração de desempenho**

ISACA®
Confiança e Valor em Sistemas de Informação
São Paulo Chapter

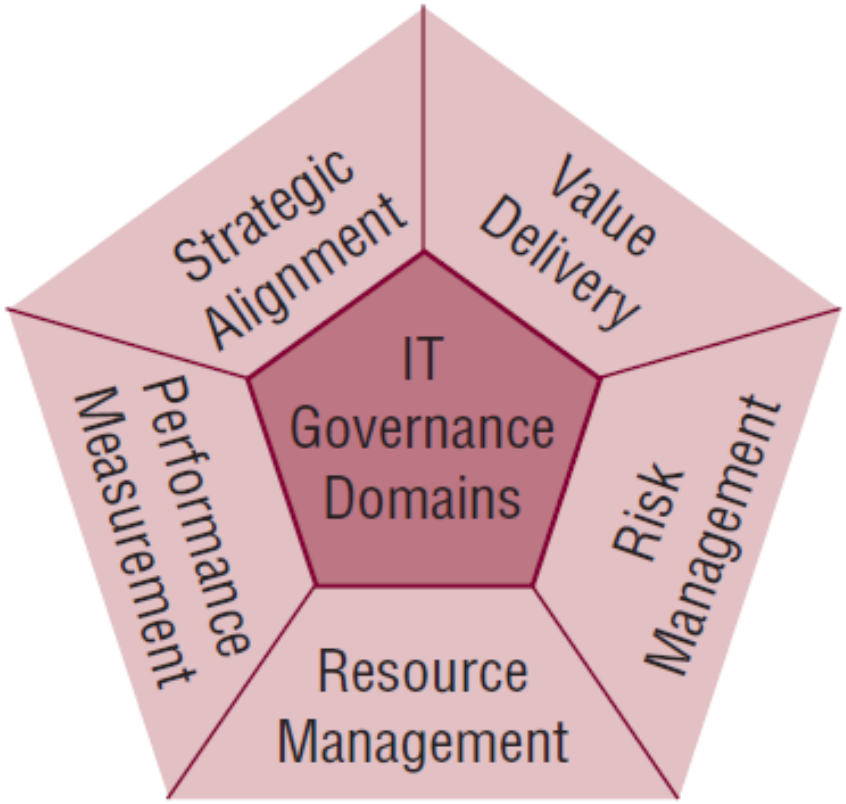
Por que geração de valor é relevante para a Governança de TI ?

- O ITGI destaca a geração de valor como um dos cinco domínios essenciais da Governança em TI, junto com alinhamento estratégico, métricas de desempenho, gerenciamento de recursos e gerenciamento de riscos
- Sem o sucesso nos outros quatro domínios, obter valor seria uma tarefa mais difícil
- A figura seguinte mostra estes domínios

ISACA®
Confiança e Valor em Sistemas de Informação
São Paulo Chapter

Domínios da Governança de TI

Figure 1—Five Domains of IT Governance



Principais considerações

- Todo investimento, seja relacionado a TI ou não, somente deve ser aceito a partir de um completo entendimento dos custos esperados e retorno antecipado. Expectativas de retorno devem estar relacionadas ao risco, por exemplo, dada uma alta probabilidade de falha, projetos de alto risco devem ter sempre uma alta taxa antecipada de retorno.

- Garantir que os projetos certos sejam aprovados em primeiro lugar, implica em uma previsão correta dos custos totais do projeto ao longo de seu tempo de vida, e previsões mais sólidas do potencial de retorno, incluindo a quantificação dos benefícios diretos e indiretos.

- Estabelecer mecanismos de monitoramento que determine o real valor obtido e permitir a contabilização, para garantir que o processo seja eficiente e faça parte da cultura da organização .

Key Players in IT Governance

Principais papéis e responsabilidades
em IT Governance

- **The Board of Directors**
- **Executive Management**
- **The Chief Information Officer**
- **Business Unit Executives**

ISACA®
Confiança e Valor em Sistemas de Informação
São Paulo Chapter

Key Players in IT Governance

Principais papéis e responsabilidades em IT Governance

- **The Board of Directors**
- A alta administração – o nível mais estratégico da organização, o corpo de diretores tem uma responsabilidade geral pela governança corporativa (*enterprise governance*)

- Como definido nos *Princípios de Governança Corporativa,* publicado pela OECD (Organisation for Economic Co-operation and Development), em 1998, a alta administração ou *board of directors* deve:
  - Garantir que exista um modelo consistente para fornecer uma orientação estratégica à organização
  - Monitorar os demais níveis da administração
  - Supervisionar a integridade dos sistemas e informações da companhia

Key Players in IT Governance

- **The Board of Directors**

O *board* deve ter claras suas próprias responsabilidades de administração e manter um sistema para alocar as responsabilidades, para garantir que:

• A TI gere valor para o negócio em linha com seus objsetivos estratégicos

• Exista processos apropriados e eficientes para monitorar o risco, e que o sistema de controles internos seja eficaz em reduzir esses riscos a um nível aceitável

• Ativos de informação sejam protegidos, garantida sua integridade, e utilizados de forma eficiente e eficaz para o crescimento do negócio e aumento do valor ao acionista.

Key Players in IT Governance

- **The Board of Directors**

  Interação e comunicação entre os diversos níveis da organização

- Para atingir um nível efetivo de Governança em TI, diretores, gerentes e pessoal em todos os níveis da organização devem colaborar na aplicação dos mesmos princípios, desde a definição de objetivos até o fornecimento de medidades de avaliação de performance

- É importante garantir que princípios consistentes de governança sejam aplicados, comunicados, compreendidos, aceitos e seguidos em toda a organização

Key Players in IT Governance

- **Executive Management**
- As gerências executivas, ou diretorias executivas, têm responsabilidades mais diretas sobre os processos que fornecem suporte à governança e melhores práticas em toda a organização e na comunicação de sua importância a todos os colaboradores, incluindo funções terceirizadas

- A gerência executiva é responsável também por reportar à Diretoria sobre a performance de TI e exerce um papel central em garantir que os objetivos de governança em TI sejam alcançados

Key Players in IT Governance

- **Chief Information Officer**
- O CIO, ou Diretor de TI, devem ter um entendimento rápido das oportunidades e riscos que a TI oferece, em apoio aos objetivos e iniciativas da organização, e devem agir como uma ponte entre a TI e as áreas de negócios.
- O CIO deve também garantir uma entrega segura e confiável dos serviços de TI.
- Este papel requer um conhecimento especializado, e um particular conjunto de competências ou habilidades.
- Por estar posicionado de forma central na organização, o CIO deve ter uma visão geral das estratégias de negócios, os direcionadores do negócio e os processos que agregam valor à organização .

Key Players in IT Governance

- **The Chief Information Officer (cont)**

- O CIO deve entender como a tecnologia contribui para o valor do negócio com mudanças através de inovação e entrega de serviços que suportam os processos críticos de negócio. Deve compreender como administrar e mitigar os riscos associados

- O CIO deve auxiliar os executivos de negócios a entender as mudanças nos processos e na organização que podem ser necessárias para que o objetivo de valor seja realizado.

- É importante manter uma colaboração bem próxima com as áreas de negócios. Uma cultura de confiança e mútuo respeito entre TI e negócios é essencial.

Key Players in IT Governance

- **Business Unit Executives**
- Os Gerentes ou Executivos das Unidades de Negócios exercem também um papel importante, pois são responsáveis pelas responsabilidades diárias da organização, dentro dos processos de governança

- Os executivos de negócios devem assumir a responsabilidade por investimentos que afetam suas funções , e fornecer um retorno crítico aos *stakeholders*.

- Devem garantir que suas operações estejam alinhadas à estratégia geral da organização, e as estratégias de TI e de serviços operacionais que a suportam

Key Players in IT Governance

ISACA
Confiança e Valor em Sistemas de Informação
São Paulo Chapter

Definição dos Requisito do Cargo de Gestão de Segurança da Informação: Orientação para Executivos e Gerentes

CISM
CERTIFIED INFORMATION SECURITY MANAGER®

Definição do Papel do Gestor de Segurança da Informação

ISACA
Confiança e Valor em Sistemas de Informação
São Paulo Chapter

Muitas empresas estão chegando à conclusão de que a segurança da informação é um aspecto de negócios que afeta sua situação financeira geral.

CISM
CERTIFIED INFORMATION SECURITY MANAGER®

Definição do Papel do Gestor de Segurança da Informação

ISACA
Confiança e Valor em Sistemas de Informação
São Paulo Chapter

Relatório elaborado com base em uma pesquisa conduzida pela ISACA mostra as definições do Papel do Gestor de Segurança da Informação e as competências requeridas.

CISM
CERTIFIED INFORMATION SECURITY MANAGER®

ISACA frameworks

Modelos para Governança de TI

Estudos de Caso

How Organizations Around the World
Are Customizing COBIT to Their Benefit

Educação
Curtin University of Technology, Western Australia
July 2002

Energia
Adnoc Distributions
December 2008

Bancos e Instituições Financeiras
Central Bank of the Republic of Armenia
February 2009

Indústrias, Serviços e diversos setores

Governo
Government of Dubai
April 2009

No Brasil – Governo, Bancos e Grandes instituições

- TCU, supervisão da Administração pública federal
- Bacen - Auditoria Interna

Definição do Papel do Gestor de Segurança da Informação

ISACA
Confiança e Valor em Sistemas de Informação
São Paulo Chapter

Relatório elaborado com base em uma pesquisa conduzida pela ISACA mostra as definições do Papel do Gestor de Segurança da Informação e as competências requeridas.

CISM
CERTIFIED INFORMATION SECURITY MANAGER®

Figura 2—Modelo típico de progresso e gestão de segurança da informação

Diretoria Segurança da Informação/Comitê de Garantia

Equipe multidisciplinar em nível de diretoria

Nível	Gestão		Tecnologia	Arquitetura	Garantia	Jurídico/ Gestão de Riscos/ Privacidade
Executivo sênior (Nível de Diretoria)	**CIO COO**		**CTO CISO CArO**		**CAO**	**GC CRO CPO**
Gerente/ diretor	Operações consultoria	Desenvolvimento/segurança de sistemas e informações de infraestrutura			Auditoria interna	Risco à informação/ consultoria de privacidade
Especialista	Consultor principal de TI	Profissional de sistemas sênior de TI	Engenheiro de desenvolvimento sênior de TI	Arquiteto sênior de TI	Auditor sênior de segurança da informação	Consultor principal de TI
Especialista, gerente	Gerente de produtos/programas/projetos, líder de equipe, gerente de vendas de conta					
Especialista, técnico	Consultor de segurança, analista de negócios	Gerente de produtos de segurança	Projetista de segurança	Profissional de sistemas de segurança	Auditor de segurança	Consultor de risco de informação
Iniciante	Analista		Desenvolvedor	Projetista de segurança estagiário	Estagiário de sistemas de segurança	Estagiário de auditoria de segurança

Níveis de Carreira

O progresso na carreira até o nível de Diretoria pode ser vertical, horizontal e/ou diagonal.

Fonte: Adaptado de Lynas, David; John Sherwood; "Professionalism in Information Security: A Framework for Competency Development," 12ª Conferência Anual da COSAC, Reino Unido, 2005

Legendas do Nível de Diretoria:

CIO = Diretor de Informática (Chief Information Officer)
COO = Diretor de Operações (Chief Operating Officer)
CTO = Diretor de Tecnologia (Chief Technology Officer)
CISO = Diretor de Segurança da Informação (Chief Information Security Officer)
CARO = Diretor de Arquitetura (Chief Architecture Officer)
CAO = Diretor de Garantia (Chief Assurance Officer)
GC = Diretor Jurídico (General Counsel)
CRO = Diretor de Risco (Chief Risk Officer)
CPO = Diretor de Privacidade (Chief Privacy Officer)

Descrição do cargo do Gestor de Segurança da Informação

ISACA
Confiança e Valor em Sistemas de Informação
São Paulo Chapter

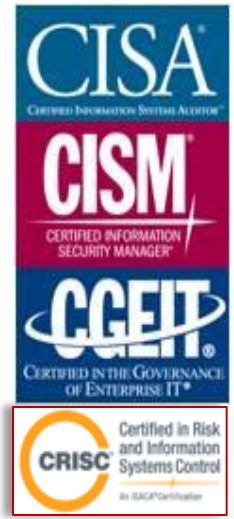
Qualidades e áreas de conhecimento requeridas:

- Habilidades em negócios
- Habilidades gerenciais
- Conhecimento mais profundo de exigências legais/de conformidade
- Conhecimento da lei Sarbanes-Oxley
- Habilidades em avaliação de riscos/gestão de riscos
- Perícia forense
- Segurança, incluindo gestão de segurança da informação, segurança patrimonial e segurança de rede

CISM
CERTIFIED INFORMATION SECURITY MANAGER®

ISACA®
Confiança e Valor em Sistemas de Informação
São Paulo Chapter

A Importância das Certificações
CISA - CISM - CGEIT



Certificações Profissionais
mundialmente reconhecidas

ISACA®
Confiança e Valor em Sistemas de Informação

- CISA® mais de 70.000 em mais de 160 países
- CISM® mais de 12.000 em 80 países

Reconhecimento Internacional

ANSI Accreditation

- ANSI (The American National Standards Institute) em 2008 reconheceu os programas de certificação CISA e CISM de acordo com a ISO/IEC 17024
  - Reconhecimento internacional
  - Mobilidade de profissionais entre diferentes países e diferentes áreas
  - Maior Credibilidade nos programas de certificação e nos profissionais certificados

ISACA®
Confiança e Valor em Sistemas de Informação
São Paulo Chapter

CISA no Mercado de Trabalho

Perfil dos profissionais com certificação CISA no mundo

- Aprox. 2.400 - CEO, CFO ou em posições de diretoria em grandes organizações
- Mais de 2.000 - chief audit executives (CAEs), audit partners ou audit heads
- Aprox. 6.000 - CIO, CISO, security directors, security managers, consultores
- Mais de 10.500 - audit directors, managers ou consultores
- Mais de 15.400 - consultoria ou gerência de IT ou compliance
- Mais de 14.400 - auditores (IS/IT e auditores operacionais)

Certified Information Systems Auditor

Over 70,000 professionals in more than 160 countries have earned the CISA certification since 1978. CISA is known world-wide as the recognized achievement for those who control, monitor and assess an organization's information technology and business systems.

CISA
Certified Information Systems Auditor™

As an IS auditor, being a CISA means you have proven ability and experience.

Earn the designation that employers and clients are looking for. There is a growing demand for professionals possessing IS audit, control and security skills and CISA has become a preferred certification by individuals and enterprises around the world. Many enterprises recognize ISACA's CISA credential as the standard for information systems auditors. Its demand continues to grow as organizations increasingly expect their IS auditors to hold the certification.

Notice: *A CISA job practice analysis is underway to reflect the vital and evolving responsibilities of IT auditors and stay current with the market. Results of this analysis will be incorporated into the June 2011 exam.*
www.isaca.org/cisajpa

"The world of technology is ever-changing, and I need to know that my employees are prepared to face such challenges. The CISA designation is an excellent indicator of proficiency in technology controls."

–Marios Damianides, CISA, CISM, Partner, Ernst and Young LLP, USA

SC Magazine AWARDS 2009 WINNER Honored in the U.S.

A recent independent study conducted by Foote Partners rates ISACA's CISA designation as the third highest paying in the IT profession. Additionally, CISA is ranked as one of the top five most sought after certifications by IT professionals in an annual survey by Information Security Media Group.

The chart below describes the CISA job practice areas and approximate percentage of test questions allocated to each area.

For more information, visit *www.isaca.org/cisa.*

Requisitos para a Certificação CISA

- Aprovação no Exame CISA
  - 6 áreas de dominio (Job Practice Areas)
  - Prova: 200 questões em 4 horas – em Inglês ou Espanhol

- Comprovar 5 anos de experiência em Auditoria de TI, controle ou segurança da informação
  - Substituições aceitas, ex. Curso de Graduação ou Mestrado, corresponde a um ano (detalhes no manual do candidato)

- Submeter solicitação para aprovação (CISA Application)

- Aderir ao Código de Ética Profissional ISACA e padrões de Auditoria (IS Auditing Standards)

- CPE(continuing professional education policy)
  - Reportar mínimo 20 Horas anuais de educação continuada
  - Minimo 120 Horas em 3 anos (ou seja, em média 40 horas/ano)
  - Manter documentação para eventual auditoria (seleção anual)

O Exame CISA

CISA Job Practice Areas

- IS Audit Process – 10%
- IT Governance – 15%
- Systems and Infrastructure Lifecycle – 16%
- IT Service Delivery and Support – 14%
- Protection of Information Assets – 31%
- Business Continuity and Disaster Recovery – 14%

ISACA®
Confiança e Valor em Sistemas de Informação
São Paulo Chapter

Certified Information Security Manager

CISM certification is for individuals who design, build and manage enterprise information security programs. Over 12,000 individuals from more than 80 countries have already earned the CISM designation.

Stand out from other information security professionals and increase your earning potential.

The demand for skilled information security management professionals is on the rise and earning a CISM will give you a competitive advantage.

According to an October 2009 report by the independent Foote Partners, the CISM designation was **ranked first** among IT security certifications that earn the highest pay premiums. CISM ranked as the second most sought after certification by IT professionals in a survey by Information Security Media Group.

The CISM certification is the leading credential for information security managers. CISMs differentiate themselves from traditional information security certification holders.

"The CISM designation signifies integrity, responsibility, knowledge and experience...all of which I expect from a prospective employee."

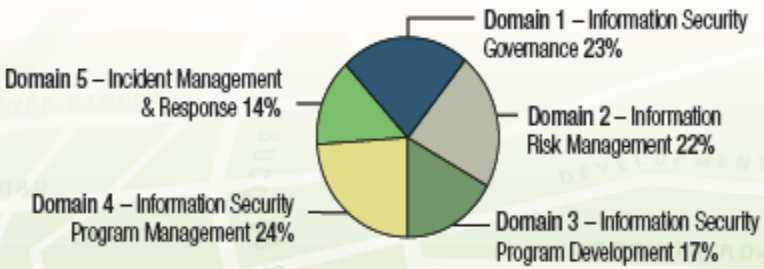
– William C. Boni, CISM, Corporate Vice President, Motorola, USA

Being a CISM:

- Demonstrates your understanding of the relationship between an information security program and broader business goals and objectives,
- Distinguishes you as having not only information security expertise, but also knowledge and experience in the development and management of an information security program and
- Puts you in an elite peer network.

The chart below describes the CISM job practice areas and approximate percentage of test questions allocated to each area.

CISM Job Practice Areas



For more information, visit *www.isaca.org/cism.*

CISM Target Market

A quem se destina a Certificação CISM

Individuals who design, implement and manage an enterprise's information security program.

- Security managers
- Security directors
- Security officers
- Security consultants
- Security staff

Reconhecimentos Recentes da Certificação CISM

- Janeiro 2010 – Estudo pela Mile High Research, colocou as certificacoes CISA e CISM entre as 10 mais requisitadas certificacoes para novas oportunidades de trabalho

- CISM – corresponde a parte de experiência requerida pelo DRII (Disaster Recovery Institute International') para a certificação CBCA (Certified Business Continuity Auditor) certification.

- Securities Exchange Board of India exige uma auditoria de sistemas de todos os fundos mutuos, conduzida por um profissional certificado CISA/CISM ou equivalente

Reconhecimentos Recentes da Certificação CISM

- CIO Magazine, SC Magazine and Foote Partners research continually cite CISM as a credential that earns top pay when compared to other credentials.
  - In April 2009, the Foote Partners "Salary Survey" ranked the CISM certification as the highest paying IT Security certification. CISM was also found to be the only security certification to gain value within the past twelve months.
- Certification Magazine's 2008 and 2009 salary survey ranked the CISM certification as the third highest paying certification.
- CISM has also been recognized in the following publications as a unique security management credential:
  - Information Security Magazine - eWeek
  - CSO Magazine Online - Security Magazine (Brazil)
  - Computerworld Today (Australia) - Cramsession.com

Certified in the Governance of Enterprise IT

CGEIT recognizes a wide range of professionals for their knowledge and application of enterprise IT governance principles and practices.

CGEIT
CERTIFIED IN THE GOVERNANCE OF ENTERPRISE IT®

You have the knowledge and expertise in the governance of enterprise IT. Enhance your credibility and influence with CGEIT.

Boards and executive management expect IT to deliver business value. They want fast, secured, high-quality solutions and services; a reasonable return on investment; and a move from efficiency and productivity gains toward value creation and business effectiveness. IT governance is a key component of enterprise governance and success.

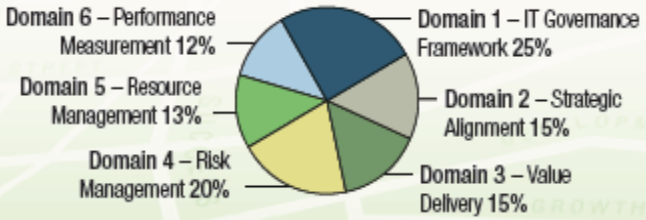
But you already know this. You have the knowledge and expertise to add value to your enterprise. Earn your CGEIT and earn influence at the executive level.

"The CGEIT qualification provides me with the credibility to discuss critical issues like governance and strategic alignment based on my recognized professional knowledge, skills and business experience."

– Vernon R. Poole, CGEIT, CISM, Head of Business Consultancy, Sapphire Technologies Ltd., UK

The chart below describes the CGEIT job practice areas and approximate percentage of test questions allocated to each area.

CGEIT Job Practice Areas



For more information, visit *www.isaca.org/cgeit*.

O Exame CGEIT

CGEIT Job Practice Areas

1. IT Governance Framework (25%)
2. Strategic Alignment (15%)
3. Value Delivery (15%)
4. Risk Management (20%)
5. Resource Management (13%)
6. Performance Measurement (12%)

CRISC™ - Certified in Risk and Information Systems Control™

Nova Certificação – Exame em 2011

- Profissionais que identificam e gerenciam riscos através do desenvolvimento, implementação e manutenção de controles em sistemas de informação e

- Ajudam as organizações a atingir seus objetivos de negócio, eficiência e eficacia das operações, confiança nos relatórios financeiros e conformidade com regulamentações e requisitos legais

Exame para Certificação CRISC – em 2011

Programa grandfathering – aberto em Abril 2010 – mais informações em http://www.isaca.org/crisc

ISACA® Confiança e Valor em Sistemas de Informação São Paulo Chapter

CRISC™
Certified in Risk and Information Systems Control™

Nova Certificação – Exame em 2011

- Áreas de domínio da Certificação CRISC
  - Risk identification, assessment and evaluation (Identificacao, analise e avaliadao de riscos)
  - Risk response (Resposta a riscos)
  - Risk monitoring (Monitoramento dos riscos)
  - IS control design and implementation (Projeto e Implementação de Controles em Sistemas de Informação)
  - IS control monitoring and maintenance (Manutenção e Monitoramento dos Controles)

ISACA® Confiança e Valor em Sistemas de Informação São Paulo Chapter

Exames CISA, CISM and CGEIT

Duas edições do Exame: ***Junho e Dezembro***

Próxima data: 11 Dezembro 2010

Mais informações em:

http://www.isaca.org/cisa

http://www.isaca.org/cism

http://www.isaca.org/cgeit

ISACA®
Confiança e Valor em Sistemas de Informação
São Paulo Chapter

Contato com ISACA São Paulo – www.isaca.org.br

Email: info@isaca.org.br

Diretor de Associados: fabio.penna@isaca.org.br