MARCOS ASSI

Gestão de riscos com controles internos

Ferramentas, certificações e métodos para garantir a eficiência dos negócios

Saint Paul
Editora

Sumário

Apresentação 17

CAPÍTULO 1
Conceito de riscos e controles internos 19
1.1 Conceito de risco 19
1.2 Conceito de controles internos 22
1.3 Cultura organizacional 25
1.4 O lado comportamental das pessoas 27

CAPÍTULO 2
Controles internos 31
2.1 Entendimento sobre controles internos 31

CAPÍTULO 3
Gestão de riscos 41
3.1 Entendendo os riscos 41
3.2 Gestão de crises e continuidade de negócios 48
3.3 Resultados esperados pelos métodos para identificação dos riscos 50

CAPÍTULO 4
Casos de fraudes 51
4.1 Conscientização e cultura 51
4.2 Exemplos de casos reais 54

CAPÍTULO 5
Lei Sarbanes-Oxley 63
5.1 Lei Sarbanes-Oxley 63
5.2 Impactos gerais da Lei Sarbanes-Oxley 67
5.3 Impactos da SOX em TI (Tecnologia da Informação) 68
5.4 Impactos da SOX nos custos 69
5.5 Desafios na implantação 70
5.6 Vantagens com a implementação 70
5.7 Ferramentas que auxiliam a adequação à lei 71
5.8 Categorias de controles segundo à SOX 71

CAPÍTULO 6
Conhecendo o COSO 7
6.1 COSO – Committee of Sponsoring Organizations of the Treadway Commission 7
6.2 Componentes de controles internos de acordo com o COSO 7
6.3 Processos de identificação dos riscos segundo o COSO 8

CAPÍTULO 7
ISO 31000:2009 (riscos) 8
7.1 Introdução à ISO 31000:2009 8
7.2 Princípios da gestão de riscos 8
7.3 Estrutura da gestão de riscos 9
7.4 Concepção da estrutura para gerenciar riscos 9
7.5 Processo: comunicação e consulta 9
7.6 Estabelecimento do contexto 9
7.7 Processo de avaliação de riscos 9
7.8 Tratamento de riscos 9
7.9 Monitoramento e análise crítica 9
7.10 Registros do processo de gestão de riscos 9

CAPÍTULO 8
Metodologia do FMEA (*Failure mode and effect analysis*) 10
8.1 A metodologia de análise do tipo e efeito de falha 10
8.2 Aplicação da metodologia FMEA 10
8.3 Atribuições da gestão de risco operacional 10

CAPÍTULO 9
Indicadores, recursos e possíveis ferramentas 11
9.1 Análise SWOT 11
9.2 Análise KPI – *Key performance indicator* 11
9.3 Análise BSC – *Balance scorecard* 11
9.4 Procedimentos internos 11
9.5 Mapeamento de processos, riscos e controles 11
9.6 Mapas e relatórios 12
9.7 CSA – *Control self-assessment* 12

CAPÍTULO 10
Segurança da informação 12
10.1 Conceito 12
10.2 As normas de segurança da informação ISO/IEC 27001 e ISO/IEC 27002 e os seus documentos eletrônicos 13
10.3 Os benefícios da certificação em ISO 27001 13

CAPÍTULO 11
Coletânea de artigos do autor sobre fraudes, controles internos e riscos 13
1. Qual é a sua tolerância à fraude? 13
2. Cultura organizacional, folclore ou realidade? 13
3. Como reduzir fraude no mundo corporativo 14

4. Como controlar terceirização? 141
5. Minimizando os riscos 142
6. A sua empresa está em *compliance*? 143
7. Auditoria de controles internos no foco 144
8. Segurança da informação e riscos corporativos 145
9. Fraude contábil: de quem é a culpa? 146
10. Controles internos na gestão de riscos 148
11. O futuro do *compliance* de TI 149
12. Postura profissional – Conduta e ética 150
13. Controles internos, gestão de negócios e de TI, melhorando a gestão 152
14. Cultura organizacional de controle e gestão 153
15. Segurança da informação, fraude e divisórias 154
16. Operações não autorizadas? Falta de controle interno? Negligência operacional? 155
17. Controles internos e gestão de riscos, como obter resultados? 156
18. Controles de incidentes e "não" incidentes, como demonstrar? 157
19. Titanic operacional 158

Lista de abreviaturas e siglas 161

Referências 163