GESTÃO DE RISCO

Docentes: Dr. Sérgio Mavie, MSc. | Dr. Alfredo Covele, MSc.

Maputo, 2024

OBJECTIVOS

- Definir gestão de riscos, identificação de riscos e controlo de riscos;
- Descrever como o risco é identificado e avaliado;
- Avaliar o risco com base na probabilidade de ocorrência e provável impacto;
- Explicar os aspectos fundamentais da documentação do risco através do processo de avaliação de risco;

OBJECTIVOS

- Descrever as várias opções de estratégia de mitigação de risco;
- Identificar as categorias que podem ser usadas para classificar os controlos;
- Reconhecer as estruturas conceptuais existentes para avaliar os controlos de risco e formular um análise de benefícios; e
- Descrever como manter e perpetuar os controlos de risco.

INTRODUÇÃO

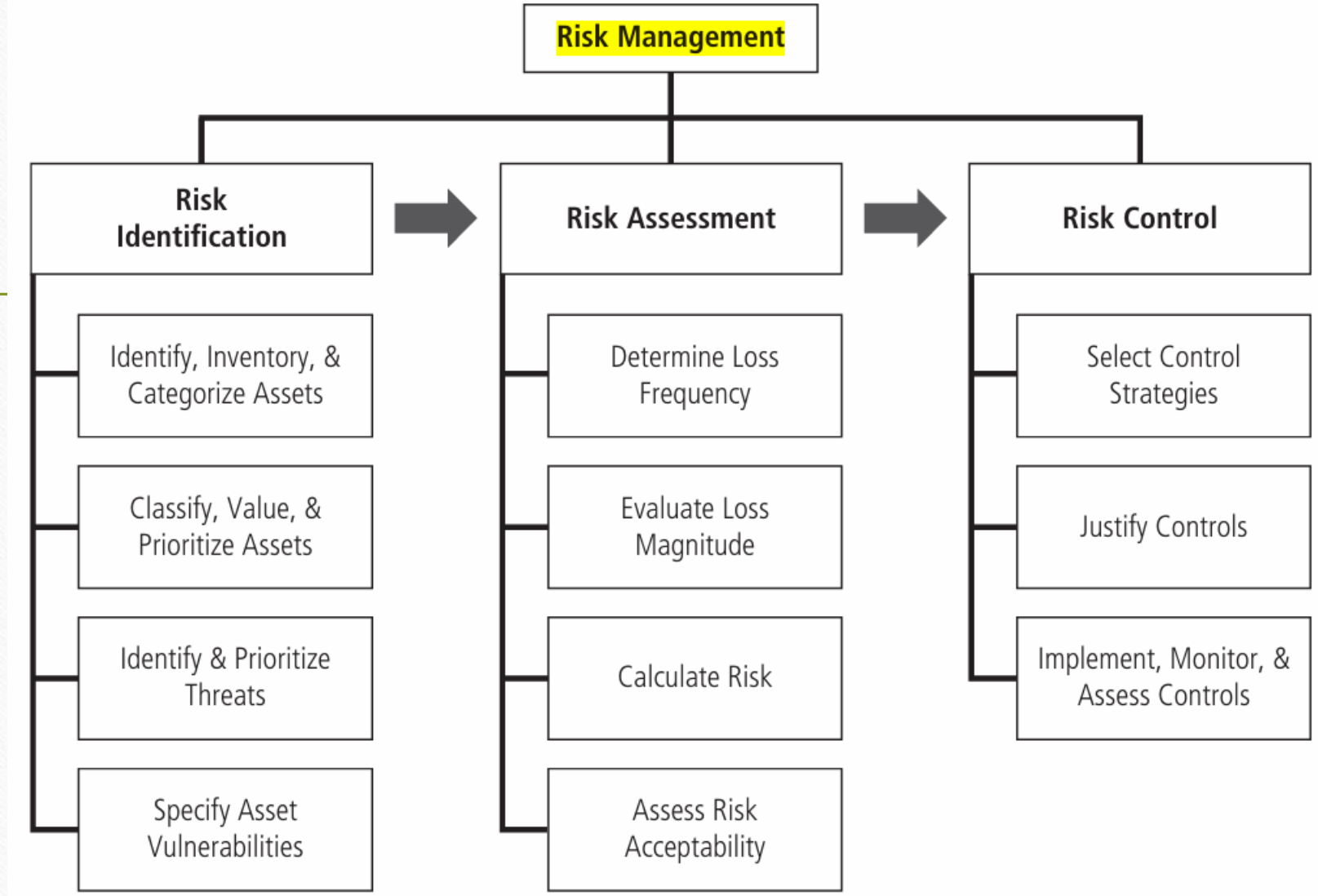
- Para acompanhar a concorrência, as organizações devem projectar e criar ambientes seguros nos quais processos e procedimentos de negócios podem funcionar.
- Esses ambientes devem **manter confidencialidade e privacidade e assegurar a integridade dos dados** organizacionais - objetivos que são atendidos **através da aplicação dos princípios de gestão de riscos**.

Gestão de Risco

- **A gestão de riscos** - é o processo de identificação do risco, avaliar a sua magnitude relativa, e executar passos para reduzir esse risco a um nível aceitável.
- A gestão de riscos envolve três grandes empreendimentos:
  - **Identificação de riscos**
  - **Avaliação de riscos; e**
  - **Controlo de risco.**

Gestão de Risco

- **Identificação de riscos** - é o exame e documentação (1) da postura de segurança da tecnologia da informação de uma organização e (2) dos riscos que ela enfrenta.
- **Avaliação de risco** - é a determinação da extensão/nível em que os activos de informação da organização estão expostos ou em risco.
- **Controlo de risco** - é a aplicação de controlos para reduzir os riscos aos dados e sistemas de informação de uma organização


Risk Management
Risk Identification
Identify, Inventory, & Categorize Assets
Classify, Value, & Prioritize Assets
Identify & Prioritize Threats
Specify Asset Vulnerabilities
Risk Assessment
Determine Loss Frequency
Evaluate Loss Magnitude
Calculate Risk
Assess Risk Acceptability
Risk Control
Select Control Strategies
Justify Controls
Implement, Monitor, & Assess Controls

Gestão de Risco

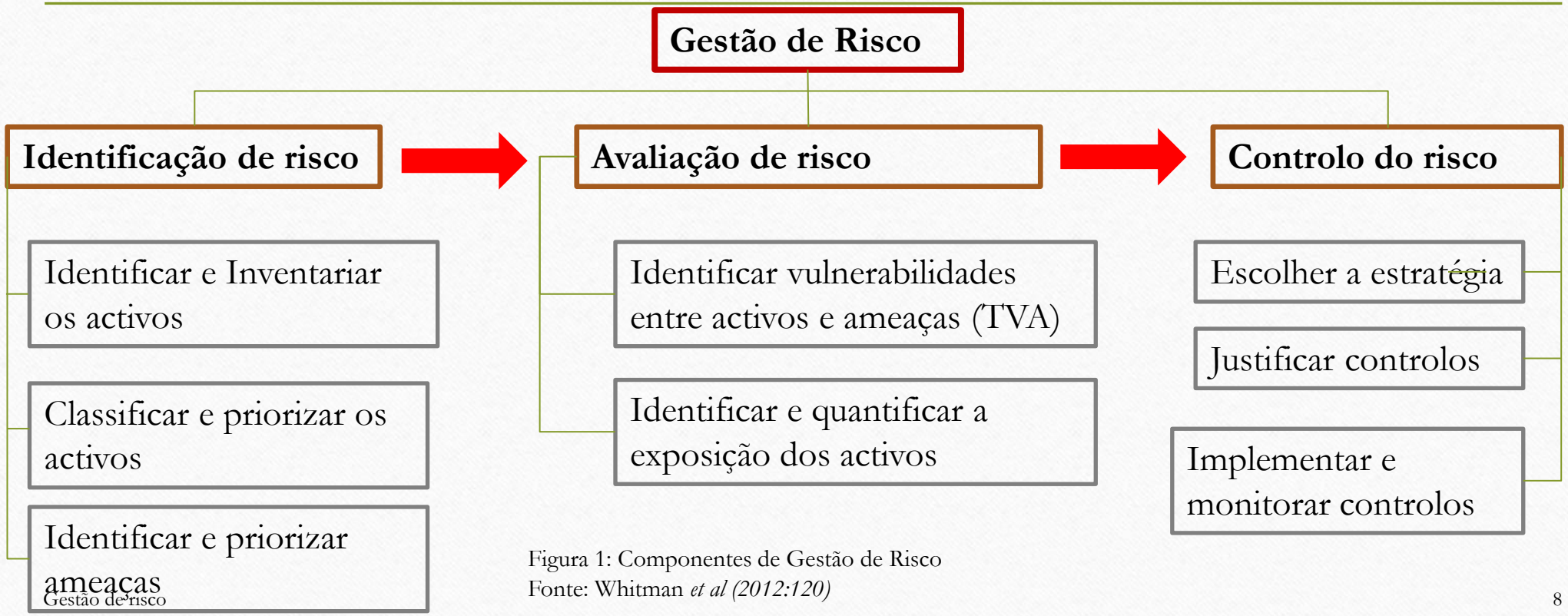


Figura 1: Componentes de Gestão de Risco
Fonte: Whitman *et al (2012:120)*

Gestão de Risco

"If you know the enemy and know yourself, you need not fear the result of a hundred battles. If you know yourself but not the enemy, for every victory gained you will also suffer a defeat. If you know neither the enemy nor yourself, you will succumb in every battle"

By General Sun Tzu Wu 2400 years ago

Gestão de Risco

- **Conhecer-se a si próprio** significa que:
  - Você deve identificar, examinar e entender as informações e os sistemas actualmente em vigor em sua organização; e
  - saber como estes agregam valor à organização e quais vulnerabilidades são susceptíveis.

Gestão de Risco

- **Conhecer o inimigo** significa identificar, examinar e entender as ameaças que a organização enfrenta para:
  - (1) poder determinar quais aspectos da ameaça afetam mais diretamente a segurança da organização e seus ativos de informação, e;
  - com base nessas informações, criar uma lista de ameaças em que cada uma é classificada de acordo com a importância dos ativos de informações que ela ameaça.

1. Identificação de Risco

- Consiste em:
  1. Planificar e organizar o processo;
  2. **Categorizar os componentes do Sistema de Informação;**
  3. **Inventariar e categorizar os activos;**
  4. **Classificar e priorizar os activos**
  5. **Identificar e priorizar as ameaças**; e
  6. Especificar as vulnerabilidades dos activos.

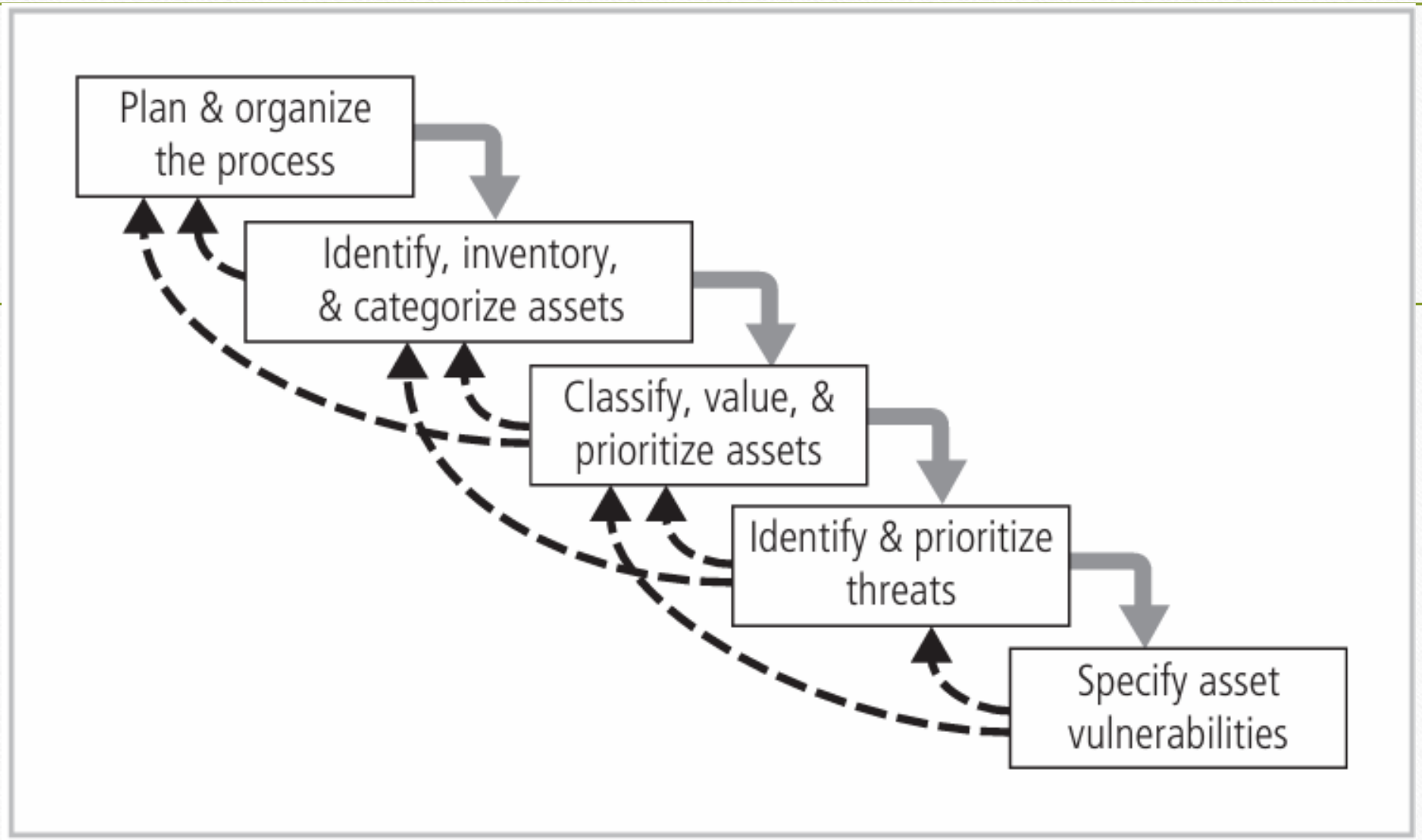


Figure 5-4 Components of risk identification

1.1. Identificação de Risco - Inventariar e categorizar os activos

Quadro 1: Categorização de Componentes de um SI (Whitman *et al, 2014:237*)

COMPONENTES DO SI	COMPONENTES(SecSDLC)	COMPONENTES DE SGR
PESSOAS	Empregados.	Empregados de Confiança. Outro Staff
	Não empregados	Contratados. Consultores. Estranhos
PROCEDIMENTOS	Procedimentos	Procedimentos padrão e Procedimentos Sensíveis de TI e negócios
DADOS	Informação	Transmissão. Processamento. Armazenamento
SOFTWARE	Software	Aplicações. SO. Componentes de Segurança
HARDWARE	Dispositivos do sistema e periféricos	Sistemas e periféricos. Dispositivos de segurança
	Componentes de Rede	Componentes da intranet. Internet ou Componentes DMZ.

1.1. Identificação de Risco - Inventariar e categorizar os activos

- **Identificação de Ativos de Hardware, Software e Rede**:
  - Nome;
  - Endereço IP;
  - Endereço MAC;
  - Tipo de Elemento (eg.):
    - S (Server)
    - W2K (Windows 2000)
    - AS (Advanced Server)
  - Número de Série;
  - Nome do fabricante;
  - Número do modelo de fabricante;
  - Versão do Software;
  - Endereços físico;
  - Endereços lógico;
  - Entidade controladora;

1.2. Identificação de Risco – Classificar e priorizar os activos

- **Externa/Pública**: todas as informações que foram aprovadas pela gerência para divulgação pública.
- **Interna/ Somente para Uso Oficial**: Usado para todas as informações internas que não atendem aos critérios da categoria confidencial e deve ser visualizado apenas por funcionários corporativos, contratados autorizados e outros terceiros;
- **Confidencial/Sensível/Proprietário**: usado para as informações corporativas mais sensíveis que devem ser rigorosamente controladas, mesmo dentro da empresa;
- **Classificada**: Informação do maior sigilo para a organização cuja divulgação poderia afectar seriamente o bem-estar da organização.

1.2. Identificação de Risco - Classificar e priorizar/valorizar os activos

System Name: SLS E-Commerce
Date Evaluated: February 2012
Evaluated By: D. Jones

Information assets	Data classification	Impact to profitability
Information Transmitted:		
EDI Document Set 1—Logistics BOL to outsourcer (outbound)	Confidential	High
EDI Document Set 2—Supplier orders (outbound)	Confidential	High
EDI Document Set 2—Supplier fulfillment advice (inbound)	Confidential	Medium
Customer order via SSL (inbound)	Confidential	Critical
Customer service request via e-mail (inbound)	Private	Medium
DMZ Assets:		
Edge router	Public	Critical
Web server #1—home page and core site	Public	Critical
Web server #2—Application server	Private	Critical

Notes: BOL: Bill of Lading
DMZ: Demilitarized Zone
EDI: Electronic Data Interchange
SSL: Secure Sockets Layer

Figura 2: Exemplo de Folha de Inventário com priorização

1.2. **Identificação de Risco** - Classificar e priorizar/valorizar os activos

Information asset	Criterion 1: Impact to revenue	Criterion 2: Impact to profitability	Criterion 3: Impact to public image	Weighted score
Criteria weights must total 100	30	40	30	
EDI Document Set 1—Logistics BOL to outsourcer (outbound)	0.8	0.9	0.5	75
EDI Document Set 2—Supplier orders (outbound)	0.8	0.9	0.6	78
EDI Document Set 2—Supplier fulfillment advice (inbound)	0.4	0.5	0.3	41
Customer order via SSL (inbound)	1.0	1.0	1.0	100
Customer service request via e-mail (inbound)	0.4	0.4	0.9	55

Table 5-2 Example of a Weighted Factor Analysis Worksheet

Note: In the table, EDI stands for *electronic data interchange*, BOL stands for *bill of lading*, and SSL is Secure Sockets Layer

NIST SP 800-30, Risk Management for Information Technology Systems

Figura 2: Exemplo de Folha de Inventário com priorização

1.3. **Identificação de Risco** - Identificar e priorizar as ameaças

- Tomando todas as ameaças apreendidas, começa-se a avaliação de ameaça respondendo a algumas perguntas básicas, da seguinte maneira:
  - Quais ameaças representam um perigo para os ativos de uma organização no ambiente em questão?
  - Nem todas as ameaças têm o potencial de afectar todas as organizações. Embora seja improvável que inteira categorias de ameaças possa ser eliminada, a tal eliminação acelera o passos posteriores do processo.

1.3. **Identificação de Risco** - Identificar e priorizar as ameaças

- Tomando todas as ameaças apreendidas, começa-se a avaliação de ameaça respondendo a algumas perguntas básicas, da seguinte maneira:
  - Quais ameaças representam perigo para activos da organização num dado ambiente?
  - Quais ameaças representam o maior perigo para as informações da organização?
  - Quanto custaria para se recuperar de um ataque bem-sucedido?
  - Qual das ameaças exigiria o maior gasto para evitar?
- O processo de identificação do Risco culmina com a lista TVA [TPC].

2. Avaliação de Risco

- Depois da identificação dos ativos de informações da organização e as ameaças e vulnerabilidades, é possível avaliar o risco relativo de cada uma das vulnerabilidades. Este processo é chamado **Avaliação de Risco.**

Risco é **Probabilidade** da ocorrência da vulnerabilidade MULTIPLICADO POR **valor** do activo de informação MENOS a percentagem do risco mitigado pelos controlos actuais MAIS a **incerteza** do conhecimento actual da vulnerabilidade.

2. Avaliação de Risco

- Maiores fases da avaliação de risco:
  - Atribuir valor ao ataque sobre os activos;
  - Avaliar a probabilidade de ataque sobre vulnerabilidades;
  - Calcular o factor de risco relativo por activo;
  - Rever possíveis controlos; e
  - Documentar os resultados/conclusões

2. Avaliação de Risco

- **Probabilidade** é a probabilidade de uma vulnerabilidade específica ser objeto de um ataque bem-sucedido.
- Na avaliação de risco, atribui-se um valor numérico à probabilidade. O Instituto Nacional de Padrões e Tecnologia recomenda na Publicação Especial 800-30 a atribuição de um número entre 0,1 (baixo) e 1,0 (alto).
- Por exemplo, a probabilidade de um ativo ser atingido por um meteorito dentro de casa seria classificado com 0,1. No outro extremo, receber pelo menos um e-mail contendo um vírus ou worm no próximo ano seria avaliado como 1,0.

Asset	Asset Impact or Relative Value	Vulnerability	Vulnerability Likelihood	Risk-Rating Factor
Customer service request via e-mail (inbound)	55	E-mail disruption due to hardware failure	0.2	11
Customer order via SSL (inbound)	100	Lost orders due to Web server hardware failure	0.1	10
Customer order via SSL (inbound)	100	Lost orders due to Web server or ISP service failure	0.1	10
Customer service request via e-mail (inbound)	55	E-mail disruption due to SMTP mail relay attack	0.1	5.5
Customer service request via e-mail (inbound)	55	E-mail disruption due to ISP service failure	0.1	5.5
Customer order via SSL (inbound)	100	Lost orders due to Web server denial-of-service attack	0.025	2.5
Customer order via SSL (inbound)	100	Lost orders due to Web server software failure	0.01	1

Figura 3: Folha do Ranking de Risco de Vulnerabilidade

3.Controlo de Risco

- O Controlo de Risco é feito com base em cinco estratégias:
  - Defender;
  - Transferir;
  - Mitigar;
  - Aceitar; e
  - Encerrar.

3. Estratégia de Controlo de Risco - Defender

- A estratégia de controle de defesa tenta impedir a exploração da vulnerabilidade.
- Esta é a abordagem preferida e é realizada por meio do combate às ameaças, removendo vulnerabilidades de ativos, limitando o acesso a ativos e adicionando proteções de proteção.
- Existem três métodos comuns usados para defender: (1) Aplicação de política; (2) Educação e treinamento; e (3) Aplicação de tecnologia.

3. Estratégia de Controlo de Risco - Transferir

- A estratégia de controle de transferência tenta transferir o risco para outros ativos, outros processos ou outras organizações.
- Isso pode ser feito repensando como os serviços são oferecidos, revisando modelos de implantação, terceirizando para outras organizações, comprando seguros ou implementando contratos de serviços com provedores.

3. Estratégia de Controlo de Risco - Mitigar

- A estratégia de controle de mitigação tenta reduzir o impacto causado pela exploração da vulnerabilidade por meio de planeamento e preparação.
- Essa abordagem requer a criação de três tipos de planos: o plano de resposta a incidentes, o plano de recuperação de desastre e o plano de continuidade de negócios.
- Cada um desses planos depende da capacidade de detectar e responder a um ataque o mais rápido possível e depende da qualidade dos outros planos.

3. Estratégia de Controlo de Risco - Aceitar

- A estratégia de controle de aceitação é a escolha de não fazer nada para proteger uma vulnerabilidade e aceitar o resultado de sua exploração. Isso pode ou não ser uma decisão comercial consciente.
- Essa estratégia baseia-se na conclusão de que o custo de proteger um ativo não justifica os gastos com segurança.

3. Estratégia de Controlo de Risco - Encerrar

- A estratégia de controle de término direciona a organização a evitar as atividades de negócios que apresentam riscos incontroláveis.
- Ao terminar a atividade questionável, a organização reduz a exposição ao risco.

3. Selecção de Estratégia

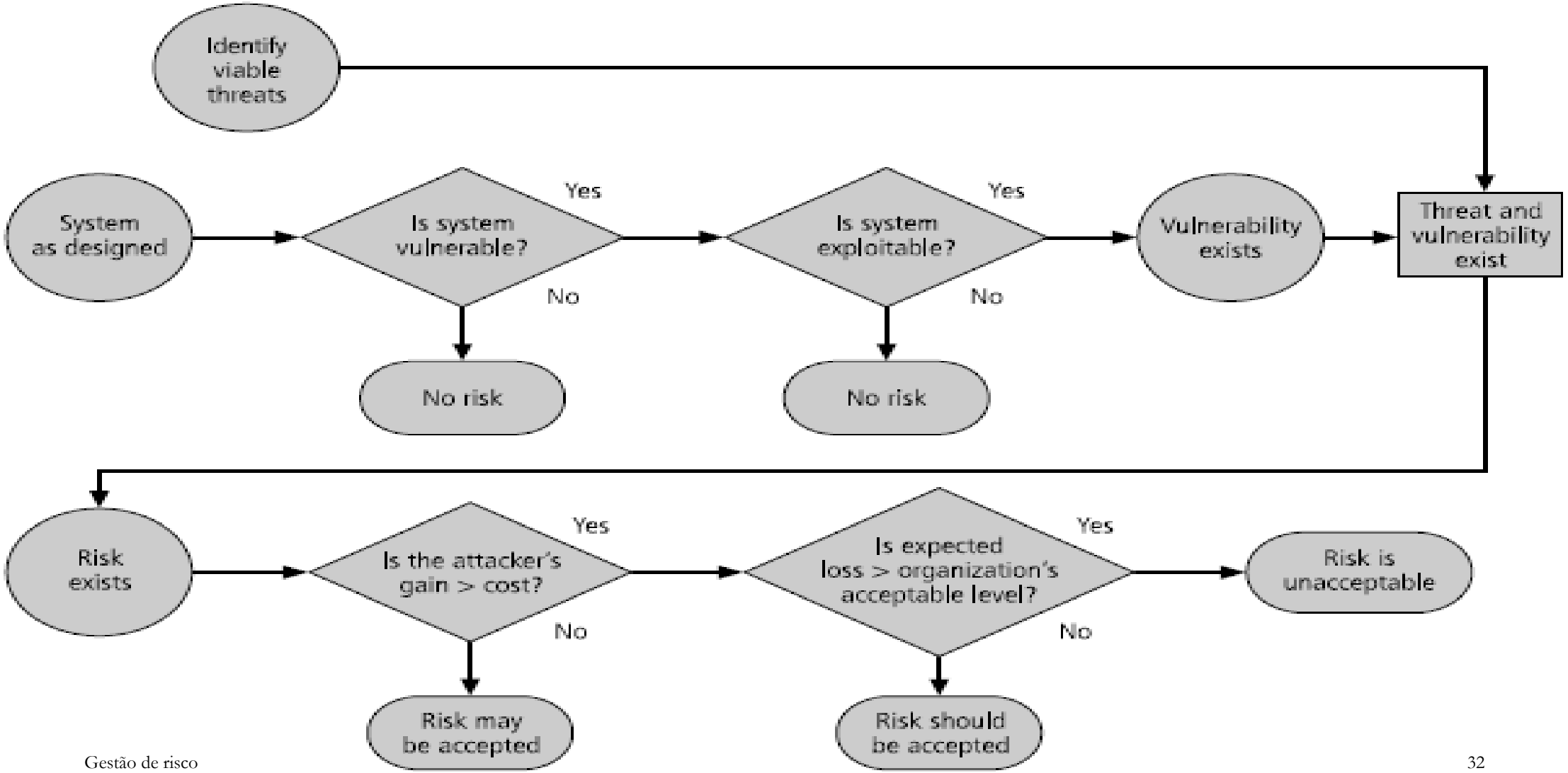


Figura 4: Pontos de Decisão para Tratamento de Risco

Análise de Custo-Benefício (CBA)

- CBA é uma técnica muito utilizada por organizações para determinar a vantagem de um controlo específico.
- Recomenda-se que as organizações iniciem a análise de custo-benefício avaliando o valor dos ativos de informação a serem protegidos e a perda de valor se esses ativos de informação forem comprometidos pela exploração de uma vulnerabilidade específica.

Análise de Custo-Benefício (CBA)

- É apenas senso comum que uma organização não deve gastar mais para proteger um ativo do que o património vale.
- O processo formal de tomada de decisão é chamado de **análise custo-benefício** ou **estudo de viabilidade económica**.
- Assim como é difícil determinar o valor da informação, também é difícil determinar o custo das salvaguardas.

Análise de Custo-Benefício (CBA)

Alguns dos itens que afetam o custo de um controlo ou salvaguarda incluem:

- **Custo de desenvolvimento ou aquisição** (custo de aquisição) de hardware, software e serviços;
- **Honorários de treinamento** (custo de treinamento de pessoal);
- **Custo de implementação** (custo para instalar, configurar e testar hardware, software e Serviços);
- **Custos de serviço** (taxas de fornecedores para manutenção e atualizações); e
- **Custo de manutenção** (despesa de mão-de-obra para verificar e testar, manter e atualizar).

Análise de Custo-Benefício (CBA)

Benefício	valor que uma organização realiza usando controlos para evitar perdas associadas a uma vulnerabilidade específica **(CBA)**
A avaliação de ativos	processo de atribuição de valor financeiro ou valor a cada ativo de informação
Expectativa de perda única (SLE)	cálculo do valor associado à perda mais provável de um ataque
Fator de Exposição (EF)	percentagem esperada de perda que ocorreria de um ataque em particular
	SLE = Valor do Activo * EF

Análise de Custo-Benefício (CBA)

Taxa de Ocorrência Anualizada (ARO).	ARO é simplesmente quantas vezes você espera um específico tipo de ataque para ocorrer ou como a **probabilidade de ocorrência de uma ameaça (num período em anos).**
Expectativa de Perda Anualizada (ALE)	determinar o potencial total perdido por risco
	ALE = SLE * ARO

CBA = ALE(anterior) - ALE(posterior) - ACS

Avaliação, Análise e Manutenção de Controlos de Risco

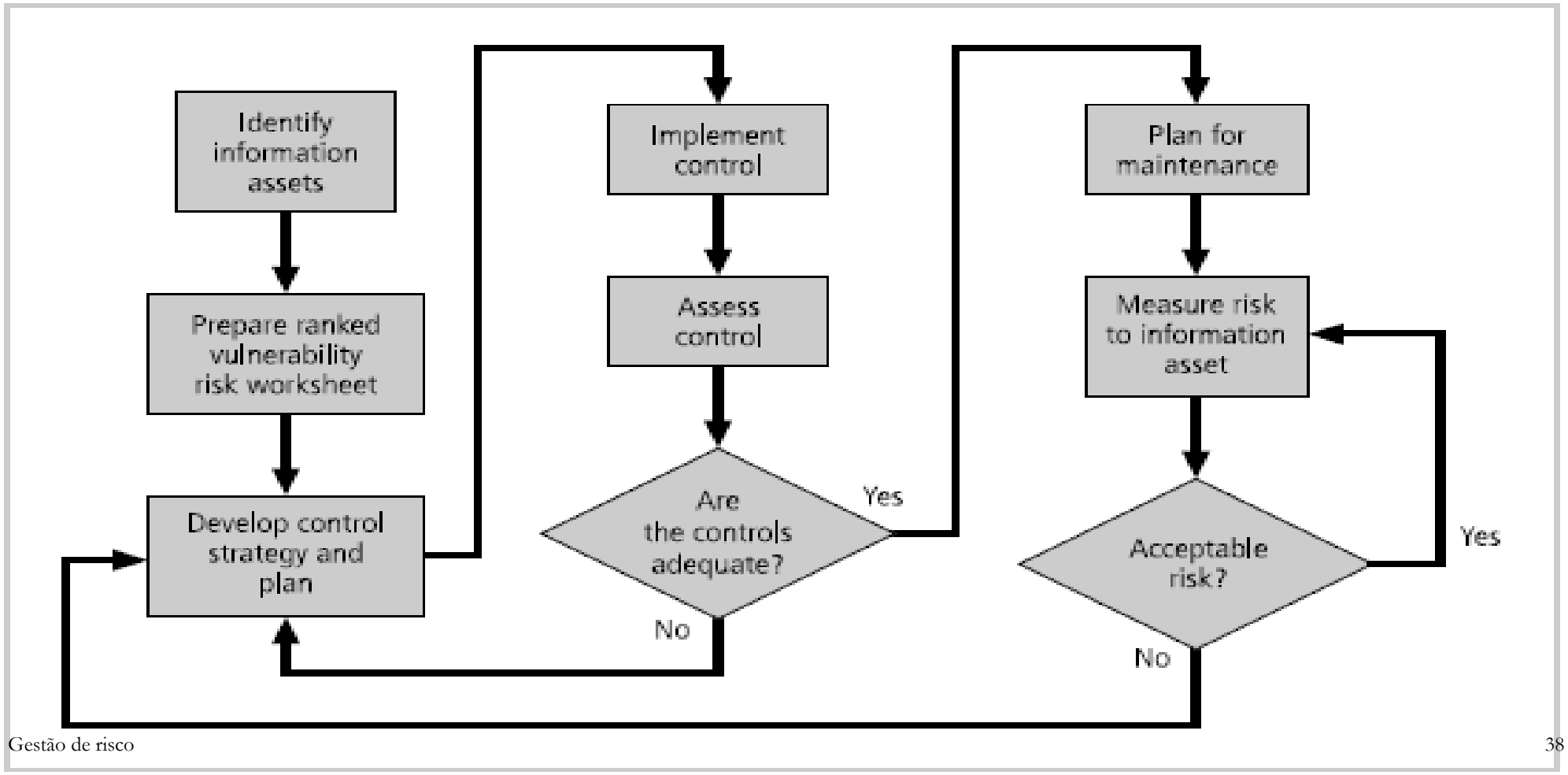


Figura 5: Ciclo de Controlo de Risco

Práticas quantitativas versus práticas qualitativas de controlo de risco

- As várias etapas descritas anteriormente foram realizadas usando valores ou estimativas reais, isto é, como uma **avaliação quantitativa**.
- No entanto, uma organização pode decidir que não pode colocar números específicos nesses valores.
- Felizmente, é possível repetir essas etapas usando um processo de avaliação, chamado **avaliação qualitativa**, que não usa medidas numéricas.

Práticas quantitativas versus práticas qualitativas de controlo de risco

- Por exemplo, em vez de colocar um valor de uma vez a cada 10 anos para o ARO, a organização poderia listar todos os possíveis ataques em um determinado conjunto de informações e classificar cada um pela probabilidade de ocorrência.
- Isso pode ser feito usando escalas em vez de estimativas específicas como: nenhuma chance de ocorrência, baixa, média, alta, até muito alta, representando uma ocorrência quase certa. As organizações podem, naturalmente, preferir outras escalas: A a Z, 0 a 10, 1 a 5 ou 0 a 20.

TPC

- Benchmarking e Melhores Práticas
- Problemas com a aplicação do benchmarking e melhores práticas
- Outros estudos de viabilidade

Bibliografia

- WHITMAN, M. & MATTORD, H. Principles of Information Security, 4º Edition, 2011.

Obrigado!