AULA 05: Governança de TI: Noções de Cobit e Riscos em TI – Exercícios.

SUMÁRIO	PÁGINA

1.Exercícios.

Vamos ver como é cobrado em provas? Bem, primeiramente vou apenas listar os exercícios e depois na primeira página seguinte coloco os comentários e logo depois os gabaritos, não trapaceiem gente, não vale olhar o gabarito no final antes de tentarem resolver, isso é ruim inclusive para vocês.

Tentem resolver os exercícios; se não conseguirem, voltem na parte teórica, pois está tudo lá, se não verifiquem os comentários e discutam no grupo.

Cobit

AFC – CFU – Infraestrutura - 2008

1) 10- Para que as atividades de Tecnologia da Informação sejam efetivamente governadas, é importante considerar as atividades e riscos da área de TI a serem gerenciadas. As atividades são classificadas em domínios de responsabilidade. No COBIT, estes domínios são denominados

a) Planejar e Organizar; Adquirir e Implementar, Entregar e dar Suporte, Monitorar e Avaliar.

b) Planejar e Organizar; Adquirir e Executar, Entregar e dar Suporte, Monitorar e Medir.

c) Planejar e Organizar; Implementar, Entregar e dar Suporte, Medir e Avaliar.

d) Planejar e Organizar; Adquirir e Desenvolver, Entregar e dar Suporte, Monitorar e Melhorar.

e) Planejar e Organizar; Adquirir e Implementar, Entregar e dar Suporte, Medir e Melhorar.

AFC – CFU – Desenvolvimento - 2008

2) 1 - O COBIT - Control Objectives for Information and related Technology fornece boas práticas por meio de uma estrutura de domínio e processos e apresenta atividades de forma gerencial e lógica para a Governança de TI. O COBIT contém componentes inter-relacionados, provendo suporte para a governança, gerenciamento, controle e atendimento das necessidades de diferentes organizações. O componente Atividades-Chaves do COBIT (versão 4.1) está relacionado com

a) Indicadores de Performance.

b) Modelos de Maturidade.

c) Controle de Objetivos.

d) Responsabilidades e Contabilização.

e) Controle de Práticas.

AFC – STN – Desenvolvimento – 2008

3) 29- Analisem as seguintes afirmações relacionadas ao COBIT (Control Objectives for Information and related Technology):

I - Determina os objetivos de controle de gerenciamento a serem considerados.

II - Considera os requisitos de negócio.

III - Organiza as atividades de TI (Tecnologia da Informação) em um modelo de processos.

Indique a opção correta.

a) Apenas a afirmação I é correta.

b) Apenas a afirmação II é correta.

c) Apenas a afirmação III é correta.

d) Apenas as afirmações I e II são corretas.

e) As afirmações I, II e III são corretas.

ANA – Analista - DES e BD - 2009

4) 1 - O _____ é empregado na governança de recursos de Tecnologia da Informação (TI).

Assinale a opção que completa corretamente a frase acima.

a) OPM3

b) CMMI

c) GED

d) COBIT

e) Portal corporativo

CVM – Analista – TI – 2010

5) 38- Os níveis dos modelos de maturidade do COBIT são:

a) Insipiente (0). Inicial / Ad hoc (1). Repetitivo mas intuitivo (2). Programado (3). Gerenciado e qualitativo (4). Finalizado (5).

b) Inexistente (0). Programado (1). Repetitivo mas dedutivo (2). Definido (3). Gerenciado e mensurável (4). Repetitivo (5).

c) Inexistente (0). Em definição (1). Restritivo mas intuitivo (2). Otimizado (3). Gerenciado e mensurável (4). Disponibilizado (5).

d) A definir (0). Inicial / Ad hoc (1). Repetitivo e redundante (2). Definido (3). Orientado para mensuração (4). Maximizado (5).

e) Inexistente (0). Inicial / Ad hoc (1). Repetitivo mas intuitivo (2). Definido (3). Gerenciado e mensurável (4). Otimizado (5).

CVM – Analista – Sistemas – 2010

6) 56- Assinale a opção correta.

a) A estratégia de *outsourcing* decide **como gerenciar o desempenho dos equipamentos.**

b) O objetivo principal da Governança de TI é gerenciar *outsourcing*.

c) A estratégia de *outsourcing* decide **como gerenciar os negócios internos dos fornecedores ou prestadores de serviços.**

d) O objetivo principal da Governança de TI é escolher a melhor alternativa de programação.

e) O objetivo principal da Governança de TI é alinhar TI aos requisitos do negócio.

7) 58- O ciclo da Governança de TI engloba

a) Negócio Estratégico e *Compliance*. Decisão, Ação, Priorização e Alocação de Pessoas. Estrutura, Processos, Operações e Gestão. Planejamento do Desempenho.

b) Alinhamento Tático e Estratégico. Informação, Decisão e Ação. Estrutura, Procedimentos, Operações e Monitoramento. Medição do Desempenho.

c) Alinhamento Estratégico e *Compiling*. Decisão, Compromisso, Programação e Alocação de Recursos. Planos, Programas, Processos e Gestão. Medição da Aceitação.

d) Alinhamento Estratégico e *Compliance*. Decisão, Compromisso, Priorização e Alocação de Recursos. Estrutura, Processos, Operações e Gestão. Medição do Desempenho.

e) Estratégias Alinhadas e *Pipelining*. Decisão, Compromisso, Priorização e Busca de Resultados. Estrutura, Processos, Planilhas e Operação. Desempenho Organizacional.

SUSEP – Analista – TI – 2010

8) 6 - Em relação ao COBIT, é correto afirmar que o mesmo

a) estabelece posicionamentos com os registros do negócio.

b) identifica os principais recursos de WFD, nos quais deve haver menos requisitos.

c) organiza as atividades de TI em um modelo de processos genérico.

d) estabelece prioridades entre os responsáveis pelo negócio.

e) define as métricas sem controle que devem ser seqüenciadas no desenvolvimento.

9) 7 - Entre as aplicações do COBIT em uma organização, situam-se

a) auditoria de riscos operacionais de concorrentes e qualificação de armazenadores de TI.

b) implantação modular da Governança de TI e realização de *benchmarking*.

c) avaliação dos *topservers* de TI e desenvolvimento dos riscos situacionais de TI.

d) desmembramento de riscos e benefícios da TI e realização de *branch and bound*.

e) atualização de *casual failures* e implantação exógena da Governança de TI.

10) 8 - As áreas foco da Governança de TI na visão do COBIT são:

a) Alinhamento Estratégico, Agregação de Valor, Gerenciamento de Riscos, Gerenciamento de Recursos e Medições de Desempenho.

b) Alinhamento Estratégico, Medições de Perdas, Gerenciamento de Riscos, Gerenciamento de Requisitos e Condições de Mercado.

c) Planejamento Estratégico, Valores de Ativos, Gerenciamento de Pessoas, Agregação de Componentes e Medições de Custos.

d) Aquisições Estratégicas, Composição de Valor, Gerenciamento de Benefícios, Gerenciamento de Recursos e Modificações de Desempenho.

e) Alinhamento de Desempenho, Associação de Valores e Benefícios, Gerenciamento de Decisões, Gerenciamento de Perda de Recursos e Medições de Riscos.

11) 41- Um dos fatores motivadores da Governança de TI é

a) a dependência do negócio em relação à TI.

b) o ambiente de trabalho.

c) a integração organizacional.

d) a TI como provedora de serviços.

e) o valor da informação.

12) 42- A Governança de TI deve

a) garantir o posicionamento da TI como norteador das estratégias do negócio.

b) alinhar as estratégias da organização aos objetivos e à infraestrutura da TI no negócio.

c) garantir o alinhamento da TI ao negócio, tanto no que diz respeito às aplicações como à infraestrutura de serviços de TI.

d) garantir o planejamento da TI em conformidade com as diretrizes dos fornecedores relativas aos sistemas de informações.

e) garantir o alinhamento da TI ao negócio, tanto no que diz respeito aos provedores como à infraestrutura de serviços da concorrência.

Riscos

AFC – CFU – Infraestrutura - 2008

13) 42. Considerando uma adequada gestão de riscos para a segurança da informação, analise as afirmações a seguir e assinale a opção correta.

I. É recomendável estabelecer regras para o uso aceitável de ativos associados aos recursos de processamento da informação.

II. É recomendável efetuar, criticamente, a análise de riscos de segurança, uma vez que esta considera ameaças, vulnerabilidades e impactos em função dos negócios da organização.

III. É recomendável estabelecer responsabilidades e procedimentos de gestão para assegurar respostas rápidas e efetivas a incidentes de segurança.

a) Apenas I e II são verdadeiras.

b) Apenas II e III são verdadeiras.

c) Apenas I e III são verdadeiras.

d) I, II e III são verdadeiras.

e) I, II e III são falsas.

AFC – CFU – Desenvolvimento - 2008

14) 48. Gerenciamento de riscos significa identificar riscos e traçar planos para minimizar seus efeitos sobre o projeto. Assinale a opção que contenha a descrição de um exemplo de Risco de Negócios.

a) A tecnologia sobre a qual o sistema está sendo construído foi superada por nova tecnologia.

b) O tamanho do sistema foi subestimado.

c) As especificações de interface não estavam disponíveis dentro do prazo.

d) Haverá uma mudança no gerenciamento organizacional, com a definição de prioridades diferentes.

e) Haverá maior número de mudanças nos requisitos do que o previsto.

SEMUT – Prefeitura de Natal – ATM – Informática - 2008

15) 35. Analise as seguintes afirmações relacionadas à Segurança da Informação:

I. Uma Vulnerabilidade é um evento com conseqüências negativas resultante de um ataque bem-sucedido.

II. Uma Ameaça é uma expectativa de acontecimento acidental ou proposital, causada por um agente, que pode afetar um ambiente, sistema ou ativo de informação.

III. A Vulnerabilidade é uma fonte produtora de um evento que pode ter efeitos adversos sobre um ativo de informação.

IV. O Ataque é um evento decorrente da exploração de uma vulnerabilidade por uma ameaça.

Indique a opção que contenha todas as afirmações verdadeiras.

a) I e II

b) II e III

c) III e IV

d) I e III

e) II e IV

16) 39. A Gestão de Risco de uma organização é o conjunto de processos que permite identificar e implementar as medidas de proteção necessárias para diminuir os riscos a que estão sujeitos os seus ativos de informação. Com relação aos conceitos utilizados na Gestão de Riscos, é correto afirmar que o Tratamento do Risco é

a) a decisão de aceitar um risco com sua constante monitoração.

b) a ação de contratar um seguro para cobrir conseqüências da ocorrência de um risco.

c) o compartilhamento com um terceiro do prejuízo da perda ou benefício do ganho em relação a determinado risco.

d) o processo de seleção e implementação de medidas para modificar o risco.

e) a decisão de não se envolver, ou a ação de fuga de uma situação de risco.

União – Federal – Nível V - 2008

17) 8. Analise as seguintes afirmações relacionadas à Análise e Gerenciamento de Riscos de um projeto:

I. A Análise Quantitativa de Riscos é o processo de analisar numericamente o efeito dos riscos identificados nos objetivos gerais do projeto.

II. Um risco é um evento ou uma condição certa que sempre irá ocorrer e que provocará um efeito positivo ou negativo nos objetivos de um projeto.

III. Mitigação de riscos é uma técnica de planejamento de resposta a riscos que busca reduzir a probabilidade de ocorrência ou impacto de um risco.

IV. Considerando o ciclo de vida completo do projeto de desenvolvimento de um software, a Análise Qualitativa dos Riscos do projeto ocorre ao longo da fase de Manutenção Corretiva.

Indique a opção que contenha todas as afirmações verdadeiras.

a) I e II

b) II e III

c) III e IV

d) I e III

e) II e IV

ANA – Analista – Administração de Redes - 2009

18) 31. Um risco de segurança pode ser considerado uma função da ameaça em relação a

a) impacto, apenas.

b) probabilidade de ocorrência, apenas.

c) ocorrência ou não da ameaça.

d) ocorrência ou não da ameaça, num intervalo de tempo pré-especificado.

e) impacto e probabilidade de ocorrência.

SEFAZ – Analista – TI - 2010

19) 30. O Fluxo de Análise das ameaças e riscos, na ordem apresentada, consiste de

a) diversificação das ameaças, minimização das probabilidades dos riscos, redução dos pesos dos riscos, controle do risco, eliminação dos riscos prioritários, adoção de medidas de proteção lógica.

b) determinação das probabilidades dos riscos, quantificação dos riscos, avaliação do risco, proteção de ativos, eliminação dos riscos.

c) restrição das ameaças, planejamento das probabilidades dos riscos, determinação da hierarquia dos riscos, aquisição de software, estabelecimento de propriedades, redimensionamento.

d) identificação das medidas de proteção, determinação das probabilidades de ameaças, determinação das prioridades dos pesos dos riscos, vinculação de ameaças a riscos, realocação de pessoal.

e) identificação das ameaças, determinação das probabilidades dos riscos, determinação dos pesos dos riscos, avaliação do risco, estabelecimento de prioridades de proteção, adoção de medidas de proteção.

2.Comentários.

Cobit

AFC – CGU – Infraestrutura - 2008

1) 10- Para que as atividades de Tecnologia da Informação sejam efetivamente governadas, é importante considerar as atividades e riscos da área de TI a serem gerenciadas. As atividades são classificadas em domínios de responsabilidade. No COBIT, estes domínios são denominados

a) Planejar e Organizar; Adquirir e Implementar, Entregar e dar Suporte, Monitorar e Avaliar.

b) Planejar e Organizar; Adquirir e Executar, Entregar e dar Suporte, Monitorar e Medir.

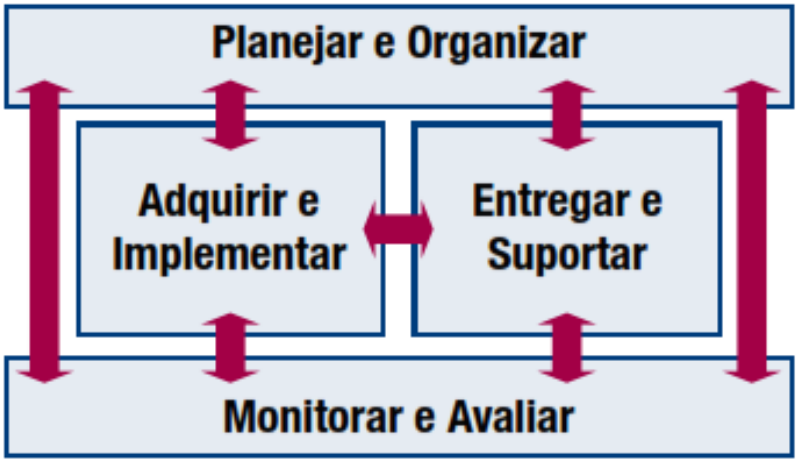
c) Planejar e Organizar; Implementar, Entregar e dar Suporte, Medir e Avaliar.

d) Planejar e Organizar; Adquirir e Desenvolver, Entregar e dar Suporte, Monitorar e Melhorar.

e) Planejar e Organizar; Adquirir e Implementar, Entregar e dar Suporte, Medir e Melhorar.

***Comentário**: Os domínios de processo apresentados pelo Cobit são:*

- *PO (Planejar e Organizar) - Provê direção para entrega de soluções (AI) e entrega de serviços (DS).*
- *AI (Adquirir e Implementar) - Provê as soluções e as transfere para tornarem-se serviços.*
- *DS (Entregar e Suportar) - Recebe as soluções e as tornam passíveis de uso pelos usuários finais.*
- *ME (Monitorar e Avaliar) - Monitora todos os processos para garantir que a direção definida seja seguida.*



A correta é a letra A.

AFC – CGU – Desenvolvimento - 2008

2) 1 - O COBIT - Control Objectives for Information and related Technology fornece boas práticas por meio de uma estrutura de domínio e processos e apresenta atividades de forma gerencial e lógica para a Governança de TI. O COBIT contém componentes inter-relacionados, provendo suporte para a governança, gerenciamento, controle e atendimento das necessidades de diferentes organizações. O componente Atividades-Chaves do COBIT (versão 4.1) está relacionado com

a) Indicadores de Performance.

b) Modelos de Maturidade.

c) Controle de Objetivos.

d) Responsabilidades e Contabilização.

e) Controle de Práticas.

***Comentário**: Dentro do Cobit, cada processo possui requisitos de controle genéricos a serem considerados juntamente aos objetivos de controle para que tenhamos uma visão completa dos requisitos de controle.*

Os requisitos de controle genéricos são:

- *PC 1 Metas e objetivos de controle: Assegura que os processos estejam ligados aos objetivos de negócios e que são suportados por métricas apropriadas. Define e comunica as metas e objetivos de controle (SMARRT):*
  - *Específicos.*
  - *Mensuráveis.*
  - *Acionáveis.*
  - *Realísticos.*
  - *Orientados a resultados.*
  - *Tempo apropriado.*
- *PC 2 Propriedade dos processos: Designa um proprietário para cada processo de TI e claramente define os papéis e responsabilidades de cada proprietário de processo.*
- *PC3 Repetibilidade dos Processos: Elabora e estabelece cada processo-chave de TI de maneira que possa ser repetido e produzir de maneira consistente os resultados esperados*
- *PC4 Papéis e Responsabilidades: Define as **atividades-chaves** e as entregas do processo.*
- *PC5 Políticas Planos e Procedimentos: Define e comunica como todas as políticas, planos e procedimentos que direcionam os processos de TI são documentados, revisados, mantidos, aprovados, armazenados, comunicados e utilizados para treinamento.*
- *PC6 Melhoria do Processo de Performance: Identifica um conjunto de métricas que fornecem direcionamento para os resultados e performance dos processos.*

A correta é a letra D.

AFC – STN – Desenvolvimento – 2008

3) 29- Analisem as seguintes afirmações relacionadas ao COBIT (Control Objectives for Information and related Technology):

I - Determina os objetivos de controle de gerenciamento a serem considerados.

II - Considera os requisitos de negócio.

III - Organiza as atividades de TI (Tecnologia da Informação) em um modelo de processos.

Indique a opção correta.

a) Apenas a afirmação I é correta.

b) Apenas a afirmação II é correta.

c) Apenas a afirmação III é correta.

d) Apenas as afirmações I e II são corretas.

e) As afirmações I, II e III são corretas.

***Comentário**: Conforme apresentado em nosso conteúdo teórico, O Cobit é focado em fazer a ligação, fechar um relacionamento entre a TI e os requisitos de negócio, organizar as atividades de TI em um modelo de processos geralmente aceito, identificar os mais importantes recursos de TI a serem utilizados e definir os objetivos de controle gerenciais a serem considerados.*

Tem como características ser:

- *Focado no negócio.*
- *Orientado para processos.*
- *Baseado em controles.*
- *Orientado por medições.*

Vejam então que todos os itens atendem à definição do Cobit, que inclusive foi retirada do próprio livro do Cobit 4.1.

A correta é a letra E.

ANA – Analista - DES e BD - 2009

4) 1 - O _____ é empregado na governança de recursos de Tecnologia da Informação (TI).

Assinale a opção que completa corretamente a frase acima.

a) OPM3

b) CMMI

c) GED

d) COBIT

e) Portal corporativo

***Comentário**: Esta é somente para verem que a conceituação básica de Cobit cai em concursos, vejamos que quem é empregado na governança de recursos de TI é o Cobit.*

A correta é a letra D.

CVM – Analista – TI – 2010

5) 38- Os níveis dos modelos de maturidade do COBIT são:

a) Insipiente (0). Inicial / Ad hoc (1). Repetitivo mas intuitivo (2). Programado (3). Gerenciado e qualitativo (4). Finalizado (5).

b) Inexistente (0). Programado (1). Repetitivo mas dedutivo (2). Definido (3). Gerenciado e mensurável (4). Repetitivo (5).

c) Inexistente (0). Em definição (1). Restritivo mas intuitivo (2). Otimizado (3). Gerenciado e mensurável (4). Disponibilizado (5).

d) A definir (0). Inicial / Ad hoc (1). Repetitivo e redundante (2). Definido (3). Orientado para mensuração (4). Maximizado (5).

e) Inexistente (0). Inicial / Ad hoc (1). Repetitivo mas intuitivo (2). Definido (3). Gerenciado e mensurável (4). Otimizado (5).

Comentário: *Os níveis do modelo de maturidade do Cobit são:*

- *0 inexistente – Completa falta de um processo reconhecido.*
- *1 inicial / Ad hoc – Existe evidências que a empresa reconheceu que existem questões e que precisam ser trabalhadas. No entanto, não existe processo padronizado.*
- *2 repetível, porém intuitivo – Os processos evoluíram para um estágio onde procedimentos similares são seguidos por diferentes pessoas fazendo a mesma tarefa.*
- *3 Processo definido – Procedimentos foram padronizados, documentados e comunicados através de treinamento.*
- *4 Gerenciado e Mensurável – A gerencia monitora e mede a aderência aos procedimentos e adota ações onde os processos parecem não estar funcionando bem.*
- *5 Otimizado – Os processos foram refinados a um nível de boas práticas, baseado no resultado de um contínuo aprimoramento e modelagem da maturidade como outras organizações.*

A correta é a letra E.

CVM – Analista – Sistemas – 2010

6) 56- Assinale a opção correta.

a) A estratégia de *outsourcing* decide **como gerenciar o desempenho dos equipamentos.**

b) O objetivo principal da Governança de TI é gerenciar *outsourcing*.

c) A estratégia de *outsourcing* decide **como gerenciar os negócios internos dos fornecedores ou prestadores de serviços.**

d) O objetivo principal da Governança de TI é escolher a melhor alternativa de programação.

e) O objetivo principal da Governança de TI é alinhar TI aos requisitos do negócio.

Comentário: *Esta é uma questão interessante, pois traz conhecimento da área de Governança de TI e de Planejamento Estratégico empresaria.*

Primeiro de tudo devemos saber que outsourcing designa uma ação que existe por parte de uma organização em obter mão-de-obra de forma da empresa, mão-de-obra terceirizada.

E também devemos ter em mente que o principal objetivo da Governança de TI é manter alinhados TI e negócio e para tal feito ela não faz uso de outsourcing, foge à governabilidade sua. (ARAGON).

Repare então que as letras A, B, C e D acabam por chocar tais conceitos apresentados e se tornam letras falsas.

Definitivamente esta última é a que realmente nos cabe como certa, ela traz justamente o objetivo da Governança de TI apresentado no livro do Cobit 4.1.

A correta é a letra E.

7) 58- O ciclo da Governança de TI engloba

a) Negócio Estratégico e *Compliance*. Decisão, Ação, Priorização e Alocação de Pessoas. Estrutura, Processos, Operações e Gestão. Planejamento do Desempenho.

b) Alinhamento Tático e Estratégico. Informação, Decisão e Ação. Estrutura, Procedimentos, Operações e Monitoramento. Medição do Desempenho.

c) Alinhamento Estratégico e *Compiling*. Decisão, Compromisso, Programação e Alocação de Recursos. Planos, Programas, Processos e Gestão. Medição da Aceitação.

d) Alinhamento Estratégico e *Compliance*. Decisão, Compromisso, Priorização e Alocação de Recursos. Estrutura, Processos, Operações e Gestão. Medição do Desempenho.

e) Estratégias Alinhadas e *Pipelining*. Decisão, Compromisso, Priorização e Busca de Resultados. Estrutura, Processos, Planilhas e Operação. Desempenho Organizacional.

***Comentário**: Senhores, outra questão retirada do livro do Aragon – Implantando a Governança de TI.*

O ciclo da Governança de TI é composto por 4 grandes etapas:

- *Alinhamento estratégico de TI.*
- *Decisão, compromisso, priorização e alocação de recursos.*
- *Estruturas, processos, operações e gestão.*
- *Medição e desempenho. (ARAGON).*

A correta é a letra D.

SUSEP – Analista – TI – 2010

8) 6 - Em relação ao COBIT, é correto afirmar que o mesmo

a) estabelece posicionamentos com os registros do negócio.

b) identifica os principais recursos de WFD, nos quais deve haver menos requisitos.

c) organiza as atividades de TI em um modelo de processos genérico.

d) estabelece prioridades entre os responsáveis pelo negócio.

e) define as métricas sem controle que devem ser seqüenciadas no desenvolvimento.

***Comentário:** Vejamos então que o COBIT suporta (oferece suporte) a Governança de TI com metodologia para assegurar que:*

- *A área de TI esteja alinhada com os negócios.*

- *A área de TI habilite o negócio e maximize os benefícios.*
- *Os recursos de TI sejam usados responsavelmente.*
- *Os riscos de TI sejam gerenciados apropriadamente.*

O Cobit é focado em fazer a ligação, fechar um relacionamento entre a TI e os requisitos de negócio, organizar as atividades de TI em um modelo de processos geralmente aceito, identificar os mais importantes recursos de TI a serem utilizados e definir os objetivos de controle gerenciais a serem considerados.

Para tanto ele faz uso dos principais frameworks do mercado, trazendo assim uma visão unificada de processos genéricos que poderão ser utilizados por empresas que pretendem implantar a Governança de TI.

A correta é a letra C.

9) 7 - Entre as aplicações do COBIT em uma organização, situam-se

a) auditoria de riscos operacionais de concorrentes e qualificação de armazenadores de TI.

b) implantação modular da Governança de TI e realização de *benchmarking*.

c) avaliação dos *topservers* de TI e desenvolvimento dos riscos situacionais de TI.

d) desmembramento de riscos e benefícios da TI e realização de *branch and bound*.

e) atualização de *casual failures* e implantação exógena da Governança de TI.

Comentário: *Conforme comentário já feito anteriormente e complementando a idéia agora cobrada pelo avaliador.*

O COBIT suporta (oferece suporte) a Governança de TI com metodologia para assegurar que:

- *A área de TI esteja alinhada com os negócios.*
- *A área de TI habilite o negócio e maximize os benefícios.*
- *Os recursos de TI sejam usados responsavelmente.*
- *Os riscos de TI sejam gerenciados apropriadamente.*

O Cobit é focado em fazer a ligação, fechar um relacionamento entre a TI e os requisitos de negócio, organizar as atividades de TI em um modelo de processos geralmente aceito, identificar os mais importantes recursos de TI a serem utilizados e definir os objetivos de controle gerenciais a serem considerados.

Para tanto ele faz uso dos principais frameworks do mercado, trazendo assim uma visão unificada de processos genéricos que poderão ser utilizados por empresas que pretendem implantar a Governança de TI.

Utiliza como ferramentas em seus processos técnicas de benchmarking com o objetivo de analisar a situação atual da instituição no mercado e projetá-la no futuro.

A correta é a letra B.

10) 8 - As áreas foco da Governança de TI na visão do COBIT são:

a) Alinhamento Estratégico, Agregação de Valor, Gerenciamento de Riscos, Gerenciamento de Recursos e Medições de Desempenho.

b) Alinhamento Estratégico, Medições de Perdas, Gerenciamento de Riscos, Gerenciamento de Requisitos e Condições de Mercado.

c) Planejamento Estratégico, Valores de Ativos, Gerenciamento de Pessoas, Agregação de Componentes e Medições de Custos.

d) Aquisições Estratégicas, Composição de Valor, Gerenciamento de Benefícios, Gerenciamento de Recursos e Modificações de Desempenho.

e) Alinhamento de Desempenho, Associação de Valores e Benefícios, Gerenciamento de Decisões, Gerenciamento de Perda de Recursos e Medições de Riscos.

Comentário: *Conforme colocado em nosso conteúdo teórico, o Cobit prove um modelo de processo genérico que representa todos os processos normalmente encontrados nas funções de TI, fornecendo assim um modelo de referência comum compreendido por gerentes operacionais de TI e gerentes de negócios, como foco nas áreas (áreas foco):*

- *Alinhamento Estratégico: ligação entre plano de negócio e TI.*
- *Entrega de Valor: TI entrega os prometidos benefícios previstos na estratégia da organização.*
- *Gestão de recursos: melhor utilização possível.*
- *Gestão de riscos: riscos assumidos e delegados aos funcionários mais experientes.*
- *Mensuração (medição) de desempenho: acompanha e monitora a implementação da estratégia.*

A correta é a letra A.

11) 41- Um dos fatores motivadores da Governança de TI é

a) a dependência do negócio em relação à TI.

b) o ambiente de trabalho.

c) a integração organizacional.

d) a TI como provedora de serviços.

e) o valor da informação.

Comentário: *Esta questão caberia recurso, com certeza, pois observe bem que o maior ativo a ser preservado e que motivaria a Governança de TI em uma visão ampla seria a informação.*

Mas o avaliador considerou o que é encontrado inclusive no próprio livro do Cobit em seu sumário, veja bem que as organizações consideram como seu bem mais valioso a informação e a tecnologia que a suporta.

A correta é a letra A.

12) 42- A Governança de TI deve

a) garantir o posicionamento da TI como norteador das estratégias do negócio.

b) alinhar as estratégias da organização aos objetivos e à infraestrutura da TI no negócio.

c) garantir o alinhamento da TI ao negócio, tanto no que diz respeito às aplicações como à infraestrutura de serviços de TI.

d) garantir o planejamento da TI em conformidade com as diretrizes dos fornecedores relativas aos sistemas de informações.

e) garantir o alinhamento da TI ao negócio, tanto no que diz respeito aos provedores como à infraestrutura de serviços da concorrência.

***Comentário**: Conforme definição apresentada em nosso conteúdo teórico.*

A Governança de TI é a "capacidade organizacional exercida pela alta direção, gerência de negócios e gerência de TI para controlar a formulação e implementação da estratégia de TI e, com isso, assegurar o alinhamento entre negócios e TI" (Van Grembergen, 2004)

A correta é a letra C.

Riscos

AFC – CFU – Infraestrutura - 2008

13) 42. Considerando uma adequada gestão de riscos para a segurança da informação, analise as afirmações a seguir e assinale a opção correta.

I. É recomendável estabelecer regras para o uso aceitável de ativos associados aos recursos de processamento da informação.

II. É recomendável efetuar, criticamente, a análise de riscos de segurança, uma vez que esta considera ameaças, vulnerabilidades e impactos em função dos negócios da organização.

III. É recomendável estabelecer responsabilidades e procedimentos de gestão para assegurar respostas rápidas e efetivas a incidentes de segurança.

a) Apenas I e II são verdadeiras.

b) Apenas II e III são verdadeiras.

c) Apenas I e III são verdadeiras.

d) I, II e III são verdadeiras.

e) I, II e III são falsas.

Comentário: *Pela definição apresentada nas normas 27.001 e 27.005 podemos dizer que a gestão de riscos é uma série de atividades relacionadas à forma como a organização irá tratar os riscos, trata de todo o ciclo de vida de um risco.*

Dentre suas práticas temos a necessidade da identificação e gestão dos ativos organizacionais de forma que a proteger a informação da organizacionais.

Uma outra prática publicada nas normas diz respeito a análise de riscos de segurança levando-se em conta as presentes ameaças, vulnerabilidades e os impactos dentro da visão de riscos de segurança da informação.

Por final, uma outra prática publicada nestas normas diz respeito à delegação de responsabilidades específicas no contexto de segurança da informação e gestão de riscos de forma que seus responsáveis saibam quando e como agirem no momento necessário.

A correta é a letra D.

AFC – CFU – Desenvolvimento - 2008

14) 48. Gerenciamento de riscos significa identificar riscos e traçar planos para minimizar seus efeitos sobre o projeto. Assinale a opção que contenha a descrição de um exemplo de Risco de Negócios.

a) A tecnologia sobre a qual o sistema está sendo construído foi superada por nova tecnologia.

b) O tamanho do sistema foi subestimado.

c) As especificações de interface não estavam disponíveis dentro do prazo.

d) Haverá uma mudança no gerenciamento organizacional, com a definição de prioridades diferentes.

e) Haverá maior número de mudanças nos requisitos do que o previsto.

Comentário: *O Risco de negócio pode ser definido como a incerteza inerente às projeções do resultado operacional, ou seja, o resultado antes de impostos e encargos financeiros. Vejamos que mesmo que cause certo tipo de polêmica, esta questão nos traz de uma forma muito clara a letra A com a única opção que cobre o conceito aplicável a Risco de negócio, vejam que a letra B nos traz na verdade uma falha de estimativa do tamanho do sistema, a letra C uma falha no timer de atendimento a uma informação solicitada e a letra D e E definitivamente não se enquadram no conceito de risco.*

A correta é a letra A.

SEMUT – Prefeitura de Natal – ATM – Informática - 2008

15) 35 Analise as seguintes afirmações relacionadas à Segurança da Informação:

I. Uma Vulnerabilidade é um evento com conseqüências negativas resultante de um ataque bem-sucedido.

II. Uma Ameaça é uma expectativa de acontecimento acidental ou proposital, causada por um agente, que pode afetar um ambiente, sistema ou ativo de informação.

III. A Vulnerabilidade é uma fonte produtora de um evento que pode ter efeitos adversos sobre um ativo de informação.

IV. O Ataque é um evento decorrente da exploração de uma vulnerabilidade por uma ameaça.

Indique a opção que contenha todas as afirmações verdadeiras.

a) I e II

b) II e III

c) III e IV

d) I e III

e) II e IV

***Comentário**: Para resolver este tipo de questão a melhor forma é procurarmos qual das alternativas está errada e já em seguida eliminar as letras que estiverem com ela listada.*

Uma vulnerabilidade é uma fraqueza que acaba criando situações que poderão ser exploradas por ameaças, vejam então que a alternativa I já está errada e é o que justamente já elimina as letras "a" e "d".

Uma ameaça é vista como tudo aquilo que tem potencial de causar algum tipo de dano a um ativo da organização, seja causada de forma proposital ou acidental, repare então que a opção II está correta o que já nos traz então as letras "b" ou "e" como corretas.

Veja então que a opção III acaba por se tornar errada por não trazer a definição correta de vulnerabilidade (apresentado no inicio do comentário desta questão), o que torna então como correta a letra E.

E o ataque é justamente a exploração de uma vulnerabilidade.

A correta é a letra E.

16) 39. A Gestão de Risco de uma organização é o conjunto de processos que permite identificar e implementar as medidas de proteção necessárias para diminuir os riscos a que estão sujeitos os seus ativos de informação. Com relação aos conceitos utilizados na Gestão de Riscos, é correto afirmar que o Tratamento do Risco é

a) a decisão de aceitar um risco com sua constante monitoração.

b) a ação de contratar um seguro para cobrir conseqüências da ocorrência de um risco.

c) o compartilhamento com um terceiro do prejuízo da perda ou benefício do ganho em relação a determinado risco.

d) o processo de seleção e implementação de medidas para modificar o risco.

e) a decisão de não se envolver, ou a ação de fuga de uma situação de risco.

***Comentário**: Vamos diretamente para a definição de Tratamento de Riscos.*

Segunda fase da Gestão de Riscos tem como objetivo a seleção e implementação de medidas de forma a reduzir os riscos negativos. Os tratamentos a serem dados aos riscos podem ser:

1. ***Evitar**: neste caso a instituição estará preocupada em não se envolver ou não se expor a uma situação de risco, simplesmente tentará evitá-lo.*
2. ***Transferir**: caso clássico da contratação de um seguro, na qual o responsável pelo risco transfere o impacto dele, mas ainda permanece responsável pelo seu monitoramento. Está relacionado ao ônus da perda ou ao benefício do ganho. Em segurança da informação somente riscos negativos são considerados para efeitos de transferência.*
3. ***Reter**: uma forma de tratamento de risco na qual a alta administração decide realizar a atividade, assumindo as responsabilidades caso ocorra o risco identificado. (04/IN01/DSIC/GSIPR/Presidência da República). Aceitação do ônus da perda ou do benefício do ganho.*

4. ***Reduzir:*** *implementar algum tipo de proteção que reduza a probabilidade ou o impacto negativo do risco, caso mesmo assim ocorra, acaba por gerar risco residual.*

Vemos então claramente que a única alternativa que atendo ao que é solicitado dentro da definição de tratamento de riscos é a letra D, todas as outras dizem respeito a algum tipo de tratamento a ser dado ao risco.

A correta é a letra D.

União – Federal – Nível V - 2008

17) 8 Analise as seguintes afirmações relacionadas à Análise e Gerenciamento de Riscos de um projeto:

I. A Análise Quantitativa de Riscos é o processo de analisar numericamente o efeito dos riscos identificados nos objetivos gerais do projeto.

II. Um risco é um evento ou uma condição certa que sempre irá ocorrer e que provocará um efeito positivo ou negativo nos objetivos de um projeto.

III. Mitigação de riscos é uma técnica de planejamento de resposta a riscos que busca reduzir a probabilidade de ocorrência ou impacto de um risco.

IV. Considerando o ciclo de vida completo do projeto de desenvolvimento de um software, a Análise Qualitativa dos Riscos do projeto ocorre ao longo da fase de Manutenção Corretiva.

Indique a opção que contenha todas as afirmações verdadeiras.

a) I e II

b) II e III

c) III e IV

d) I e III

e) II e IV

***Comentário**:*

A correta é a letra D.

ANA – Analista – Administração de Redes - 2009

18) 31 Um risco de segurança pode ser considerado uma função da ameaça em relação a

a) impacto, apenas.

b) probabilidade de ocorrência, apenas.

c) ocorrência ou não da ameaça.

d) ocorrência ou não da ameaça, num intervalo de tempo pré-especificado.

e) impacto e probabilidade de ocorrência.

***Comentário**: Um risco pode ser encarado como a probabilidade de uma ameaça explorar uma ou mais vulnerabilidades causando prejuízos aos ativos da organização, estão sempre relacionados à ocorrência de incidentes.*

*Sua escala de criticidade para a organização será dada pela combinação (produto, multiplicação, X, *) de dois fatores, a probabilidade de sua ocorrência e as conseqüências trazidas pela ocorrência do incidente (impacto).*

Risco (ameaça) = Probabilidade X Impacto.

A correta é a letra E.

SEFAZ – Analista – TI - 2010

19) 30. O Fluxo de Análise das ameaças e riscos, na ordem apresentada, consiste de

a) diversificação das ameaças, minimização das probabilidades dos riscos, redução dos pesos dos riscos, controle do risco, eliminação dos riscos prioritários, adoção de medidas de proteção lógica.

b) determinação das probabilidades dos riscos, quantificação dos riscos, avaliação do risco, proteção de ativos, eliminação dos riscos.

c) restrição das ameaças, planejamento das probabilidades dos riscos, determinação da hierarquia dos riscos, aquisição de software, estabelecimento de propriedades, redimensionamento.

d) identificação das medidas de proteção, determinação das probabilidades de ameaças, determinação das prioridades dos pesos dos riscos, vinculação de ameaças a riscos, realocação de pessoal.

e) identificação das ameaças, determinação das probabilidades dos riscos, determinação dos pesos dos riscos, avaliação do risco, estabelecimento de prioridades de proteção, adoção de medidas de proteção.

***Comentário**: Esta é uma questão um pouco avançada, mas pode ser encontrada na norma NBR ISO/IEC e é característica da ESAF fazer questões do gênero.*

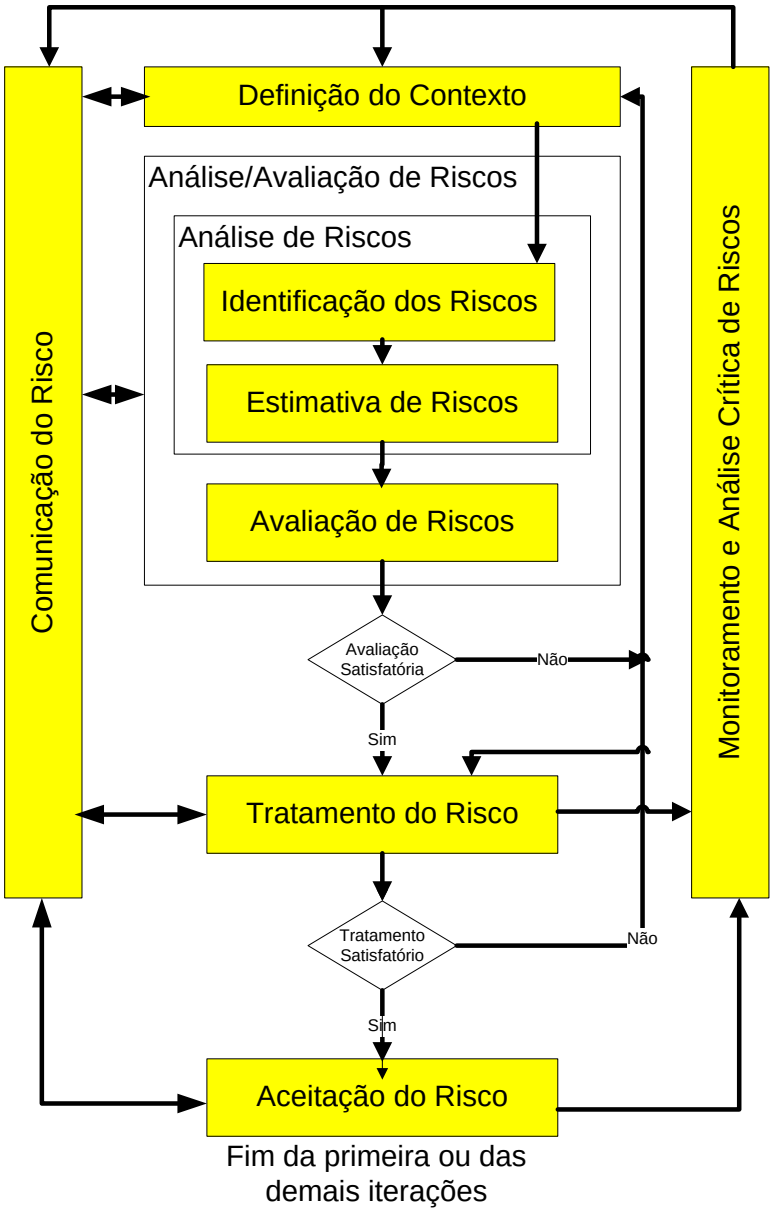
O termo AAR – Análise e Avaliação dos Riscos vem do inglês Risk Assesment e a sua primeira definição análise (risk analysis) trata da identificação de ameaças (threat identification) e estimativa do risco (risk estimation), já a avaliação (risk evaluation) trata de comparar os riscos que foram previamente identificados e estimados com os critérios de risco definidos pela organização.

Risco {
- *Probabilidade.*
- *Evento*
- *Conseqüência.*

Mas o avaliador está procurando pelo fluxo completo seguido quando falamos de Análise da ameaças e riscos, que deverá ser avaliada em um visão um pouco mais abrangente, conforme gráfico abaixo presente na NBR ISO/IEC 27.005.

Bem, em uma primeira olhada poderíamos dizer que não existe resposta correta certo? Errado gente, pois ao expandirmos a estimativa de riscos iremos encontrar a determinação das probabilidades e dos pesos dos riscos, o que nos traz então a letra E como correta.

Fiquem atentos a esta característica da ESAF em ficar mergulhando e entrando mais que as outras bancas em relação às definições e seus conceitos internos, isso é feito tanto nesta disciplina quanto em Gerenciamento de Projetos ou Gestão e Governança de TI como um todo.



A correta é a letra E.

3.Gabaritos.

Cobit

AFC – CGU – Infraestrutura - 2008

1) A

AFC – CGU – Desenvolvimento - 2008

2) D

AFC – STN – Desenvolvimento – 2008

3) E

ANA – Analista - DES e BD - 2009

4) D

CVM – Analista – TI – 2010

5) E

CVM – Analista – Sistemas – 2010

6) E
7) D

SUSEP – Analista – TI – 2010

8) C
9) B
10)A
11)A
12)C

Riscos

AFC – CGU – Infraestrutura - 2008

13)D

AFC – CGU – Desenvolvimento - 2008

14)A

SEMUT – Prefeitura de Natal – ATM – Informática - 2008

15)E
16)D

União – Federal – Nível V - 2008

17)D

ANA – Analista – Administração de Redes - 2009

18)E
19)E

Utilizem nosso canal aberto de comunicação via e-mail no endereço gabrielpacheco@estrategiaconcursos.com.br no qual (na medida do possível ☺) dúvidas sobre questões e considerações feitas nas aulas poderão ser tiradas, mas reforço que dou preferência ao Fórum criado, assim todos ficam sabendo e podem inclusive participar. Ao enviarem e-mail para este endereço, favor colocarem sempre no campo assunto sobre qual curso, cargo ou concurso está falando.

Caso achem necessária a criação de um fórum de discussão, favor me enviarem e-mail com tal solicitação que crio mesmo fora da estrutura do Estratégia para discutirmos em grupo as dúvidas e questões referentes à nossa disciplina no concurso.

Como deu trabalho para escrever esta aula e todas as outras que virão também vão dar, caso resolva utilizá-la para qualquer fim, favor citar a fonte e também me avisar. ☺

Lembrem-se sempre, **seu maior adversário é você.**

Abraços a todos!!!!