Curso GRC - Governança, Gestão de Riscos e Conformidade

O acrônimo GRC tem origem na união dos termos governança, riscos e compliance, ou em inglês, governance, risk and compliance. Uma tendência recente, de integração das áreas de conhecimento de Gestão de Riscos, Governança Corporativa e práticas de auditoria e controle que visa garantir a conformidade com leis, regulamentos, imposições de padrões consolidando-os dentro de um único modelo, integrado inteligentemente e tendo como um dos seus objetivos a unificação dos interesses comuns e conciliação de interesses opostos de cada uma destas funções.

Para que se entenda o significado do GRC, é necessário que o mesmo seja compreendido dentro de um contexto global, evitando analisar cada uma das palavras separadamente, todavia antes é bom conhecer o conceito de cada uma delas antes:

Governança: Este enfoque está relacionado à forma como as decisões são tomadas. A governança refere-se ao desenvolvimento de políticas e procedimentos, à definição de responsabilidades e também à criação de diretrizes para orientar as pessoas e os processos da organização. A finalidade é garantir que ninguém se perca, ou seja, que todos atuem em prol de um objetivo em comum, e que haja transparência e igualdade em todas as áreas envolvidas.

De acordo com o ITGI (IT Governance Institute), Governança é o conjunto de responsabilidades e práticas exercidas pelos executivos e pela alta direção da empresa com o objetivo de fornecer orientação estratégica, assegurando que os objetivos da companhia sejam alcançados e que os recursos sejam utilizados de forma responsável.

Risco: tem como foco a análise de forma quantitativa e qualitativa do que pode ocorrer no ambiente que interfere diretamente na execução dos processos e sua relevância de acordo com os objetivos que influenciam a governança, quais são os possíveis imprevistos que podem acontecer no caminho. Por meio da gestão de risco, a empresa pode antecipar cenários caso ocorram imprevistos, analisar seus impactos e estudar o que fazer para evitá-los ou contorná-los. Os riscos podem ser estratégicos ou operacionais e podem estar associados a fatores externos, como a economia ou a falhas internas, como erros no processo.

Conformidade: Consiste na observância do comportamento dos processos tendo em vista garantir que a empresa esteja de acordo com as normas, legislações e boas práticas de seu segmento. Por meio da gestão de conformidade, a organização tem uma maior garantia de qualidade e conformidade, o que implica que não perderá tempo nem dinheiro por não seguir determinada regra. A gestão conformidade funciona por meio do monitoramento constante para garantir a adequação da empresa ao ambiente em que está inserida.

“O conceito de GRC diz respeito à combinação dessas áreas – Governança, Risco e Conformidade – para garantir que a empresa atue de forma eficiente e transparente, integrando as atividades, evitando erros e retrabalhos e agindo em conformidade com as diretrizes e leis relacionadas ao seu negócio.”

Com a pressão cada vez maior dos interesses dos acionistas sobre as organizações, normatizações cada vez mais detalhadas a respeito da maneira com que os diversos elementos da organização devem se comportar, e o aumento da importância de se ter cada vez mais controle e transparência sobre incertezas nos resultados das organizações às diversas partes interessadas (acionistas majoritários e minoritários, governo, comunidade, etc...) as empresas passaram a adotar, inicialmente, de maneira isolada e espalhada pela organização práticas distintas de governança, gestão de riscos e controle, que muitas vezes se mostravam redundantes aos de outras áreas, ou até mesmo, traziam conflitos de interesse, no conjunto, perda de produtividade, gastos desnecessários e ambientes conflituosos, caracterizados por disputas internas constantes originadas da redundância ou dubiedade das funções, busca por culpados ao invés de soluções e interações políticas difíceis dentro das organizações. As decisões se tornaram difíceis com tendência de perda de agilidade, tão necessária na gestão moderna dasempresas.

Fontes: https://www.ibm.com & https://pt.wikipedia.org/wiki/GRC

Veja também:

Curso Introdução ao Gerenciamento de Riscos em TI

Curso Capacitação em Gerenciamento de Riscos de TI

Para conhecer o nosso conteúdo sobre Governança de TI acesse o seguinte link:

http://www.grupotreinar.com.br/treinamentos.aspx?a=1192

Para saber um pouco mais sobre Governança de TI acesse o nosso Blog através do seguinte link:

http://www.grupotreinar.com.br/blog.aspx?filterby=Governan%C3%A7a%20de%20TI

Objetivos

Gerais:

O Curso aborda as disciplinas relacionadas à continuidade, com enfoque a partir da segurança da informação, em diversos cenários, sua evolução como instrumento estratégico e a aplicabilidade como prática de adequação da resiliência organizacional.

Específicos:

- Reconhecer a importância do gerenciamento de riscos da segurança da informação para a preservação do valor para os processos de negócio da organização;
- Entender a contribuição dos modelos de melhores práticas para a implantação dos processos de gerenciamento de riscos de governança da informação;
- Instanciar os modelos de melhores práticas para a realidade da empresa.

Público alvo

Executivos, Gestores de Negócio, Executivos de TI, Analistas e Partes Interessadas envolvidas na Governança da Segurança da Informação.

Benefícios

As Organizações vêm desenvolvendo seu Programa de Governança de Segurança da Informação sendo que a seguir destacamos os principais benefícios trazidos por esta capacitação neste sentido:

- A adoção das boas práticas apregoadas irá contribuir para maior integração entre as áreas, melhorando a comunicação, o trabalho em equipe e a gestão da informação;
- Maior segurança e eficiência dos processos por conta da melhoria na orientação dos profissionais;
- Maior transparência entre as áreas envolvidas na operação, dando mais credibilidade e segurança aos processos;
- Menos custos por conta de trabalhos redundantes nos controles e processos internos da empresa;
- Estudando e avaliando profundamente os riscos inerentes à organização, há uma maior confiança e estabilidade nas ações estratégicas e portanto na governabilidade;
- Maior resistência às crises de mercado, por conta da estabilidade e eficiência gerada pela adoção efetiva dos princípios da Gestão do Risco e Continuidade de Negócios;
- Por fim, a garantia do atendimento às normas corporativas e a conformidade com a legislação proporciona mais credibilidade e respeito à organização como um todo.

Resultados esperados:

Os resultados esperados com a capacitação são:

- Implantação de um modelo de processo de Governança da Segurança da Informação;
- Manutenção do processo de gerenciamento de riscos e continuidade de negócios;
- Melhoria contínua do processo de gerenciamento de riscos e continuidade de negócios.

Competências a serem desenvolvidas:

A competência que os participantes deverão ter ao final do processo de capacitação é:

- Ter a capacidade de projetar um processo de governança da informação considerando as melhores práticas.

Habilidades a serem desenvolvidas:

- Analisar e interpretar modelos de melhores práticas quanto a aspectos ligados ‘a governança da informação;
- Instanciar e desenvolver processo de governança da informação.

Atitudes a serem desenvolvidas:

- Reconhecer a importância dos riscos e da governança da segurança da informação para o negócio;
- Aplicar o processo em projetos, serviços e inovações;
- Implantar requisitos de avaliação de riscos em projetos, processos, serviços e inovações.

Metodologia de ensino

Ação educacional com forte conteúdo prático com experimentação das técnicas em exercícios e em casos reais.

Níveis de Avaliação

Reação: nível de satisfação dos participantes em relação à ação educacional aplicada logo após o seu término.

Formas de Avaliação da Aprendizagem

Avaliação do tipo Formativa com função de orientar, corrigir, informar sobre a aprendizagem do participante da ação através de feedbacks.

Pré requisitos

Conhecimentos da Organização de TI, estrutura e processos de gerenciamento.

Material Didático

- Apostila contendo os slides;
- Estudos de caso.

Conteúdo Programático

MÓDULO 1 – INTRODUÇÃO AO GRC

Este módulo demostra como incidentes ligados a falhas nas áreas de Governança, Gestão o de Riscos e Conformidade podem comprometer o valor de mercado e o lucro das empresas, além de apresentar alguns conceitos importantes para a compreensão da integração de GRC.

- A necessidade do GRC
- Cases de empresas afetadas por problemas de GRC
- Definições
- Stakeholder; Sociedades Anônimas; Shareholders; Bolsa de Valores

MÓDULO 2 – A HISTÓRIA DO GRC

Este módulo explica, através de eventos históricos, como as pessoas se comportavam em relação ao risco e como a matemática e estatística criaram uma nova visão sobre a causa dos eventos. Paralelamente, a história da Governança Corporativa e contada em uma linha do tempo que começa com a primeira sociedade de ações do mundo, em 1250, e avança até a crise da Enron, que culminou na Lei Sarbanes-Oxley. A linha histórica da conformidade aparece como uma resposta a eventos como a quebra da bolsa de NY em 1929 e a quebra da Enron. Por esse motivo, esses eventos são apontados como marcos de governança e conformidade.

Gestão de Risco s

- A Vontade dos Deuses dita as regras,
- Algarismos Indo-Arábicos
- 1654 – Luca Paccioli e o desafio da renascença
- 1703 a 1760 - Jabob Bernoulli e a lei dos grandes nu meros
- 1875 – Regressa o a me dia
- 1952 – Ovos em cestas separadas
- 1992 – O Cubo COSO
- 2004 – Coso II

Governança

- 1250 – Societe des Moulins bu Bazacle
- 1600 – Companhia das Índias orientais
- 1602 – Amsterdam Stock Exchange
- 1915 a 1929 – A Economia Liberal
- 1929 – Euforia na Bolsa de NY
- 1929 – O Crash da Bolsa de NY
- 1930 – A Grande Depressa o
- 1961 – A Criação da OECD

- 1980 – O Ativismo de Robert Monks
- 1992 – O Relatório Cadbury
- 1999 – Os Princípios de Governança da OECD
- 2000 - Enron
- Compliance
- 1934 – New Deal e a SEC
- 1969 – A Criação da ISACA
- 1976 – A CVM no Brasil
- 1973 – A Criação da IASC
- 1977 – A FCPA
- 1985 – COSO
- 1992 – A Convenção anti-suborno da OECD
- 1996 – HIPAA
- 1996 – Cobit 1.0
- 1998 – The Anti-Bribery Act
- 1998 – O Acordo de Basiléia
- 1999 – Gramm-Leach-Bliley Act
- 2002 – A Lei Sarbanes-Oxley
- 2004 – Basiléia II
- 2004 – IFRS
- 2005 – O Roubo de dados de Cartões de Crédito na TJX
- 2006 – O PCI Council
- 2010 – Basiléia III

MÓDULO 3 – GOVERNANÇA

Este módulo apresenta os conceitos de governança (corporativa e de TI), visando criar um melhor entendimento das necessidades das empresas, facilitando o entendimento de quais devem ser os objetivos de Tecnologia da Informação e Segurança da Informação para que estas áreas estejam alinhadas aos objetivos da alta gestão.

Governança Corporativa - Definições do IBGC (Instituto Brasileiro de Governança Corporativa), níveis de governança e o novo mercado da Bovespa, transparência, equidade, prestação de Contas, responsabilidade corporativa, conselho de administração, relações com os investidores, gesta o de riscos, relatório anual, código de conduta.

Governança de TI - Estrutura de governança de TI, estudo da norma ABNT ISO/IEC 38500.

MÓDULO 4 - GESTÃO DE RISCOS

Este módulo demonstra os conceitos de risco positivo e negativo, que juntos com os conceitos de apetite e tolerância a riscos demonstram a necessidade do risco para a o crescimento e sucesso das organizações. O módulo aborda também todos os conceitos e as principais normas e frameworks para a avaliação e tratamento de riscos.

Definições de risco - Riscos positivos e negativos, fontes de risco, nível de risco e probabilidade, consequência, análise quantitativa, qualitativa e semi-quantitativa, matriz de riscos, percepção de riscos, responsabilidade pelo risco, apetite e tolerância a riscos

Análise de Riscos - Explica os processos de análise (quantitativa e qualitativa) e avaliação de riscos, a relação entre uma ameaça e um risco, assim como as estratégias para tratamento dos riscos e aceitação de riscos residuais.

Gestão de Riscos - Princípios e processo de Gestão de Riscos, estudo da norma ABNT ISO 31000, critérios de Risco (ALARP – As Low as Reasonable Practicable), processo de avaliação de riscos, tratamento de riscos, monitoração do risco, reporte de riscos, gestão de riscos através da ABNT ISO 27005, comparação do Coso ERM (Coso II) com a ISO 31000.

MÓDULO 5 - CONFORMIDADE

Este módulo apresenta os principais conceitos relacionados a conformidade, assim como as mais importantes regulamentações as quais as empresas nacionais estão sujeitas. Ao final dos estudos e apresentada a norma Australiana de Compliance e os principais pontos abordados por esta.

Conceitos e definições, sistema normativo (Leis e Regulamentações), tipos de conformidade, CVM, CVM 358/2002 – Fato Relevante, CVM 456/2007 – IFRS, decreto 11.638 – Contabilidade das Sociedades por Ações, Basiléia II e III, Banco Central, resolução 2554, resolução 3380, SUSEP 249/2004, culpa e dolo, responsabilidades dos Administradores, lei das S.A.'s, business judgement rule, conflito de Interesses, dever de qualificar-se e informar-se, dever de informar, dever de sigilo, insider trading, concorrência desleal, dever de vigiar, investigar e punir, código de ética, política de propriedade intelectual, política de segurança da informação, sustentabilidade, a norma AS 3806/2006, o papel do CCO/CECO.

MÓDULO 6 – IT GRC UTILIZANDO O COBIT

Este módulo complementa os três anteriores ao mostrar o Conjunto Cobit+Val IT+Risk IT, delimitando o seu relacionamento com as áreas de Governança, Gesta o de Riscos e Compliance. Em uma segunda etapa, apresentamos o Cobit 5, o framework de GRC da ISACA que integrou o Val IT e RisK IT ao CobiT e tem a proposta de ser um framework de GRC para qualquer área da organização.

Governança de TI segundo o Cobit - Áreas de foco na Governança de TI, produtos do CobiT, objetivos e Arquitetura de TI, ciclo de vida de TI, domínios do CobiT, objetivos de Controle, tabela RACI, modelo de maturidade, objetivos de negócio, objetivos de negócio transformados em objetivos de TI, objetivos de TI transformados em objetivos de processo.
VAL IT - Definição e Objetivos, os quatro "Estamos?", Val IT x CobiT, Domínios e Processos, quadro de atividades, entradas e saídas
Risk IT - Posicionando Cobit, ValIT e RiskIT, hierarquia dos riscos, resposta e priorização de riscos, governança de riscos, avaliação de riscos, articulação de riscos.
Cobit 5 - Princípios e aspectos gerais, arquitetura e objetivos em cascata, objetivos de governança, modelo de "Enablers" integrados, objetivos de governança, objetivos de TI,

governança e gestão, governança corporativa de TI, novo modelo de maturidade (ISO 15504), ciclo de implementação.

MÓDULO 7 – CONSIDERAÇÕES FINAIS

Neste módulo trazemos uma reflexão sobre os desafios para a implantação do GRC desde uma definição do termo e de sua real função até o perfil do profissional de GRC.
O que esperar do GRC, visa o do modelo de negócio (OCEG), colaboração, stakeholders internos do GRC, stakeholders externos do GRC, sistemas eficientes, eficazes e responsivos, implantação do GRC na organização, vencendo resistências, perfil do profissional de GRC.