Instituto Politécnico de Setúbal

Escola Superior de Ciências Empresariais

IT Governance

Risco e Segurança dos SI no sector financeiro

Prova de Conceito no Regulador Português

Alexandre Barão

Dissertação apresentada para cumprimento dos requisitos necessários à obtenção do grau de

MESTRE em Sistemas de Informação Organizacionais

Orientador: Professor Coordenador Pedro Anunciação

Setúbal, 2015

INDICE

INDICE DE FIGURAS

INDICE DE TABELAS

LISTA DE SIGLAS E ABREVIATURAS

A/C	Ar-condicionado
ACL	Access Control List
BCP	Plano de Continuidade de Negócio
BD	Bases de Dados
BdP	Banco de Portugal
BITS	KEY RISK MEASUREMENT TOOL FOR INFORMATION SECURITY OPERATIONAL RISKS
CFO	Chief Financial Officer
CIA	Confidential, Integrity, Availability
CIT	Chief Information Technology
COBIT	Control Objectives for Information and related Technology
COO	Chief Operating Officer
COSO	*Committee of Sponsoring Organizations* of the Treadway Commission
DBA	Database Adminitrator
DRP	Plano de Desastre e Recuperação
ERM	Enterprise Risk Managment
ESCB	European System of Central Banks
FFIEC	Federal Financial Institutions Examination Council
GA	Gestor de Alterações
IEC	International Electrotechnical Commission
IRAM	Information Risk Analysis Methodology
IRM	Information Risk Managment
IS	Information Systems
ISF	Information Security Forum
ISO	International Organization for Standardization
ISO27002	Information technology -- Security techniques -- Code of practice for information security controls
IT	Information Techonology
ITGCs	Information Techonology General Controls
ITGI	IT Governance Institute
ITIL	Information Technology Infrastructure Library
NIST	National Institute of Standards and Technology
NPV	Net Present Value
ORM	Gestão de Risco Operacional
OS	Sistema Operativo
PA	Pedido de Alteração
PCAOB	Public Company Accounting Oversight Board

PID	Documento de Início de Projeto
PPSA	Avaliação de Segurança de Pré-Produção
PTR	Planto de Tratamento de Riscos
PwC	PricewaterhouseCoopers
RACF	Resource Access Control Facility
ROI	Return of Investment
SDLC	System Development Life Cycle
SEBC	Sistema Europeu de Bancos Centrais
SI	Sistema de Informação
SOX	Sarbanes Oxley
SU	Substitute User
TCO	Total Cost of ownership
TI	Tecnologias de Informação
UPS	*Uninterruptible Power Supply*
WCGW	What-Can-Go-Wrong

AGRADECIMENTOS

A elaboração deste trabalho de projeto, no âmbito do Mestrado em Sistemas de Informação Organizacionais, só foi possível graças ao apoio de inúmeras pessoas que me acompanharam ao longo deste percurso, nomeadamente aos meus colegas do grupo de trabalho do SEBC. A estes pretendo deixar o meu sincero agradecimento.

A todos o meu sincero bem-haja!

RESUMO

O trabalho de projeto de mestrado aplicado ao contexto do sector financeiro, nomeadamente o Sistema Europeu de Bancos Centrais, teve como objetivo analisar a atual metodologia de Information Risk Management (IRM), utilizada pelos bancos centrais na gestão da segurança dos sistemas de informação.

Nesta análise foi utilizada uma metodologia assente num focus group com sessões de brainstorming suportado por um guião de entrevista com questões semiestruturadas. Como resultado dessa análise foi possível identificar algumas oportunidades de melhoria no que respeita à metodologia IRM, nomeadamente:

- Atualização do standard da ISO27002:2005 para ISO27002:2013;
- Conceptualizar a metodologia com uma vertente de gestão de risco;
- Relacionar os sistemas de informação com os processos de negócio, pela identificação como o negócio é afetado pelos riscos dos sistemas de informação.

De forma breve estes foram os principais resultados, e os mesmos tornam-se críticos quando o sector financeiro, nomeadamente no âmbito do Sistema Europeu de Bancos Centrais, os processos de negócio tem uma grande dependência dos SI, e nesse sentido considera-se critico uma adequada gestão do risco associado.

Como principais benefícios esperados da proposta da metodologia de um processo de gestão de risco da informação (IRM) será providenciar uma metodologia objetiva e de fácil aplicação, no sentido de identificar os riscos associados aos sistemas de informação que possam afetar os processos de negócio (riscos de negócio). Em termos práticos visa facultar um meio para avaliar as medidas de segurança e identificar e selecionar os requisitos/ medidas de segurança que melhor mitigam o risco para o sistema de informação.

O seu objetivo será assegurar que a segurança da informação é tratada adequadamente em cada fase do ciclo-de-vida do sistema. Desenvolver a segurança em sistemas durante o seu desenvolvimento é mais eficaz e seguro, do que quando realizadas numa fase posterior ao seu desenvolvimento.

Palavras-chave: risco, criticidade, requisitos de segurança, ciclo de vida, catálogo

ABSTRACT

The Master's project work applied to the financial sector context, in particular the European System of Central Banks, aimed to examine the current methodology of Information Risk Management (IRM), used by central banks in the security management of information systems.

- In this analysis we used a methodology based on a focus group with brainstorming sessions supported by a semi-structured interview guide with questions. As a result of this analysis it was possible to identify some opportunities for improvement regarding the IRM methodology, including:update the standard from ISO27002:2005 to ISO27002:2013;
- Conceptualize the methodology with a risk management focus;
- Linking information systems with business processes by identifying how the business is impacted by the risks of information systems.

Briefly these were the main results, and they become critical when the financial sector in particular within the European System of Central Banks, business processes have a great dependence on SI, and in that sense it is considered critical an adequate risk management. Main benefits expected from the proposal of a process to manage information risk (IRM), will provide an objective and easily applicable methodology, to identify the risks associated with information systems that may affect the business processes (business risks). In practical terms it aims to provide a means to assess the security measures and identify and select requirements / security measures to better mitigate the risk to the information system.

Its goal will be to ensure that information security is handled appropriately at each stage of the system life-cycle. Building security systems during development is more efficient and secure than when carried out at a later stage the development.

Keywords: risk, criticality, security requirements, life cycle, baseline

INTRODUÇÃO

A oportunidade para o desenvolvimento deste trabalho surgiu na sequência da criação de um grupo de trabalho internacional, na sequência da atualização do standard de segurança ISO27002:2013, com especialistas de segurança de sistemas de informação, composto pelos seguintes bancos centrais da Alemanha, França, Luxemburgo, Bélgica, França, Espanha, Holanda, Itália, República Checa, Portugal e Banco Central Europeu.

Com a criação desse grupo foi aproveitada a oportunidade para criar um focus group e analisar a atual metodologia de Information Risk Management (IRM), como técnicas de trabalho foram efetuadas sessões de brainstorming com um guião de entrevista com questões semiestruturadas.

Com o objetivo de analisar a atual metodologia de Information Risk Management (IRM), utilizada pelos bancos centrais na gestão da segurança dos sistemas de informação, constatou-se da análise que a atual metodologia carecia de uma componente de gestão risco, verificando-se que havia a necessidade de identificar e definir novas fases para uma adequada gestão do risco associado aos sistemas de informação.

A proposta de modelo foi concebido com base em referenciais obtidos através da revisão da literatura, e da atual metodologia, quer das métricas e do normativo considerado adequado ao estudo desta problemática.

Numa perspetiva prática, este trabalho tem como objetivo propor um novo processo de gestão de risco para os sistemas de informação no âmbito do Sistema Europeu de Bancos Centrais, tendo como intuito a definição de orientações práticas sobre a gestão de risco ao longo das diferentes fases do ciclo-de-vida do sistema. A gestão de risco é um dos processos mais relevantes na segurança dos sistemas de informação, tendo como premissa a necessidade de controlar e minimizar os riscos dos sistemas de informação. Para que se efetive esta gestão é necessário que seja aplicado a todos os aspetos relevantes dos SI, onde quer que estes se encontrem.

A informação é um ativo tal como outros ativos comerciais importantes, é essencial para o negócio de uma organização e consequentemente precisa de ser protegida adequadamente. Isto é especialmente importante nos ambientes de negócio cada vez mais interligados. Como resultado desta crescente interconetividade, a informação é agora exposta a um número cada vez maior e uma maior variedade de ameaças e vulnerabilidades.

Considerando o impacto que o IT atualmente tem no negócio das empresas (resultado da automatização dos processos de negócio e sua dependência, temos:

- Naturalmente, o incremento do risco associado, uma vez que são a base para as operações;
- São fornecidos transversalmente pela organização, e não segregados por processos de negócio ou unidade de negócio;

- Consequente generalização e confiança depositada nos sistemas e IT, são necessários controlos sobre tais sistemas, independentemente da sua dimensão. Estes controlos gerais de IT geralmente incluem controlos sobre o ambiente de IT, operações, o acesso a programas e dados, desenvolvimento e manutenção de programas. Estes controlos em princípio, aplicam-se a sistemas que tenham sido identificados na avaliação de criticidade do sistema com impacto significativo.

Tendo em consideração os pontos supra, o objetivo será a definição de um processo de gestão de risco suficientemente abrangente e consistente, de modo a que as medidas de proteção sejam selecionadas e implementadas de forma oportuna, e que os riscos remanescentes sejam transparentes e expressamente aceites.

O público-alvo será as organizações económico-financeiras e os gestores responsáveis pela gestão de risco.

Os benefícios esperados com este trabalho são:

- Construir e manter uma "fotografia" dos riscos genéricos / específicos de IT;
- Permitir executar uma priorização das ações de mitigação do risco, o que pode requerer mudanças nas políticas e contribuir para um relatório representativo do risco de segurança da informação;
- Identificar os riscos associados com sistemas de informação que podem afetar os processos de negócio (riscos negócio);
- A aplicabilidade abrange ambos os sistemas em desenvolvimento (ou seja, projetos) e sistemas em operação (ou seja, alterações nos sistemas implementados).

1. Enquadramento Teórico

Em termos de enquadramento do IT Governance, será feito uma resuma, nomeadamente uma definição do conceito e uma breve descrição no que consiste e quais as áreas chave, destacando-se as que se relacionam com a gestão de risco, controlos de IT e segurança da informação. Considerando que serão estas que irão suportar a proposta para um processo de gestão de risco para os sistemas de informação.

1.1. IT Governance

No que respeita à governação de IT as principais definições do conceito, e que são seguidas pela maioria dos profissionais da área, é das principais consultoras internacionais, das quais se destaca:

De acordo com o IT Governance Institute (ITGI, 2003):

*A Governação de TI é definida, como o processo/ modelo para **gerir** e **controlar** a organização de modo a alcançar os objetivos através de **criação** de **valor**, enquanto balanceia os **riscos** versus o **retorno** sobre as IT e respetivos **processos**.*

De acordo com a PricewaterhouseCoopers em "IT Governance - Alinhar o IT com o negócio" (2014):

*A governação de IT providencia o framework e a capacidade para efetuar e implementar as decisões necessárias para **gerir**, **controlar** e **monitorizar** as IT com o negócio.*

De acordo com a (Gartner, 2015):

"IT governance (ITG) is defined as the processes that ensure the effective and efficient use of IT in enabling an organization to achieve its goals. IT demand governance (ITDG—what IT should work on) is the process by which organizations ensure the effective evaluation, selection, prioritization, and funding of competing IT investments; oversee their implementation; and extract (measurable) business benefits. ITDG is a business investment decision-making and oversight process, and it is a business management responsibility. IT supply-side governance (ITSG—how IT should do what it does) is concerned with ensuring that the IT organization operates in an effective, efficient and compliant fashion, and it is primarily a CIO responsibility."

A importância do IT Governance pode ser levantada pela necessidade de gerir o IT por:

- A responsabilidade não está atribuída, e as funções relativas aos projetos e serviços de IT não estão claramente definidas;
- A comunicação entre os utilizadores de IT e os fornecedores tem necessidade de ser melhorada e ser baseada numa parceria para as iniciativas de IT;

- Potencial *gap* entre o que o IT pensa e o que a gestão quer, e entre o que a gestão pensa e o que o IT é capaz de desenvolver;
- Necessidade de melhorar a compreensão do valor que é criado pelo IT, tanto de fornecedores internos como externos;
- Definição de métricas para garantir/medir que os objetivos pretendidos são atingidos;
- A administração tem necessidade de estar consciente de como a sua organização está a gerir o IT, comparativamente com os seus parceiros.

O IT Governance não é uma preocupação única das funções de IT. Numa visão integrada, faz parte da gestão de uma organização, mas com um foco específico na melhoria da gestão e no controlo das Tecnologias de Informação para o benefício dos stakeholders primários.

No que respeita às partes interessadas, nomeadamente stakeholders, de acordo com o (ITGI, 2003) podemos identificar:

- Gestão de Topo, tal como, Administração, Executiva e não Executiva, e principalmente CFO, COO, CIT;
- Responsáveis pelos investimentos e pelas relações públicas;
- Auditores Internos e Externos, e Reguladores;
- Gestão Intermédia de Negócio e de IT;
- Parceiros e fornecedores chave de negócio;
- Shareholders;
- Clientes.

As considerações a ter:

- Disponibilidade, segurança, e continuidade dos serviços de IT;
- Quantificação dos custos e do ROI;
- Qualidade e fiabilidade dos serviços – confiança;
- O IT não está a conseguir responder às necessidades do negócio;
- Identificação e gestão dos riscos de IT relacionados com o negócio;
- Competência e skills dos recursos humanos;
- Conformidade com requisitos legais, reguladores e contratuais;
- Agilidade e Capacidade de resposta à mudança.

Em última instância, é da responsabilidade da Administração assegurar que o IT é, em conjunto com outras atividades críticas, gerido adequadamente. Apesar de os princípios não serem

novos, atualmente as implementações requerem novas visões, dada a especial natureza do IT.

O IT Governance difunde a cultura, a organização, as políticas e práticas para a gestão e controlo de IT, pelas seguintes cinco áreas chave.

1.1.1. Domínios do IT Governance

De acordo com o Control Objectives for Information and Related Technology 4.1 (COBIT 4.1), pode-se definir a governação dos sistemas de informação em cinco fases:

1. **Strategic Alignment**

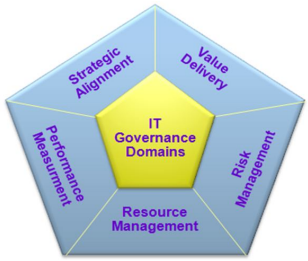


Figura 1- Domínios de IT Governance, adaptado de COBIT4.1

   - ❖ Garantir que existe alinhamento entre o plano de IT e de negócio;
   - ❖ Definição, manutenção e validação do valor proposto do IT;
   - ❖ Alinhamento das operações de IT com as operações da organização;
   - ❖ Estabelecer soluções colaborativas para os produtos e serviços, para acrescentar valor e criar uma posição competitiva;
   - ❖ Controlar os custos enquanto melhora a sua eficiência administrativa e a atividade de gestão.
   - ❖ Alinhamento da estratégia de IT com a estratégia de negócio;
   - ❖ Assegurar que o produto final do IT vai de encontro à Estratégia;
   - ❖ Coresponsabilidade de negócio e de IT;
   - ❖ Direcionar a estratégia de IT;
   - ❖ Assegurar que existe uma Cultura de abertura e colaboração entre o negócio, pelas unidades geográficas e funcionais da empresa.
2. **Value Delivery,** execução de ações através do "delivery cycle" de modo a alcançar o valor proposto, assegurando que o IT produz os benefícios pretendidos de encontro à estratégia, concentrando-se na otimização dos custos e no fornecimento do valor do IT, assegurando o controlo dos projetos e dos processos operacionais com base em práticas que permitam aumentar a probabilidade de sucesso (qualidade, risco, tempo, orçamento, custo, etc.).
   - ❖ Qualidade adequada, tempo e orçamento;
   - ❖ Definir valor, educar, envolver stakeholders e gerir perceções;
   - ❖ Monitorização do valor do IT para o negócio (requisitos de negócio & processo de alterações);

- ❖ Metodologia de gestão de projetos, com o negócio a ter papel de intervenção;
- ❖ Standards Tecnológicos.

3. **Risk Management,** a gestão estratégica deve estar consciencializada para o risco, reconhecimento de qual o risco aceitável e de quais os riscos significantes para a empresa; incluir as responsabilidades de gestão de risco nas operações da empresa e endereçar especificamente a salvaguarda dos recursos de IT, DRP, BCP.
   - ❖ **Reconhecimentos dos riscos de IT, baseada numa avaliação contínua e pró-ativa;**
   - ❖ Reconhecida por todos os stakeholders;
   - ❖ Definir responsabilidades e implementar a gestão de risco na organização;
   - ❖ Mitigação de risco gera eficiência de custos;
   - ❖ **Segurança da Informação.**
4. **Resource Management,** compreende a otimização do investimento, utilização e distribuição dos recursos e capacidades de IT (pessoas, aplicações, tecnologia, instalações, dados, etc.) respondendo às necessidades da empresa maximizando a eficiência dos recursos e otimizando os custos e especificamente direcionar-se na potencialização do conhecimento, da infraestrutura de IT, e identificando serviços que possam passar para outsourcer.
   - ❖ Inventários de hardware e software;
   - ❖ Procedimentos para treinar e manter especialistas;
   - ❖ Políticas para aquisição, claras e consistentes;
   - ❖ Infraestruturas standard e interoperacionais;
   - ❖ Gestão de níveis de serviço.
5. **Performance Measurement**, monitorização dos níveis de serviço e dos outputs do projeto, através da utilização de balanced scorecards que traduzem a estratégia na prática com objetivos mensuráveis, para além da contabilidade tradicional, quantificar os relacionamentos e os recursos de conhecimento base que são necessários para competir na sociedade da informação: foco no cliente, eficiência de processos e capacidade de aprender e crescer.
   - ❖ Definir e monitorizar métricas;
   - ❖ Relatórios de IT Balanced Scorecard;
   - ❖ Relatório de gestão do sistema que fornece input para a estratégia;
   - ❖ Alinhamento entre o negócio e o IT;
   - ❖ Providencia uma avaliação eficaz do (ROI, TCO, NPV…).

O IT Governance não é realizado pontualmente, nem é algo que seja conseguido através de um conjunto de regras. É essencial que exista um compromisso por parte da gestão estratégica para promover e incutir a melhor forma de enfrentar a gestão e o controlo do IT.

IT Governance é uma atividade que requer uma mentalidade de melhoria contínua e uma capacidade de resposta à mudança do ambiente de IT. O IT Governance pode ser incluído na metodologia de gestão da empresa, e dar suporte à integração dos novos requisitos legais e regulatórios relacionados com o Corporate Governance.

De modo sucinto podemos definir as cinco fases do IT Governance como:

1. **Strategic Alignment**

   Alinhamento com o negócio; providenciar soluções colaborativas.

2. **Value Delivery**

   Foco nos custos de IT e na criação de valor.

3. **Resource Management**

   Conhecimentos, infraestrutura e parceiros.

4. **Risk Management**

   Salvaguarda de recursos de IT, DRP, BCP.

5. **Performance Measurement**

   IT Scorecards.

1.1.2. Benefícios IT Governance

Eventualmente, poderão ser identificados investimentos necessários para melhorar e desenvolver as áreas/domínios do IT Governance. É importante que os potenciais benefícios dos investimentos sejam claramente identificados e comunicados, para que o investimento seja viável. Os benefícios esperados, poderão consequentemente ser utilizados como indicadores para medir o sucesso do projeto e para monitorização.

De acordo com o ITGI, são identificadas áreas que poderão beneficiar da eficiência da gestão no que respeita à governação das IT:

- Compreensão e Responsabilidade
  - Compreensão dos custos com IT, com os processos de IT, portfólio (projetos e serviços) de IT;
  - Definição das responsabilidades na tomada de decisão, e os relacionamentos entre os utilizadores e os fornecedores.
- Valor do ROI para os Stakeholders
  - Melhora a compreensão dos custos de IT, e qual o seu input para cada ROI;

- ❖ Perceção de que para reduzir os custos são necessários investimentos;
- ❖ Stakeholders conseguem percecionar o valor retornado da gestão do risco;
- ❖ Contributo importante para o retorno dos investimentos dos stakeholders;
- ❖ Promove e protege a reputação e imagem.

- ➢ Oportunidades e Parcerias
  - ❖ Suportar e aproveitar oportunidades que poderão não estar a ter atenção nem sponsorship;
  - ❖ Posicionamento do IT como parceiro do negócio (e definir que tipo de parceria de negócio o IT irá desempenhar);
  - ❖ Facilita joint-ventures com outras empresas;
  - ❖ Facilita a criação de relações de negócio com parceiros chave tecnológicos (vendedores e fornecedores);
  - ❖ Definição de uma metodologia sólida para gerir o risco;
  - ❖ Solicita a participação do IT na definição da estratégia de negócio (o que resultará na definição da própria estratégia Tecnológica) e vice-versa;
  - ❖ Melhora a capacidade de resposta às mudanças e às oportunidades criadas pelo mercado.
- ➢ Melhoria da Performance
  - ❖ Identifica quais os projetos ou serviços de IT que estão a suportar o negócio normalmente, e aqueles que se pretende que acrescentem valor;
  - ❖ Quanto mais compreensível for, maior será o aumento da performance, salientando que a performance seja constantemente melhorada;
  - ❖ O foco na melhoria contínua da performance, leva a que sejam adotadas as melhores práticas do mercado;
  - ❖ Evitar custos desnecessários – os custos são mapeados com os objetivos de negócio;
  - ❖ Capacidade de efetuar benchmark.
- ➢ Compliance Externa
  - ❖ Metodologia integrada que permite responder aos requisitos legais e reguladores.

1.1.3. IT Governance "Best Practice"

No planeamento de iniciativas de IT Governance, é sugerido ter em consideração as seguintes "Best Practices", ver figura 2. Para o âmbito do trabalho a ser desenvolvido e de entre as metodologias referenciadas, destacamos a ISO27002, o COSO, o IT Risk Framework e ISO31000, que serão utilizadas como input para o desenvolvimento da metodologia a ser proposta.

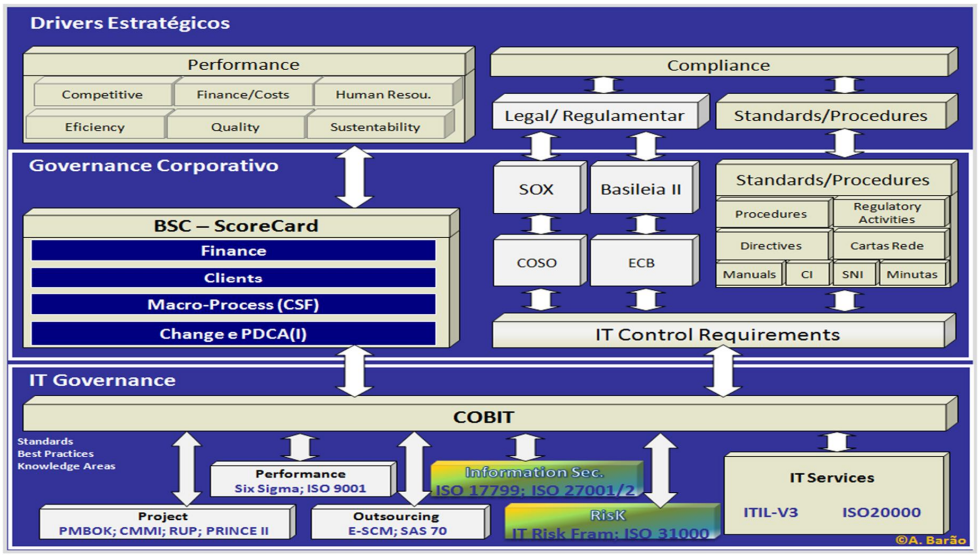


Figura 2 - IT Governance "Best Practice"

De acordo com o COBIT4.1 é necessário ter em consideração os seguintes fatores críticos de sucesso.

- Deve ser adotada uma metodologia
  - Alinhamento entre o negócio e o IT na definição e controlo de requisitos;
  - O IT terá que desenvolver um modelo de controlo aplicável a todas as unidades/divisões da empresa;
  - Recomenda-se a implementação de um comité para definir, acordar, e monitorizar as diretrizes/políticas, etc.;
  - É fundamental que exista uma visão consolidada e partilhada do IT Governance e que seja compreensível por todos na empresa;
  - Deve ser facilmente compreendida (aprovada) pelos stakeholders sobre o que deve estar dentro do âmbito do IT Governance.
- O compromisso da Gestão de Topo, é suportado por uma definição clara de responsabilidades
  - O IT Governance para ter sucesso na prática necessita de ser emanado e ter a

direção da administração;

- ❖ Garantir que as responsabilidades e os deveres no que se reporta ao negócio e ao IT estejam clarificados.

- ➢ É essencial que exista um consenso respeitante ao IT Governance e à Framework de Controlo
  - ❖ Contudo, poderão surgir desafios e retrocessos, o que exigirá consensos, a definição de uma Framework para o IT Governance que deverá ser acordada, de modo a que seja possível gerir os processos e os controlos de IT de forma efetiva;
  - ❖ O processo de IT Governance deverá estar integrado com as demais práticas de administração, de modo a que o processo não se torne unicamente do IT;
  - ❖ Os objetivos e as práticas deverão ser promovidos através de campanhas de consciencialização e comunicação, para que possam ser facilmente compreendidas;
  - ❖ Deverão ser definidos métodos de motivação para adesão à Framework;
  - ❖ Ter atenção, a eventualidade de surgirem organizações de IT informais, de forma a assegurar que exista um equilíbrio entre as políticas que são emanadas centralmente e as práticas que são implementadas localmente;
  - ❖ Evitar burocracia.
- ➢ É necessário construir um sentimento de confiança sobre a função de IT perante os demais (in house e/ou externa)
  - ❖ Para que o IT Governance possa funcionar efetivamente é necessário que os fornecedores de serviços de IT, e de know-how estejam alinhados com os requisitos do cliente, que sejam vistos como profissionais e especialistas. Deve ser estabelecida/construída uma relação de confiança, utilizando os meios à disposição, campanhas de sensibilização, workshops, considerando a intervenção do Diretor de IT como intermediário entre ambiente de IT e de negócio.
- ➢ Sistemas de Monitorização asseguram que os objetivos são controlados e monitorizados
  - ❖ A definição de IT scorecards para suportar e reforçar o cumprimento dos objetivos;
  - ❖ A definição de um conjunto de métricas iniciais poderá ser indicador de um sentimento de consciencialização, e consequentemente poderá ser despoletada um programa de IT Governance;
  - ❖ As métricas a serem definidas deverão estar numa perspetiva de negócio e

aprovadas pelos stakeholders.

- Foco nos custos
  - Após a implementação das melhores práticas de IT Governance, é provável que sejam identificadas oportunidades para redução de custos. Estas oportunidades serão importantes para suportar o desencadear de novas iniciativas de melhoria.

1.2. Gestão de Risco

1.2.1. Gestão de Risco da Empresa

A gestão de risco da empresa (ERM) representa uma mudança fundamental na maneira como os negócios devem abordar o risco. Enquanto a economia se torna mais dirigida para os serviços e orientada globalmente, os negócios não se podem dar ao luxo de deixar novas áreas imprevistas de risco permanecerem não identificadas.

As flutuações da moeda corrente, os recursos humanos em países estrangeiros, o desaparecimento de canais de distribuição, a administração incorporada, e a dependência sem precedentes na tecnologia, são apenas alguns dos novos riscos que os negócios devem avaliar.

Muitas organizações estão a escolher implementar um processo de gestão do risco empresarial para assegurar-se de que uma aproximação uniforme para identificar, medir, avaliar e controlar o risco é utilizado através da organização. Ao adotar esta aproximação pró-ativa para controlar o risco, as organizações podem mover-se de uma aproximação da gestão do "silo" para uma integração mais profunda dos seus vários negócios.

A gestão de risco empresarial (ERM) é uma aproximação estruturada e disciplinada para controlar o risco. ERM alinha as estratégias, processos, tecnologia e conhecimento da organização com a finalidade de melhorar a sua habilidade de avaliar e controlar, globalmente a empresa, as incertezas que ela enfrenta enquanto cria valor. Uma potencialidade da gestão de risco da empresa é aumentar a sensibilidade ao risco da organização e reduzir as barreiras funcionais, departamentais e culturais inevitáveis que existem na maioria das organizações. O ERM é integrado, olhando em frente e com uma abordagem por processo – orientada para controlar todos os riscos chave de negócio e as oportunidades – não apenas os financeiros – com a intenção de maximizar o valor para a empresa como um todo.

1.2.2. Definição de COSO-ERM

Em termos de enquadramento histórico, em 1992 o Committee of Sponsoring Organizations of the Treadway Commission (COSO) produziu a Framework Integrada de Controlo Interno, para ajudar as organizações a avaliar e a desenvolver os seus sistemas de controlo interno. Desde essa altura a framework tem sido reconhecida pelos organismos que estabelecem as normas reguladoras como uma Framework compreensiva para avaliar o ambiente de controlo interno.

Segundo o Committee of Sponsoring Organizations of the Treadway Commission (COSO, 2004):

A gestão do risco empresarial é um processo realizado pelo conselho de administração, pela gestão, por todos os colaboradores operacionais executantes e participantes, aplicado no ambiente estratégico e através da empresa, planeado para identificar eventos potenciais que podem afetar a entidade na gestão de riscos que se encontram dentro do desejo de risco, para proporcionar uma segurança razoável em relação à realização dos objetivos da entidade.

De certo modo reflete um conjunto de conceitos fundamentais:

- **Um processo**

  A ERM não é um evento nem uma circunstância, mas uma série de ações que se espalham por todas as atividades de uma organização. As ações são sentidas em toda a parte e são inerentes na forma como a gestão desenvolve o negócio.

- **Realizado pelas pessoas**

  A gestão do risco empresarial é realizada por uma comissão de diretores, gestores e outros colaboradores. É concretizada pelas pessoas de uma organização, pelo que elas fazem e dizem.

- **Aplicado no ambiente estratégico**

  Uma entidade define a missão, visão e estabelece os objetivos estratégicos para alcançar a missão e visão. Por outro lado define objetivos relacionados que espera alcançar, fluindo da estratégia, para as unidades de negócio, divisões e processos. No ambiente estratégico, a gestão considera o risco relativo a estratégias alternativas.

- **Aplicado através da empresa**

  Para ter sucesso na aplicação da gestão do risco, uma entidade deve considerar o âmbito de todas as atividades. A gestão do risco considera atividades a todos os níveis da organização, desde o plano estratégico e distribuição de recursos, as atividades das unidades de negócio tais como marketing e recursos humanos, e processos de negócio como produção, logística, vendas e efetuar a revisão do novo crédito ao cliente.

- **Planeado para Identificar Potenciais Eventos**

  É planeado para identificar potenciais eventos que afetam a entidade, e para gerir o risco dentro do desejo de risco.

  A gestão identifica potenciais eventos que afetam a capacidade para implementar com sucesso a estratégia e alcançar os objetivos. Eventos com potencial impacto negativo representam risco, o qual requer avaliação e resposta por parte da gestão. Eventos com impacto potencialmente positivo podem superar os impactos negativos ou representar oportunidades. A gestão encaminha as oportunidades para a estratégia e para o processo de definição de objetivos. Uma variedade de fatores internos e externos dá origem a eventos.

Quando identificados potenciais eventos, a gestão considera o âmbito total da organização. A gestão considera o contexto dentro do qual a entidade opera e a sua tolerância de risco.

- **Proporciona uma segurança razoável**

  Uma gestão do risco empresarial bem planeada e funcional pode proporcionar à gestão e à comissão de diretores uma segurança razoável respeitante à realização dos objetivos da entidade.

- **Realização dos objetivos**

  Uma gestão do risco eficiente e eficaz proporciona uma segurança razoável para a realização dos objetivos relacionados com a fidedignidade do relatório e em conformidade com leis e regulamentos. O alcançar destes objetivos está dentro do controle da entidade e depende da forma como estas atividades relacionadas são executadas.

Tendo em consideração os conceitos fundamentais o objetivo da gestão de risco é suportar a criação de valor.

O valor é criado, preservado ou gasto através das diferentes decisões de gestão do cenário estratégico para operar a empresa diariamente. Inerente às decisões está o reconhecimento do risco e da oportunidade, exigindo que a gestão considere os ambientes interno e externo, use eficazmente os recursos preciosos e equilibre/ajuste as atividades para mudar as circunstâncias.

Para as empresas, os acionistas percebem o valor quando reconhecem a criação de valor a partir do crescimento da partilha de valor. Para as entidades governamentais, o valor é percebido quando os constituintes reconhecem receber serviços de valor a um custo aceitável. “Stakeholders” de entidades não lucrativas percebem o valor quando reconhecem receber benefícios sociais. A gestão do risco empresarial facilita a capacidade de gestão para criar valor sustentável e comunicar o valor criado aos “Stakeholders”.

A gestão do risco empresarial é um processo, realizado pelo conselho de administração, gestão e outro pessoal, aplicado à estratégia e através da empresa, planeado para identificar potenciais eventos que podem afetar a entidade, e gerir o risco para estar dentro do desejo de risco da entidade, para proporcionar uma garantia em relação à realização dos objetivos da entidade. A gestão do risco empresarial consiste em oito componentes inter-relacionados, que complementam o modo como a gestão gere a empresa e estão integrados com outros processos de gestão. Os componentes estão ligados e servem para determinar se a gestão do risco empresarial é eficaz e eficiente.

Um dos objetivos desta estrutura é ajudar a gestão do negócio e outras entidades a lidarem com os riscos inerentes à realização dos objetivos. Mas a ERM tem significados distintos para diferentes pessoas. A grande variedade de significados evita um entendimento comum da ERM. Um objetivo importante é integrar vários conceitos de gestão de risco na metodologia que vai

albergar a maioria das visões e providenciar um ponto de partida para entidades individuais avaliando e melhorando a ERM, para futuras iniciativas e regras que constroem a estrutura e para a educação.

Na metodologia COSO usada na avaliação do Controlo Interno, destaca-se a componente de Avaliação do Risco.

A metodologia integra 3 componentes distintas – Processos, Estrutura Organizacional e Controlos

- **Processos:**
  - Estratégicos;
  - Operações;
  - Relatórios;
  - Compliance.
- **Estrutura Organizacional**:
  - Organização;
  - Divisões;
  - Unidades de Negócio;
  - Subsidiárias
- **Os controlos relacionam-se com:**

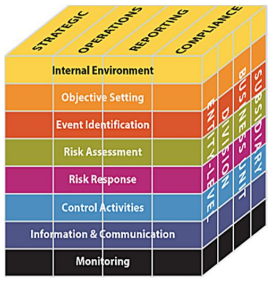


Figura 3 - COSO-ERM, adaptado

Formatted: Font: (Default) Arial

1. Ambiente de Controlo

O ambiente interno influencia a consciência de risco das pessoas, e é a fundação para todas as outras componentes da gestão do risco empresarial, proporcionando disciplina e estrutura. Os fatores do ambiente interno incluem: a filosofia da gestão do risco; o seu desejo de risco e cultura de risco; supervisão do conselho de administração; integridade, valores éticos e competência das pessoas da entidade; filosofia de gestão e estilo operante; o modo como a gestão define a autoridade e responsabilidade e organiza e desenvolve os seus colaboradores.

2. Estabelecimentos de Objetivos:

Qualquer entidade enfrenta diversos riscos de fontes internas e externas, e uma pré-condição para identificação eficaz de eventos, avaliação de risco e resposta é estabelecer objetivos ligados a diferentes níveis e internamente consistentes. Os objetivos são estabelecidos no nível estratégico, estabelecendo uma base para operações, relatório, e conformidade com objetivos. Objetivos estão alinhados com o desejo de risco da entidade, o qual dirige os níveis de tolerância de risco para as atividades da entidade.

O cenário dos objetivos é pré – condição para identificação do evento; avaliação do risco e resposta ao risco. Deve haver em primeiro lugar objetivos, antes da gestão identificar os riscos

para a sua realização e executar ações necessárias para gerir os riscos.

3. Identificação de eventos:

A gestão identifica potenciais eventos que afetam a capacidade para implementar com sucesso a estratégia e alcançar os objetivos. Eventos com potencial impacto negativo representam risco, os quais requerem avaliação e resposta por parte da gestão. Eventos com impacto potencialmente positivo podem superar os impactos negativos ou representar oportunidades. A gestão encaminha as oportunidades para a estratégia e para o processo de definição de objetivos. Uma variedade de fatores internos e externos dão origem a eventos. Quando identificados potenciais eventos, a gestão considera o âmbito total da organização. A gestão considera o contexto dentro do qual a entidade opera e a sua tolerância de risco.

- ***Definição de Evento***

Um evento é um incidente ou ocorrência emanada de fontes internas ou externas que podem afetar a implementação estratégica ou a realização dos objetivos. Os eventos podem ter um impacto positivo ou negativo ou ambos.

Como parte da identificação de eventos, a gestão reconhece que a incerteza existe, mas não sabe quando um evento vai ocorrer, ou se o seu resultado vai acontecer. A gestão inicialmente considera uma variedade de potenciais eventos – afetados por ambos os fatores internos e externos – sem necessariamente focar-se em se os impactos são positivos ou negativos.

Potenciais eventos variam do óbvio para o obscuro, e os potenciais efeitos do significante para o insignificante. Para evitar negligenciar eventos relevantes, a fase da identificação é melhor estar aparte da avaliação da probabilidade do evento ocorrer, o qual é o tópico da Avaliação do Risco.

4. Avaliação do Risco

A avaliação do risco permite a uma entidade considerar a extensão para a qual os potenciais eventos podem ter um impacto na realização dos objetivos. A gestão deve avaliar os eventos em duas perspetivas – probabilidade e impacto – e por norma usar uma combinação de métodos qualitativos e quantitativos. O impacto positivo ou negativo de potenciais eventos deve ser analisado, individualmente ou por categoria, através da entidade. Eventos potencialmente negativos são avaliados em ambas as bases de risco inerente e residual.

- ***Estimativa da probabilidade e impacto***

A incerteza de eventos potenciais é avaliada a partir de duas perspetivas: probabilidade e impacto. A probabilidade representa a possibilidade de um dado evento ocorrer, enquanto o impacto representa o seu efeito. Algumas vezes as palavras têm conotações específicas: probabilidade indica a possibilidade de um dado evento ocorrer em termos qualitativos tais como alta, média e baixa, ou outras escalas de julgamento, uma vez que a probabilidade pode ser usada para expressar medidas quantitativas como uma percentagem, frequência de

ocorrência, ou outras métricas.

- ***Contexto para a avaliação do risco***

Fatores internos e externos influenciam quais os eventos que podem ocorrer, como discutido no tópico anterior, e para que dimensão de eventos poderá afetar o alcançar de objetivos de uma entidade. Na avaliação do risco, a gestão considera o Mix de potenciais eventos futuros, relevantes para a entidade e para as atividades.

- ***Correlação de eventos***

A gestão pode avaliar como os eventos se correlacionam, onde sequências combinadas de eventos interagem para criar significativas diferenças nas probabilidades ou nos impactos. Enquanto o impacto de um evento pode ser pequeno, uma sequência de eventos pode ter um impacto significante. A gestão pode usar testes de tensão "stress tests" para avaliar o impacto de eventos extremos e usar o quadro de análise para avaliar os efeitos de múltiplos eventos. Quando os eventos potenciais não são diretamente relacionados, a gestão avalia-os individualmente.

Quando os riscos podem ocorrer em múltiplas unidades de negócio, a gestão avalia-os e coloca-os em categorias comuns. Ver as relações da probabilidade e do impacto de riscos, é uma responsabilidade da gestão.

- ***Técnicas e metodologia qualitativa e quantitativa***

A metodologia de avaliação do risco de uma entidade compreende a combinação de técnicas qualitativas e quantitativas. As técnicas quantitativas são mais precisas e são usadas nas atividades sofisticadas e mais complexas, para complementar as técnicas qualitativas.

As técnicas de avaliação quantitativas exigem alto grau de esforço e rigor. Algumas vezes utiliza-se modelos matemáticos.

- ***Exemplos de técnicas quantitativas de avaliação do risco***

Benchmarking – um processo colaborativo entre um grupo de entidades, benchmarking foca eventos específicos ou processos, compara medidas e resultados usando métricas comuns, e identifica oportunidades de melhoria. Dados sobre os eventos, processos e medidas são desenvolvidos para comparar a performance;

Modelos probabilísticos – estes modelos associam um conjunto de eventos e o resultado do impacto e a probabilidade desses eventos baseados em certas suposições. A probabilidade e o impacto são avaliados com base em dados históricos ou com base nas suposições de comportamento futuro;

Modelos não probabilísticos – estes modelos usam suposições subjetivas na estimativa do impacto dos eventos sem quantificar uma probabilidade associada. Avaliar o impacto dos eventos é baseado em dados históricos ou simulados e presunções de comportamentos futuros.

Para obter consenso na definição do impacto e probabilidade, usando **técnicas de avaliação qualitativa**, as entidades podem usar as mesmas abordagens da identificação de eventos, tais como entrevistas e Workshops. O processo de auto – avaliação de um risco, capta o parecer dos participantes sobre a probabilidade e o impacto de eventos futuros, usando escalas descritivas ou numéricas.

- ***Relaciona os horizontes de tempo e objetivos***

Porque os riscos são avaliados no contexto da estratégia e dos objetivos. A entidade tende a focar os riscos de curto e médio prazo. Contudo, alguns elementos da estratégia e objetivos são de longo prazo. Como resultado, a gestão precisa de estar informada e não ignorar os riscos distanciados.

- ***Risco residual e risco inerente***

A gestão considera ambos os riscos inerentes e residuais. Inerente, é o risco que uma entidade pode "sofrer" na ausência de ações, por parte da gestão, para alterar a probabilidade ou o impacto. Residual, é o risco que fica depois de a gestão responder ao risco.

Na avaliação do risco, a gestão considera o impacto de potenciais eventos quer esperados quer não esperados. Muitos eventos são rotina e recorrentes, e eles constam dos programas da gestão e dos orçamentos operacionais. Outros são inesperados, têm uma baixa probabilidade de ocorrer mas podem ter um impacto potencial significativo e são respondidos separadamente. Ambos os riscos, e porque há a incerteza, podem afetar a implementação estratégica e a realização dos objetivos. A gestão avalia o risco de todos os eventos potenciais, que parece que venham a ter impacto na entidade. A avaliação é aplicada em primeiro lugar nos riscos inerentes. Uma vez que as respostas são desenvolvidas, a gestão usa as técnicas de avaliação para determinar o risco residual.

5. Respostas ao Risco

Tendo avaliações de riscos relevantes, a gestão determina como vai responder. As respostas incluem evitar, reduzir, partilhar e aceitar o risco. Ao considerar estas respostas, a gestão considera custos e benefícios, e seleciona a resposta que traz probabilidade e impacto esperado dentro da tolerância do risco desejado.

- ***Avaliar possíveis respostas ao risco***

Os riscos inerentes são analisados e as respostas avaliadas com o intuito de alcançar um risco residual alinhado com as tolerâncias de risco da entidade. Alguma das inúmeras respostas pode trazer o risco residual em linha com a tolerância de risco, e algumas vezes uma combinação de respostas fornece o resultado ótimo. Similarmente, certas respostas vão afetar o risco dos potenciais eventos. Dado que as respostas ao risco podem destinar-se a múltiplos riscos, a gestão pode descobrir que medidas/ações adicionais não são autorizadas. Procedimentos existentes podem ser suficientes ou podem necessitar de serem melhor executados. A gestão considera como as respostas individuais ou combinadas, interagem

para afetar eventos potenciais.

- ***Avaliar o efeito da resposta na probabilidade e impacto***

Na avaliação das opções de resposta, a gestão considera o efeito em ambas as probabilidades de risco e do impacto, e entende que a resposta pode afetar a probabilidade e o impacto de modo diferente. A resposta potencial para avaliar a probabilidade e o impacto pode considerar eventos passados e tendências, e cenários potenciais futuros. Ao avaliar respostas alternativas, a gestão determina o seu potencial efeito usando a mesma unidade de medida para o objetivo e os riscos associados como estabelecido na componente avaliação do risco.

- ***Avaliação do custo versus benefícios***

Os recursos têm sempre constrangimentos, e as entidades devem sempre considerar os custos e benefícios relativos de opções alternativas de resposta ao risco. Faz-se a avaliação dos custos diretos, indiretos e algumas entidades consideram ainda o custo de oportunidade.

Pode ser difícil quantificar os custos relacionados com o tempo e o esforço ou gerir certos fatores internos como o compromisso da gestão para com os valores éticos, a competência dos empregados que interpretam a identificação do evento e avaliam o risco. Também pode ser difícil captar informação externa, como inteligência de mercado, envolvendo as preferências dos consumidores.

Os benefícios podem ter uma avaliação subjetiva. Por exemplo, os benefícios de um programa de treino eficaz são geralmente evidentes, mas difíceis de quantificar.

Enquanto os desafios na avaliação de custos e benefícios existirem, a análise deve ser efetuada a um nível suficiente para que se possa avaliar as respostas ao risco numa base individual ou de portfólio. Algumas entidades podem escolher avaliar as respostas ao risco em termos tais como capital adicional exigido – por exemplo, retorno do investimento (ROI) ou capital de risco – e podem considerar matérias como a inflação, taxas de desconto e análise sensíveis.

- ***Oportunidades nas opções de resposta***

São eventos com impacto potencial positivo, e são canalizados para a estratégia ou objetivos. Exemplo: é a resposta criativa por parte de uma companhia de seguros ao elevado número de acidentes em certa intersecção de estrada – decidiu financiar a melhoria das luzes do semáforo de modo a ficarem mais realçadas, reduzindo as queixas de acidentes e melhorando as margens.

- ***Respostas selecionadas***

Uma vez que as respostas alternativas ao risco são avaliadas, a gestão decide como gerir o risco. Uma gestão do risco eficaz e eficiente, exige que a gestão selecione a resposta ou combinação de respostas que antecipam a probabilidade e o impacto dentro da tolerância do

risco.

Uma vez selecionada a resposta, é necessário desenvolver um plano de implementação para executar a resposta. Adicionalmente, são necessários procedimentos para a implementação eficaz e eficiente das ações. Estes procedimentos representam Controlo das Atividades.

A gestão reconhece que algum nível do risco residual continuará a existir, não somente por que os recursos são limitados, mas também dado a uma certa incerteza futura e limitações inerentes em todas as atividades.

- ***Portfólio view***

O gestor responsável por cada departamento, função ou unidade de negócio desenvolve a avaliação do risco e a resposta ao risco para essa unidade. Esta visão reflete o perfil do risco da unidade relativo aos seus objetivos e tolerâncias de risco.

Com a visão dos riscos em unidades individuais, a gestão sénior fica com o portfólio view e pode determinar se o perfil do risco da entidade é compatível com o desejo de risco relativo aos seus objetivos. Apesar do risco de cada unidade estar dentro da tolerância de risco da unidade, juntos, os riscos podem exceder o desejo de risco da entidade. Se o Portfólio do risco é menor que o desejo de risco da entidade, a gestão deve motivar os gestores das unidades de negócio para aceitarem um risco maior em áreas alvo para melhorar o crescimento da entidade e o retorno.

Ao estabelecer um portfólio view das respostas ao risco, a gestão reconhecerá a diversidade das respostas selecionadas e o efeito de múltiplas respostas nas tolerâncias de risco da entidade. Quando os potenciais eventos não estão diretamente relacionados, a gestão deve avaliar o efeito das suas respostas ao risco nesses eventos individualmente e depois criar um compósito ou um Portfólio view. Quando riscos similares existem em múltiplas unidades de negócio, a gestão pode decidir avaliar o efeito das respostas ao risco num tipo particular ou categoria de eventos, e depois fazer o Portfólio view.

6. Atividades de Controlo

- ***Políticas e procedimentos***

As atividades de controlo envolvem 2 elementos: a política para definir o que fazer e procedimentos para realizar a política. A política pode ser transmitida oralmente, quando já é uma prática, e por escrito.

Um procedimento não vai ser útil, se executado mecanicamente e sem consciência, continuando a focar-se em condições para a qual a política é dirigida. É essencial que condições identificadas como resultado de um procedimento sejam investigadas e tomadas as apropriadas ações corretivas. Seguidamente as ações podem variar dependendo do tamanho e da estrutura de uma empresa.

- ***Controlos sobre sistemas de informação***

Há 2 grupos de atividades de controlo de sistemas de informação:

- Controlos gerais – aplicam-se a todos os sistemas de informação e assegura a sua continuidade;
- Controlos aplicacionais – incluem os passos automatizados dentro do software aplicacional para controlar a aplicação tecnológica.

Combinados com os controlos manuais do processo, quando necessário, aqueles controlos asseguram integralidade, exatidão e validade da informação.

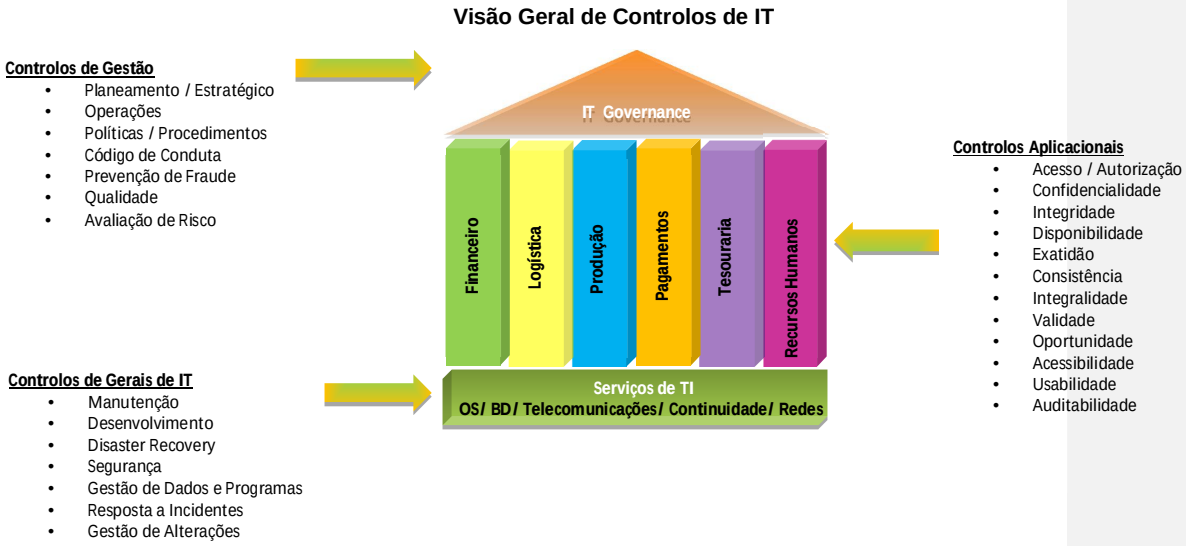


Figura 4 - "House of IT Controls", adaptado[1]

7. *Informação e Comunicação*

A informação pertinente é identificada, capturada e comunicada num formato e período de tempo que permite às pessoas realizar as suas atividades.

Sistemas de informação usados internamente geram dados e informação (sobre eventos externos, atividades e condições) fornecendo informação para a gestão de risco, e produzindo informação para decisões relativas aos objetivos. A comunicação eficaz e eficiente também ocorre top-down, bottom-up e atravessando a organização.

[1] Fonte: http://www.metricstream.com/insights/sox_it_controls.htm

- **Informação**

Informação é necessária a todos os níveis da organização para **identificar**, **avaliar** e **responder** aos **riscos**, e por outro lado orientar a entidade a alcançar os seus objetivos. A informação financeira é usada para disseminação externa e para decisões operacionais tais como a monitorização da performance e afetação de recursos. A informação financeira fidedigna é fundamental para o planeamento, orçamento, avaliação da performance dos vendedores, avaliar as joint-ventures e alianças, e outras atividades de gestão.

Similarmente, a informação operacional é essencial para o desenvolvimento dos relatórios financeiros. Isto inclui: vendas, compras e outras transações, informações das atualizações dos produtos da concorrência, ou condições económicas que afetam o inventário e valores a receber. A informação operacional a partir de fontes internas e externas, financeira e não financeira, é relevante para todos os objetivos do negócio.

A informação chega a partir de fontes internas e externas e sob a forma qualitativa e quantitativa e facilita as respostas à mudança. O desafio da gestão é processar e clarificar grandes volumes de dados em informação acionável. Este desafio é alcançado através do estabelecimento de uma infraestrutura de sistema de informação para as fontes de informação, captação, processamento, análise e elaboração de relatório da informação relevante. Os sistemas de informação também lidam com informações acerca de eventos externos, atividades e condições tais como: dados do mercado ou indústria que influenciam a procura dos produtos e serviços da empresa; dados dos bens e serviços para os processos de produção; inteligência do mercado envolvendo as preferências e necessidades dos consumidores; informação sobre as atividades desenvolvidas pelos concorrentes; iniciativas legislativas e regulamentos.

Os sistemas de informação podem ser formais ou informais. As conversas com clientes, fornecedores, reguladores e colaboradores proporcionam muitas vezes informação crítica necessária para identificar riscos e oportunidades. A comparência em seminários do setor de atividade e outros relacionados, ou profissionais, ser membro de associações empresariais e/ou outras pode proporcionar informação valiosa.

Guardar informação consistente com as necessidades é particularmente importante quando uma entidade enfrenta mudanças fundamentais na indústria, elevadas inovações e rápidos concorrentes, ou significativas alterações na procura dos consumidores. Os sistemas de informação devem mudar se necessário para apoiar os novos objetivos. Os sistemas de informação devem não somente capturar informação financeira e não financeira, mas também processar e descrever essa informação numa estrutura de modo a que seja útil para controlar as atividades da entidade.

- **Estratégia e Sistemas Integrados**

As empresas tornaram-se mais colaboradoras e integradas com clientes, parceiros de negócio e reguladores, a divisão entre a arquitetura dos sistemas de informação e as partes externas cresceu ofuscadamente. Como resultado, o processamento dos dados e os dados de gestão tornaram-se uma responsabilidade partilhada de múltiplas entidades. Em tais casos, a arquitetura do sistema de informação deve ser suficientemente flexível e ágil para integrar com eficácia novos clientes e parceiros de negócio.

O planeamento da arquitetura de sistemas de informação e aquisição de tecnologia são aspetos importantes para a estratégia da entidade, e as escolhas de tecnologia podem ser críticas para alcançar os objetivos. Decisões acerca da seleção da tecnologia e implementação dependem de muitos fatores, incluindo os objetivos organizacionais, as necessidades de mercado e as exigências da concorrência. Enquanto os sistemas de informação são fundamentais para uma gestão do risco empresarial eficaz, as técnicas de gestão do risco ajudam na tomada de decisão tecnológica.

- ***Sistemas apoiam as iniciativas estratégicas***

Os sistemas de informação têm sido planeados e utilizados para apoiar a estratégia de negócio. Este papel torna-se crítico quando as necessidades de negócio mudam e a tecnologia cria novas oportunidades para a vantagem estratégica.

- ***Integração com operações***

Muitas empresas usam sistemas de informação integrados, onde as transações são registadas e seguidas em tempo real, permitindo aos gestores um acesso imediato à informação financeira e operante, mais eficazmente no controlo das atividades de negócio.

- **Comunicação**

A comunicação é inerente a um sistema de informação. A comunicação deve ter lugar num sentido mais amplo, lidando com expectativas, responsabilidades individuais ou de um grupo, e outros assuntos importantes.

- ***Interna***

A gestão proporciona uma comunicação dirigida e específica, que trata das expectativas e das responsabilidades do pessoal. Isto inclui uma declaração clara da filosofia da gestão do risco empresarial e uma clara delegação da autoridade. Comunicação acerca dos processos e procedimentos devem estar alinhados com e sustentar a cultura do desejo de risco.

Eficazmente, a comunicação deve:

- ✓ Assegurar a consciência da importância da eficácia da gestão do risco empresarial;
- ✓ Comunicar o desejo de risco da entidade e as tolerâncias do risco;
- ✓ Implementar e apoiar uma linguagem comum de risco;

- ✓ Aconselhar o pessoal do seu papel e responsabilidades na realização e apoio dos componentes da gestão do risco empresarial.

- o ***Externa***

Com os canais de comunicação externos abertos, os clientes e fornecedores podem proporcionar inputs altamente significantes no planeamento ou qualidade dos produtos e serviços, permitindo à empresa ter em atenção as preferências e a procura dos clientes. As comunicações abertas sobre o desejo de risco da entidade e as tolerâncias de risco são importantes, particularmente para as entidades ligadas com outras na cadeia de fornecedores ou empresas de e-business. A gestão considera como o seu desejo de risco e tolerâncias de risco estão alinhados com os dos seus parceiros, assegurando que não exija demasiado risco dos seus parceiros.

- o ***Significados da comunicação***

O modo como a informação está apresentada e preparada, pode significativamente afetar o modo como a informação é interpretada e como os riscos associados ou oportunidades são vistos.

8. Monitorização

ERM é monitorização – um processo que avalia a presença e funcionalidade dos seus componentes ao longo do tempo. Isto é conseguido através de atividades contínuas de monitorização, avaliações separadas ou a combinação das duas. Monitorização contínua ocorre no normal curso das atividades de gestão. O âmbito e frequência de avaliações separadas vão depender primariamente de uma avaliação do risco e eficácia eficiência de procedimentos contínuos de monitorização. Deficiências de ERM são reportadas ascendentemente, com assuntos sérios relatados à gestão de topo e ao conselho.

- o ***Atividades de monitorização contínua***

Muitas atividades servem para monitorizar a eficiência e eficácia da gestão do risco empresarial durante o percurso normal do negócio. Isto inclui: gestão regular e atividades de supervisão, análise da variância, testes de stress, comparações, reconciliações e outras ações de rotina.

- o ***Avaliações separadas***

Enquanto os procedimentos da monitorização contínua proporcionam um feedback importante na eficiência e eficácia dos componentes da gestão do risco empresarial, é útil de vez em quando focar diretamente na eficiência e eficácia da gestão do risco empresarial. Isto proporciona uma oportunidade para considerar a eficiência e eficácia dos procedimentos da monitorização contínua.

- o ***Apresentação de relatório das deficiências***

As deficiências da gestão do risco empresarial podem surgir de muitas fontes, incluindo os

procedimentos da monitorização contínua da entidade, avaliações separadas e partes externas.

O termo deficiência refere-se a uma condição dentro do processo de gestão do risco empresarial, que precisa de atenção. Uma deficiência pode representar nota, uma falha potencial ou real ou uma oportunidade para fortalecer o processo para aumentar a probabilidade que os objetivos da entidade serão alcançados.

1.2.3. Risco da informação no contexto do risco empresarial

O risco pode ser definido como os efeitos da incerteza na realização dos objetivos.

Os efeitos, estão relacionados com as consequências / impacto na realização do objetivo, ou seja, um desvio relativamente aos resultados esperados, este efeito poderá ser positivo ou negativo.

O risco é frequentemente caraterizado, com referência a eventos (uma ocorrência ou a alteração de um determinado conjunto de circunstancias) potenciais e o impacto (que afetam os objetivos, quer o resultado seja positivo ou negativo), ou a combinação de ambos. Frequentemente é utilizado a combinação do impacto de um evento e a sua probabilidade de ocorrência.

No sentido de melhor compreender os riscos, estes podem ser divididos em categorias, sendo conhecidas como domínios de riscos.

Numa perspetiva de negócio, os domínios de risco que em última análise poderiam afetar a obtenção de resultados são agrupados sob o chapéu de risco empresarial. Considerando a diversidade de definições, os domínios geralmente aceites incluem risco estratégico, operacional, financeiro e regulatório / compliance.

Todos os domínios de risco podem conter de alguma forma elementos de risco tecnológico, a título de exemplo, o risco estratégico poderia incluir a não definição de um plano estratégico para os sistemas de informação, o que poderia levar à falta de investimento em tecnologia de modo a estimular a inovação e o desenvolvimento, no sentido de poder manter o negócio da organização competitivo e inovador. No que respeita ao risco de compliance poderia envolver a incapacidade de corresponder aos requisitos de conformidade tecnológicos aprovados pelos órgãos reguladores ou legais, verificando-se uma não conformidade o que poderia implicar sanções e penalizações.

Em termos práticos, maioritariamente o risco dos sistemas de informação encontra-se sob o domínio do risco operacional, que segundo o Basel Committee on Banking Supervision – 'Sound Practices for the Management and Supervision of Operational Risk' (2011) é definido como:

"O risco operacional é o risco de perda resultante de processos internos inadequados ou

deficientes, pessoas e sistemas, ou de eventos externos."

Explorando o domínio do risco dos sistemas de informação, em maior detalhe o tecnológico, na maior parte das vezes é dividido em subdomínios, alguns dos quais podem incluir elementos de domínios de risco empresarial (por exemplo, risco de compliance), como segue:

Segundo o Information Security Forum – "IRAM2 (2014):

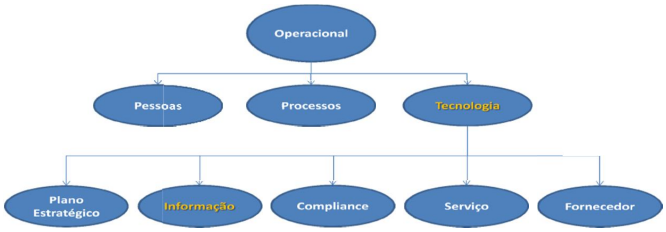


Figura 5 - Visão de Risco Operacional, adaptado de ISF-IRAM2

Gerir os riscos numa organização

O princípio de gerir o risco substancia-se na capacidade de ser capaz de balancear o risco numa perspetiva de custo vs. benefício. A maioria das organizações tem abordagens para gerir o risco de acordo com a sua maturidade, quer sejam mais estruturadas ou não.

A forma estruturada de gestão de risco envolve uma metodologia com componentes (por exemplo, políticas, processos e procedimentos) definidos e alinhados com objetivos organizacionais e culturais, mandatados pela gestão, e em cascata através das diversas unidades operacionais da organização. Esses componentes podem ser separados em duas camadas: a camada de governação de risco, e a camada de ciclo-de-vida de gestão de risco.

A avaliação de risco de informação

Quando os especialistas abordam a avaliação de risco, normalmente estão a referir-se à identificação, análise e avaliação de risco, que faz parte do ciclo-de-vida de gestão de risco, conforme figura infra.

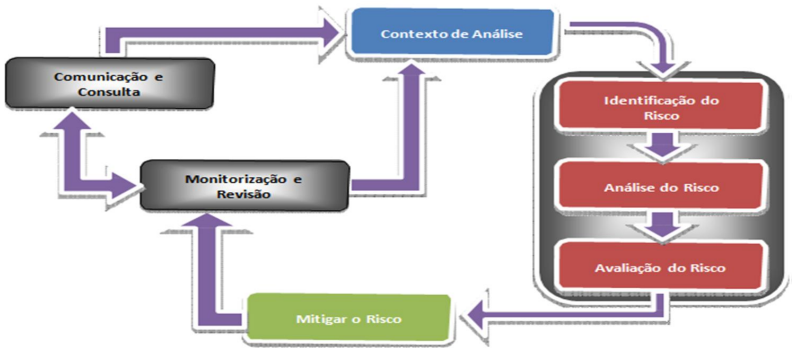


Figura 6 - Ciclo-de-Vida de Gestão de Risco (Avaliação de Risco), adaptado[2]

1.3. Controlos de Tecnologias de Informação

O IT é parte integrante do sistema de compliance, dado que as empresas estão dependentes do IT:

- Elevado grau de automatismo das transações diárias;
- A informação produzida pelo IT é fonte para a tomada de decisão;
- A disponibilidade e integridade do IT é crítica para as declarações e processos de reporte financeiros;
- Risco de a gestão não confiar nos controlos e sistemas de IT.

Classificação dos controlos de IT:

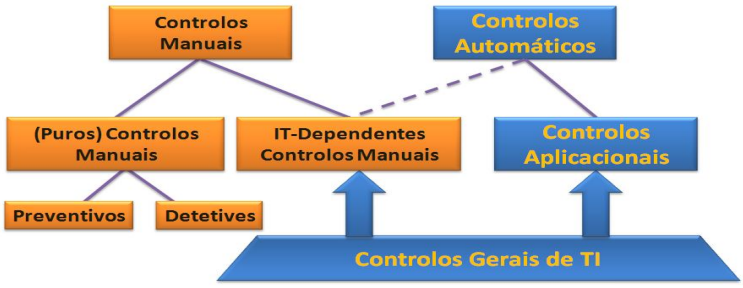


Figura 7 – Classificação dos Controlos de TI, adaptado de Ernest&Young

1.3.1 Controlos Gerais

Controlos Gerais de Tecnologias de Informação em Sarbanes Oxley

A framework de controlo interno (COSO) que o SEC recomenda às organizações para estarem em conformidade com o Sarbanes Oxley (SOX), tem em consideração os controlos de IT, mas não refere quais os requisitos recomendáveis para os objetivos e atividades de controlo.

De acordo com o IT Governance Institute (2006):

SOX 404 - Public Company Accounting Oversight Board (PCAOB) Auditing Standard No. 2 menciona a importância dos controlos de IT, mas não especifica em particular aqueles que devem ser considerados. Ficando sempre à consideração de cada organização.

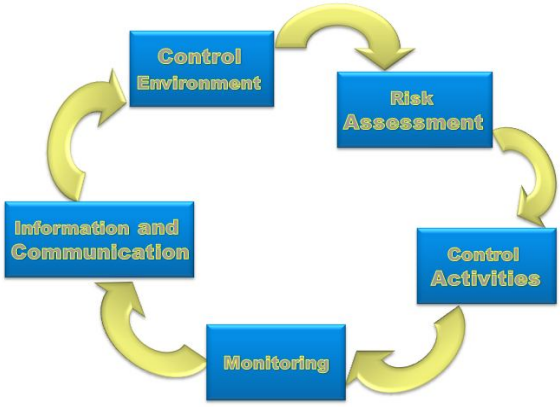


Figura 8 - COSO-Controlo Interno, adaptado[3]

Os Controlos Gerais de IT (ITGCs) influenciam diretamente a habilidade para se poder confiar nos Controlos Aplicacionais e nos Controlos Manuais dependentes do IT.

- Controlos de alto nível que influenciam individualmente os controlos aplicacionais e os dados do ambiente tecnológico.
- Ambiente de Desenvolvimento, Controlo de Alterações, Segurança da Informação, e Data Center.
- Tem de estar documentados e devem ser testados anualmente, se o Ambiente de Controlos Gerais der provas de que é um ambiente controlado, permite depositar mais confiança nos Controlos Aplicacionais.

Sem ITGCs, não existe capacidade para se poder confiar nos Controlos Aplicacionais ou nos Controlos Manuais, a menos que sejam executados procedimentos adicionais, tal como o Benchmarking. Ainda assim, estes procedimentos adicionais não dão garantias suficientes para que seja possível confiar em mais do que um controlo aplicacional de cada vez.

[3] Fonte: internet, www.googe.pt

Não existindo uma correlação direta entre os ITGCs e "what-can-go-wrong" (WCGW), estes encontram-se vinculados especificamente a controlos aplicacionais e a controlos manuais dependentes de IT que mitigam o WCGW.

Segundo o IT Governance Institute (2006):

PCAOB Standard #2, paragrafo 50, reconhece as seguintes quatro áreas chave que constituem os Controlos Gerais de IT (ITGCs):

- Ambiente de Desenvolvimento
  - Existe um System Development Life Cycle (SDLC) que é utilizado para orientar o desenvolvimento e o processo de aquisição;
  - Os pedidos para desencadear projetos e alterações são documentados e aprovados pelos stakeholders;
  - Nos pedidos deve estar evidenciado a documentação da definição, da manutenção e aprovação dos requisitos;
  - Nos pedidos deve estar evidenciado os testes, a manutenção e aprovação.
- Controlo de Alterações (Gestão de Alterações)
  - Existe um processo standard que é suportado por um documento que detalha um conjunto de regras/procedimentos/políticas para implementação de aplicações, infraestruturas, e software (novo, releases, updates, etc);
  - Existe um processo standard para os pedidos de alteração (eletrónico ou papel) utilizado para documentar e controlar as alterações e os pedidos aprovados;
  - Todos os pedidos de alteração são aprovados pelos responsáveis afetados, bem como por todos os que eventualmente possam ser afetados (definidos pelas políticas e procedimentos);
  - Todos os pedidos de alteração de emergência são testados e aprovados após implementação, pelas pessoas autorizadas respeitando as políticas e procedimentos.
- Segurança da Informação (Acesso a programas e dados)
  - Processo para Gestão de Acessos de Utilizadores a sistemas e aplicações (acessos, remoção, alteração), incluindo acessos remotos (i.e, processo para gestão de pedidos de acesso, e a aprovação pelo gestor responsável);
  - Perfis e Contas de utilizador individuais, de modo a aceder aos recursos do sistema, identificam cada utilizador unicamente. Todas as exceções devem ser documentadas e aprovadas;
  - Regras de password para restringir acessos (password standards: dimensão, procedimentos alteração, composição, bloqueio da conta tentativas falhadas);

- ❖ Acesso ao ambiente de produção (OS e aplicações) é controlado através de controlos físicos (i.e. RACF, Native OS ACLs) e através da segregação de funções (ex. programadores não tem acesso para modificar as bibliotecas on-line, apenas os administradores tem acesso, atributos especiais para administradores ou RACF);
- ❖ O acesso às bases de dados é autorizado com base nas responsabilidades das funções (i.e. DBA tem acesso de administrador Oracle) e o acesso a alterar os ficheiros da base de dados através do OS é restringido através de controlos físicos instalações (i.e. RACF or native OS ACL);
- ❖ O acesso a serviços sensíveis (acesso a master passwords, utilitários (incluindo scheduling packages), e sistemas de gestão de utilitários) é baseado nas responsabilidades das funções;
- ❖ Audit logs (e.g. – substitute user (SU) log) existem para registar os acessos dos utilizadores a serviços e utilitários considerados sensíveis e são revistos quando considerado apropriado;
- ❖ Firewall para proteger de tentativas de acesso não autorizadas de fonte externa (internet);
- ❖ Sistemas de Deteção de Intrusão são monitorizados periodicamente.

➢ Data Center (Ambiente de Produção)

- ❖ Incidentes Service Desk (i.e. incidentes, problemas, e erros (e.g., processamentos abortados)) são registados, analisados, escalados e resolvidos oportunamente – ITIL;
- ❖ Sistema de Processamento de jobs e batch feeds são documentados no manual de operações do IT ou outra documentação considerada;
- ❖ Checklist para as operações diárias são usadas para facilitar a monitorização do processamento dos sistemas;
- ❖ Os programas e os dados considerados críticos estão identificados, e os procedimentos de backups são executados segundo um programa;
- ❖ Existe um local off-site para armazenamento dos backups;
- ❖ Existe um Plano de Disaster Recovery para todos os data centres;
- ❖ Existe controlos ambientais e de segurança física (i.e., medidores de temperatura, Ar-condicionado, sistema de deteção de fogo, sistema de alimentação secundário (UPS), etc.) para todos os data centers.

1.3.2 Controlos Aplicacionais

- Controlos específicos para as aplicações, ex. confirmar que não estão a ser pagas faturas duplicadas pelo sistema X;
- A documentação e o teste aos controlos, tem por base uma reunião com a equipa de auditoria. Os testes aos controlos aplicacionais poderão ou não ser realizados anualmente, dependendo dos resultados aos controlos gerais.

Descrição dos Controlos Aplicacionais

- Controlos de Input
  - Controlar a edição;
  - Validar a introdução de ficheiros;
  - Relatórios de Erros e edição.
- Controlos de Processamento
  - Controlos de Reconciliação;
  - Programas de Cálculo;
  - Processamento de Estatísticas.
- Controlos de Output
  - Processamento de Relatórios;
  - Ficheiros Output;
  - Interface com Outros Sistemas.
- Controlos de Segurança
  - Controlos de Segurança Aplicacionais.

1.4. A importância dos Processos de Negócio e a função Sistemas de Informação (SI)

O que é um processo de negócio?

Essencialmente podemos definir um processo de negócio como "quem, faz o quê, quando e como".

Por outras palavras pode ser igualmente definido, conforme (ITGI, 2006):

"Os processos de negócio são os mecanismos da organização de criação e entrega de valor para os stakeholders. Input, processamento e outputs são funções de processos de negócio. Cada vez mais, os processos de negócio estão a ser automatizados e integrados com os sistemas de IT complexos e altamente eficientes."

Nesse sentido um processo pode ser definido como o conjunto de atividades inter-relacionadas ou interativas, que transforma entradas em saídas. Estas atividades exigem alocação de recursos, tais como aplicações, infraestrutura, informações e pessoas. Na figura 9, pode ser

visualizado como um processo se relaciona com os riscos e controlos.

Processos de Negócio e a função Sistema de Informação (SI)

Cada vez mais, os sistemas de IT estão a automatizar os processos de negócio, e no decorrer deste processo de automatização, os sistemas na maior partes das vezes substituem as atividades manuais de controlo por atividades de controlo dependentes de IT.

Os serviços de IT são a base para as operações e são fornecidos transversalmente pela organização, e não segregados por processos de negócio ou unidade de negócio. Geralmente incluem, gestão de rede, gestão de bases de dados, gestão de sistemas operacionais, gestão de armazenamento, gestão de instalações e segurança, e são na maior partes das vezes geridos por uma função central de IT.

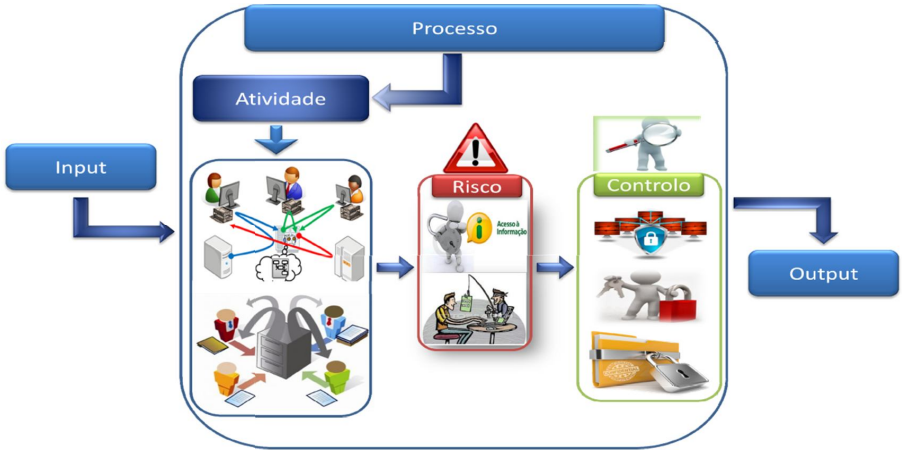


Figura 9 - Processo Organizacional, adaptado[4]

Controlos sobre Sistemas de IT

Considerando o impacto que o IT atualmente tem no negócio das empresas (resultado da automatização dos processos de negócio e sua dependência, e naturalmente incremento do risco associado) e a consequente generalização e confiança depositada nos sistemas e IT, são necessários controlos sobre tais sistemas, independente da sua dimensão. Estes controlos gerais de IT geralmente incluem controlos sobre o ambiente de IT, operações, o acesso a programas e dados, desenvolvimento e manutenção de programas. Estes controlos em princípio aplicam-se a sistemas que tenham sido identificados na avaliação de criticidade do sistema com impacto significativo.

[4] Fonte: internet, www.google.pt

1.5. ISO 27002: 2013 – Standard de Gestão da Segurança da Informação

O que é segurança da informação?

A informação é um ativo tal como outros ativos comerciais importantes, é essencial para o negócio de uma organização e consequentemente precisa de ser protegida adequadamente. Isto é, especialmente importante nos ambientes de negócio cada vez mais interligados, como resultado desta crescente interconetividade, a informação é agora exposta a um número cada vez maior e uma maior variedade de ameaças e vulnerabilidades.

As informações podem existir em muitas formas, pode ser impressa ou escrita em papel, armazenada em formato eletrónico, transmitida por correio ou por meios eletrónicos, passada em filmes, ou falada numa conversa.

Independentemente da forma que as informações assumam, ou os meios pelos quais sejam partilhadas ou armazenadas, deve ser sempre devidamente protegida.

A segurança da informação é a proteção da informação de uma ampla gama de ameaças, a fim de garantir a continuidade do negócio, minimizar os riscos de negócio e maximizar o retorno sobre investimentos e oportunidades de negócio.

A segurança da informação é conseguida através da implementação de um conjunto adequado de controlos, incluindo políticas, processos, procedimentos, estruturas organizacionais, funções de software e de hardware. Esses controlos precisam de ser estabelecidos, implementados, monitorizados, revistos e melhorados, sempre que necessário, para garantir que os objetivos de segurança e de negócio específicos da organização sejam atendidos. Isto deve ser feito em conjunto com outros processos de gestão de negócio.

Por que é necessária a segurança da informação?

A Informação e os processos de suporte, sistemas e redes são ativos comerciais importantes. Definir, realizar, manter e melhorar a segurança da informação pode ser essencial para manter a vantagem competitiva, cash-flow, rentabilidade, compliance legal e imagem comercial.

As organizações, os seus sistemas de informação e as suas redes são confrontados com ameaças de segurança de uma ampla gama de fontes, incluindo ataques assistidos por computador, fraude, espionagem, sabotagem, vandalismo, incêndio ou inundação.

Causas de danos, tais como código malicioso, hackers e ataques de negação de serviço tornaram-se mais comuns, mais ambiciosos e cada vez mais sofisticados.

A segurança da informação é importante para ambas as empresas públicas e privadas, e para proteger infraestruturas críticas. Em ambos os sectores, a segurança da informação funcionará como um facilitador, por exemplo, para atingir e-government ou e-business, e para evitar ou reduzir os riscos relevantes.

A interligação das redes públicas e privadas e a partilha de recursos de informação aumentam a

dificuldade de alcançar o controlo de acesso. A tendência à computação distribuída também enfraqueceu a eficácia de um controlo central especializado.

Muitos sistemas de informação não foram projetados para serem seguros. A segurança que pode ser alcançada através de meios técnicos é limitada, e deve ser apoiada pela administração e procedimentos adequados. Identificar que controlos devem estar implementados requer um planeamento cuidadoso e atenção aos detalhes.

Gestão de segurança da informação requer, no mínimo, a participação de todos os colaboradores da organização. Ela também pode exigir a participação de acionistas, fornecedores, terceiros, clientes ou outras entidades externas. Também pode ser necessário consultar um especialista de organizações externas.

Como estabelecer requisitos de segurança

É essencial que uma organização identifique os seus requisitos de segurança, pode-se identificar três fontes principais:

1. Derivada da **avaliação de riscos** para a organização, tendo em conta a estratégia global de negócio da organização e objetivos. Através de uma avaliação de riscos, ameaças aos ativos são identificadas, a vulnerabilidade e a probabilidade de ocorrência é avaliada e o impacto potencial é estimado.

2. Os **requisitos legais**, estatutários, regulamentares e contratuais que uma organização, os seus parceiros comerciais, fornecedores e prestadores de serviços têm de cumprir, e o seu ambiente sociocultural.

3. O conjunto específico de **princípios, objetivos e requisitos de negócio** para o processamento de informações que uma organização tem desenvolvido para apoiar suas operações.

Avaliar os riscos de segurança

Os requisitos de segurança são identificados através de uma avaliação metódica dos riscos de segurança. O custo e o esforço nos controlos têm que ser avaliado tendo em consideração o dano suscetível da consequente falha de segurança.

Os resultados da avaliação de risco vão ajudar a orientar e a determinar a ação de gestão apropriada e as prioridades para a gestão dos riscos de segurança da informação, e para a implementação dos controlos selecionados para proteger contra esses riscos.

A avaliação de riscos deve ser efetuada periodicamente para endereçar quaisquer alterações que possam influenciar os resultados da avaliação de risco.

Seleção de Controlos

Considerando que os requisitos de segurança e os riscos foram identificados e as decisões para mitigar e lidar com o risco foram tomadas, os controlos apropriados devem ser selecionados e implementados para assegurar que o risco é reduzido para um nível aceitável.

Os controlos podem ser selecionados a partir do standard ISO27002 ou de outra metodologia considerada adequada (ISF, NIST, FFIEC, BITS, etc.) ou novos controlos podem ser selecionados para atender necessidades específicas, conforme apropriado. A seleção de controlos de segurança depende de decisões organizacionais com base nos critérios de aceitação de risco, as opções de resposta ao risco, e a abordagem de gestão de risco geral aplicada pela organização, e deve ser também sujeita a toda a legislação e regulamentos nacionais e internacionais pertinentes.

Alguns dos controlos neste standard podem ser considerados como princípios orientadores para a gestão de segurança da informação e aplicável para a maioria das organizações.

Avaliação de riscos de segurança

As avaliações de risco devem identificar, quantificar e priorizar os riscos contra os critérios de aceitação de riscos e objetivos relevantes para a organização. Os resultados devem orientar e determinar as ações de resposta apropriadas e as prioridades para gestão de riscos de segurança da informação e para a implementação dos controlos selecionados para proteger contra esses riscos.

No processo de avaliação de riscos e seleção de controlos pode ser necessário, ter que ser realizado um número de vezes para cobrir diferentes partes da organização ou sistemas de informação individuais.

A avaliação de risco deve incluir a abordagem sistemática de estimar a magnitude dos riscos (análise de risco) e o processo de comparar os riscos estimados com base em critérios de risco para determinar a importância dos riscos (avaliação de risco).

As avaliações de risco devem ser realizadas periodicamente para endereçar alterações nos requisitos de segurança e na situação de risco, por exemplo nos ativos, ameaças, vulnerabilidades, impactos, a avaliação de risco, e quando ocorrerem alterações significativas.

Estas avaliações de riscos devem ser efetuadas de forma metódica capaz de produzir resultados comparáveis e reproduzíveis.

A avaliação de riscos de segurança da informação deve ter um âmbito claramente definido, a fim de ser eficaz e deve incluir as relações com avaliações de risco em outras áreas, se for caso disso.

O âmbito de uma avaliação de risco pode ser toda a organização, partes da organização, um sistema de informação individual, componentes de sistema específicos, ou serviços sempre que

tal for viável, realista e útil. Exemplos de metodologias de avaliação de risco são discutidos em ISO / IEC TR 13335-3 (Diretrizes para a Gestão da Segurança de IT: Técnicas de Gestão da Segurança de IT).

Resposta aos riscos de segurança

Antes de considerar a resposta a um risco, a organização deve definir os critérios para determinar se os riscos podem ser aceites ou não.

Os riscos podem ser aceites se, por exemplo, considera-se que o risco é baixo ou que o custo da resposta não é rentável para a organização. As decisões devem ser registadas.

Para cada um dos riscos identificados após a avaliação do risco, deve ser tomada uma decisão quanto à resposta ao risco.

Possíveis opções para a resposta ao risco:

a) Aplicar os controlos apropriados para reduzir os riscos;

b) Aceita consciente e objetivamente o risco, desde que claramente satisfaça a política e critérios de aceitação de risco da organização;

c) Evita o risco por não permitir ações que potencialmente poderiam fazer com que o risco ocorresse;

d) Transfere o risco para outras partes, por exemplo, seguradoras ou fornecedores.

Para os riscos em que a decisão de resposta ao risco tenha sido aplicar controlos apropriados, estes controlos devem ser selecionados e implementados para atender as necessidades identificadas por uma avaliação de risco. Os controlos devem assegurar que os riscos são reduzidos a um nível aceitável tendo em conta:

a) Requisitos e restrições da legislação e regulamentos nacionais e internacionais;

b) Os objetivos da organização;

c) Os requisitos operacionais e restrições;

d) O custo de implementação e operacionalização em relação aos riscos que está a ser mitigado, e permaneça proporcional aos requisitos e restrições da organização;

e) A necessidade de balancear o investimento na implementação e operacionalização dos controlos comparativamente com os danos suscetíveis que possam resultar de falhas de segurança.

É necessário reconhecer que alguns controlos podem não ser aplicáveis a todos os sistemas de informação ou ambientes, e pode não ser viável para todas as organizações.

Por exemplo:

- Os direitos podem ser segregados para impedir fraudes e erros. Pode não ser possível para pequenas organizações segregar todos os direitos, e outras formas de atingir o mesmo

objetivo de controlo pode ser necessária;

- O uso do sistema pode ser monitorizado e provas recolhidas. Os controlos descritos e.g. registro de eventos, podem entrar em conflito com a legislação aplicável, tais como a proteção da privacidade para os clientes ou no local de trabalho.

Os controlos de segurança da informação devem ser considerados no sistema e aquando da especificação dos requisitos de projetos e na fase de conceção/desenvolvimento. Caso não seja feito, pode resultar em custos adicionais e soluções menos eficazes, e eventualmente na pior das situações, a incapacidade de alcançar a segurança adequada.

Deve-se ter em mente que nenhum conjunto de controlos pode alcançar a segurança completa, e que a ação de gestão adicional deverá ser implementada para monitorizar, avaliar e melhorar a eficiência e a eficácia dos controlos de segurança para apoiar os objetivos da organização.

2. METODOLOGIA

O desenvolvimento do trabalho proposto e a prossecução dos seus objetivos, considerando a investigação a desenvolver, necessita de suporte empírico proveniente de áreas distintas (Pessoas, SI, TIC, informação, risco e segurança da informação e dos SI), pelo que se considera que a opção pela abordagem qualitativa é a mais adequada às atividades a concretizar.

Nesse sentido as metodologias de investigação adotadas foram focus group, sessões de brainstorming suportadas por um guião de entrevista semiestruturado.

Para melhor compreensão das metodologias adiante será feita uma breve descrição sobre as mesmas. Como suporte ao método foi necessário analisar um conjunto de documentos internos e internacionais sobre normas, regulações e legislação para melhor compreensão da temática e de toda a envolvência e aplicação da proposta de novo modelo de processo.

O focus group ou grupo de discussão é uma técnica que visa a recolha de dados, que pode ser usada em diferentes fases do processo de investigação.

Segundo Silva, I., Veloso A. & Keating, J. (2014) baseando-se em Morgan (1996, 1997), definem focus group como uma técnica de investigação de recolha de dados através da interação do grupo sobre um tópico apresentado pelo investigador. Tal definição, segundo o autor, comporta três componentes essenciais: os focus group são um método de investigação dirigido à recolha de dados; localiza a interação na discussão do grupo como a fonte dos dados; e, reconhece o papel ativo do investigador na dinamização da discussão do grupo para efeitos de recolha dos dados. Krueger e Casey (2009), para além das características anteriores, salientam também a focalização da discussão num dado assunto, o seu contributo para a compreensão do tópico de interesse e o facto dos participantes que os compõem terem alguma característica em comum e relevante face ao tema em discussão.

O objetivo deste focus group era conciliar as diferentes perspetivas e experiências/conhecimento dos intervenientes criando sessões de brainstorming, de modo a perspetivar uma metodologia que respondesse às diferentes realidades de cada ambiente organizacional, que fosse passível de implementação, suportada em um guião de entrevista com questões semiestruturadas. O objetivo era obter o contributo e a experiência de cada um dos intervenientes sobre o modo como aplicam a atual metodologia, através da identificação de quais os desafios, dificuldades, oportunidades de melhoria e constrangimentos.

A opção por esta metodologia de trabalho deveu-se essencialmente às vantagens proporcionadas por esta técnica de trabalho, nomeadamente:

- Desenvolve a capacidade para produzir ideias originais e soluções diferentes das habituais;
- Ajuda a superar o conformismo, a estereotipia, a rotina e a indiferença;

- Mostra que a maioria das pessoas tem soluções múltiplas, e que é sempre possível encontrar uma melhor;
- Desenvolve a flexibilidade mental;
- Estimula a relação espontânea no grupo, e produz (quando se faz num clima emocional apropriado) uma certa alegria e bem-estar na sessão e depois dela;
- Maior conhecimento e maior precisão;
- Transmissão e partilha de informação;
- Mais alternativas de soluções;
- Maior capacidade de assumir riscos;
- Maior e melhor coordenação e controlo após a decisão.

Apesar de esta técnica poder ter algumas desvantagens, considerando o objetivo do trabalho proposto e a dimensão do grupo, revelou ser a mais apropriada.

Como principais inconvenientes deparados:

- Tempo gasto (recursos caros);
- Indecisão prolongada (difícil consenso);
- Diluição de responsabilidades;
- Aspetos culturais, era um grupo heterogéneo;
- Aspetos linguísticos;
- Aspetos administrativos relativos à aprovação dos documentos de trabalho.

Em termos práticos a agregação do método de focus group em sessões brainstorming, foi concretizada em 4 fases:

1ª Fase – Recolha de formação

- Pressupostos que foram tidos em consideração na análise do modelo IRM:
  - Âmbito Sistema Europeu de Bancos Centrais;
  - Baseado no standard internacional ISO272002:2005;
  - Metodologia de gestão de segurança dos sistemas de informação.
  - Obrigatoriedade de conformidade com o standard;
  - Não existe relacionamento entre os requisitos de segurança e os processos de negócio;
  - Constituição de um grupo internacional com especialista em segurança de sistemas informação dos bancos centrais do Euro sistema.

- A criação do guião de entrevista com questões semiestruturadas;
- O estabelecimento de uma sessão de três dias em Estugarda com o grupo de trabalho;
- Reunião com os intervenientes.

2ª Fase – Realização das entrevistas e análise dos resultados

- Consistiu na agregação e análise dos resultados;
- Interpretação dos resultados.

3ª Fase – Discussão dos resultados com os intervenientes

- A discussão dos resultados com os intervenientes e a definição de uma prova de conceito com base nos resultados obtidos;
- Analisada a metodologia "Information Risk Analysis Methodology (IRAM)" do ISF (Information Security Forum), virificou-se que está alinhada com a ISO27002:2013, após uma apresentação em Amesterdão por parte de Steve Durbin do ISF, identificou-se que não preenchia as necessidades identificadas pelo grupo;

4ª Fase – Proposta de modelo

- Prova de conceito que consistiu em pegar nos dados obtidos e construir uma nova proposta de modelo face aos constrangimentos e oportunidades de melhoria identificadas, através de:
    - Identificação de "riscos/ameaças" e os consequentes requisitos de segurança associados à mitigação dessa ameaça;
    - No que respeita a objetivos e esforço a vertente que carecia de maior trabalho respeitava à atribuição de pesos (qualitativos) aos requisitos de segurança na mitigação das ameaças respeitantes que a metodologia do ISF não contemplava;
    - Numa fase posterior, o pretendido era efetuar uma avaliação aos requisitos de segurança identificados para mitigação das ameaças que foram efetivamente implementados, com base nessa avaliação é obtido como resultado final o risco residual do sistema de informação, isto é, o risco a que o SI está exposto após a implementação dos requisitos de segurança;
    - No que se refere à prova de conceito a mesma foi testada baseada num processo de melhoria continua, em que esses resultados eram posteriormente discutidos com o grupo para aferir da aplicabilidade da mesma, sendo identificadas as fragilidades, pontos fortes e constrangimentos.

Os benefícios da proposta da nova metodologia de um processo de gestão de risco da informação (IRM) é providenciar uma metodologia objetiva e de fácil aplicação, no sentido de identificar os riscos associados aos sistemas de informação que possam afetar os processos de negócio (riscos de negócio). Em termos práticos facultar um meio para avaliar as medidas de segurança e

identificar e selecionar os requisitos/ medidas de segurança para o sistema de informação.

Esta metodologia pretende assegurar que a segurança da informação é tratada adequadamente em cada fase do ciclo-de-vida do sistema. Desenvolver a segurança em sistemas durante o seu desenvolvimento é mais eficaz e seguro, do que quando realizadas numa fase posterior ao seu desenvolvimento.

3. Proposta de um processo de gestão de risco da informação (IRM)

3.1. Principais Resultados da investigação

Os processos e as atividades de qualquer instituição financeira assentam cada vez mais em sistemas de informação e tecnologias de informação (SI/TI). Assim o funcionamento correto, fidedigno e seguro dos SI/TI é um aspeto fulcral para que uma instituição consiga alcançar os seus objetivos.

Por esta razão torna-se fundamental estabelecer um método estruturado de análise das questões de segurança e gestão de riscos de segurança na implementação ou atualização de sistemas de informação.

A metodologia atual é baseada num catálogo de segurança que remonta a 2005, com a proposta deste novo processo o objetivo será mudar o foco de uma abordagem centrada num catálogo de segurança para uma abordagem centrada em ameaças.

O objetivo proposto é alterar a metodologia atual através da incorporação de fases de gestão de risco, baseado nos resultados obtidos das sessões de brainstorming com o focus group, vide Anexo 7, dos quais se destaca:

#1: Workstream E

3. Baseline Catalog

3.1 Improve the “compliance based approach” with “threats” which are related to “controls” (“best of two worlds”)

#2: Workstream H

8. Business language for reporting (for threats) (H) (H)

9. How to report the relevant risks for shared services (regularly) to the system owner?(H) (H)

10. Risk classification (temp. / regularly reviewed / permanent) (M) (H)

11. Risk reporting and register (review) (H) (H)

A existência de um conjunto requisitos de segurança pressupõe a mitigação de um conjunto de riscos. Tendo isso em consideração, surge o desafio de definir uma lista de ameaças suficientemente abrangente e de alto nível que pudesse ser aplicada a todos os sistemas de informação.

Partindo da lista de ameaças é possível efetuar uma análise das ameaças, e com base nesta análise efetuar a priorização dos requisitos de segurança, isto é conseguido pela identificação dos controlos transversais que mitigam as principais ameaças. Esta informação será relevante na medida em que será fator essencial para suportar uma análise de custo vs. benefício de modo a direcionar o esforço de implementação dos controlos.

Quem deverá ser o público-alvo desta metodologia

Serão todos aqueles que participam em atividades de gestão de risco, além do proprietário do sistema, o gestor de operações de TI, o gestor de projetos e restantes membros da equipa, especialistas em sistemas e colaboradores de segurança (peritos e operacionais), incluindo todos os colaboradores dentro da organização, que estejam envolvidos em atividades de desenvolvimento ou operação dos sistemas. Para facilitar o trabalho, mas também para garantir a qualidade comparável, especialistas em segurança devem ser envolvidos na execução das tarefas chave ou devem ser consultados sempre que necessário.

3.2. Descrição geral da metodologia atual

A gestão de riscos é o processo contínuo de avaliação de risco (avaliação do impacto ou da criticidade do sistema e a probabilidade de perdas / danos), levando à definição de requisitos de segurança e medidas adicionais de mitigação e / ou a aceitação dos riscos remanescentes.

Nesse sentido, a metodologia pode ser dividida em três processos distintos, conforme descritos:

O processo de gestão de riscos para sistemas de informação

O processo aplica-se a novos sistemas ou alterações a sistemas atualmente em produção consistindo em cinco passos, os quais serão explicados em maior detalhe na tabela 1 em anexos, onde será descrito o objetivo, as atividades chave, input, output e funções responsáveis.

Inicia-se sempre com um trigger, tais como:

- Requisitos de negócio que levam a uma alteração ou a um novo sistema de informação;
- Pedidos de alteração;
- Novas ameaças ou o resultado de uma avaliação (regular) de risco ou vulnerabilidades;
- Testes de penetração, procedimentos de monitorização, follow-ups de incidentes, etc.;
- Desenvolvimentos de segurança (novas medidas, como a biometria);
- Tempo.

A monitorização contínua e avaliação da segurança dos sistemas em operação

Adicionalmente às etapas de avaliação de risco efetuadas, conforme descritas supra, durante um projeto ou no ciclo-de-vida das alterações, os sistemas de informação em operação devem ser

monitorizados continuamente em conformidade com as medidas operacionais identificadas (por exemplo, log de monitorização, monitorização de vulnerabilidades, follow-up de incidentes) e os riscos do sistema devem ser regularmente avaliados (por exemplo, testes de penetração, auditorias).

É importante a realização de revisões periódicas dos riscos de segurança e os controlos implementados para confirmar que os controlos permanecem eficazes e apropriados. Nesta fase poderá ser interessante envolver a auditoria e o controlo interno, no sentido de assegurar uma certa independência, em conformidade com o princípio de segregação de funções.

As revisões devem ser realizadas em diferentes níveis de profundidade, dependendo dos resultados das avaliações anteriores e das alterações dos níveis de risco que a gestão está disposta a aceitar. As avaliações de risco são frequentemente realizadas numa primeira fase a alto nível, sem grande detalhe, como meio de priorização de recursos em áreas identificadas com risco elevado. Posteriormente será desencadeado uma análise com maior detalhe, para endereçar riscos específicos.

O processo de gestão de risco para o cumprimento dos requisitos de segurança

Regularmente (por exemplo, a cada dois anos) especialistas em segurança devem verificar a implementação dos requisitos de segurança e as medidas do catálogo de segurança e, quando necessário, propor a implementação de novos requisitos e atualização das medidas. Também devem verificar se os requisitos de segurança novos ou atualizados precisam de ser integrados no catálogo.

A estrutura da metodologia atual em cinco fases:

1. Avaliação de criticidade do sistema
   - Identificar as fronteiras entre a criticidade e os sistemas de informação.
2. Identificação dos requisitos de segurança
   - De acordo com a criticidade identificada e com base no catálogo de segurança definido.
3. Seleção e implementação de medidas de segurança
   - Selecionar, configurar, detalhar; e
   - Implementar as medidas de segurança.
4. Avaliação de Conformidade
   - Avaliar a conformidade com os requisitos e identificar os riscos remanescentes.
5. Relatórios e aceitação
   - Para aceitar os riscos remanescentes e onde necessário implementar medidas adicionais.

Figura 10 - IRMv2, adaptado de documentação interna.

Tabela 1: Processo de gestão de risco para os SI

	Fase 1: **Avaliação da criticidade do Sistema**	**Fase 2:** **Identificação dos requisitos de segurança**	**Fase 3:** **Seleção da solução de segurança**	**Fase 4:** **Verificação de conformidade**	**Fase 5:** **Relatório e Aceitação**
Objetivo	Adquirir um entendimento comum sobre o risco do negócio e acordar o nível básico necessário de proteção.	Identificar os requisitos de segurança e chegar a um compromisso sobre eles.	Elaborar a solução de segurança em conformidade com os requisitos de segurança e chegar a um compromisso.	Verificar se a implementação está em conformidade com os requisitos de segurança identificados.	Aceitação do nível de segurança do sistema e os riscos remanescentes e / ou elaborar um plano de ação.
Atividade chave	**Avaliação da criticidade do Sistema** Reunir com os responsáveis do negócio para avaliar o impacto no negócio da perda de confidencialidade, integridade ou disponibilidade da informação e avaliar a probabilidade e as ameaças.	**Identificação dos requisitos de segurança** Reunir com os responsáveis do negócio para selecionar os requisitos de segurança e as medidas com base no catálogo de segurança. Medidas adicionais, podem ter de ser definidas com a ajuda de uma análise de risco mais detalhada.	**Seleção e implementação das medidas de segurança** Reunir com especialistas para desenhar uma solução detalhada que inclua a segurança e informar o negócio sobre os riscos remanescentes.	**Verificação de conformidade** Reunir com a equipa de projeto, negócio e as operações para verificar a implementação (conformidade) de todos os requisitos de segurança e medidas. Realizar avaliação (pré-produção) de segurança (possivelmente suportada por testes de penetração), adicionalmente, se necessário uma análise de risco.	**Relatório e aceitação** Reportar riscos remanescentes e, em certos casos, ações de mitigação adicionais. Aprovação dos riscos remanescentes e das medidas de segurança sugeridas
Input	Descrição do trigger, por exemplo um novo sistema de informação e / ou business case novo ou modificado, pedidos de alteração, incidentes, uma nova ameaça ou o resultado de uma avaliação de vulnerabilidade.	**Output da fase 1**: Limites e âmbito do sistema ou da alteração, a avaliação de criticidade de sistema de alto nível com a identificação dos principais riscos em termos de perda de confidencialidade, integridade ou disponibilidade.	**Output da Fase 2:** Lista dos requisitos e medidas (necessidades de proteção) de segurança definidos, e adicionalmente normas de conformidade (políticas específicas, conceitos de segurança e orientações).	**Output da fase 3:** Proposta da arquitetura e medidas de segurança, bem como especificações de segurança.	**Output da fase 4:** Avaliação dos riscos remanescentes e das medidas de segurança propostas.
Output	Os **limites** do sistema e o **âmbito do trigger** claramente definidos, para estabelecer o âmbito da avaliação do risco. Validar o trigger (por exemplo, pedido de alteração, documento de início de projeto (PID)). Identificação da criticidade com base na confidencialidade, integridade e disponibilidade (por exemplo, o que acontece se o sistema está indisponível por um período x?).	Definição dos **requisitos de segurança** e das **medidas** (de proteção necessárias) com base em riscos de negócio e análises de impacto.	Proposta de **arquitetura de segurança** e medidas. **Especificações de segurança**, por exemplo, Especificação de segurança Windows 2008.	**Riscos remanescentes** e as medidas de **segurança associadas** (com uma visão gráfica sobre a situação de risco, se possível).	Validação da avaliação de segurança, incluindo um plano de ação com outras medidas de mitigação. Lista de riscos remanescentes aprovados e medidas de mitigação recomendadas.
Quem?	Negócio (proprietário do sistema) com o apoio do analista de negócio & IS especialista em segurança.	Negócio (proprietário do sistema) com o apoio do analista de negócios & IS especialista em segurança.	IT e IS especialistas em segurança, arquiteto e negócio (proprietário do sistema).	IT e IS especialistas em segurança, IT operações e negócio (proprietário do sistema).	Negócio (proprietário do sistema) com o apoio da IS especialistas em segurança.

3.3. Proposta de novo modelo

A proposta de alteração à metodologia atual prevê a inclusão de três fases, conforme se pode verificar na ***tabela 2***, que pretendem dar uma visão mais orientada aos riscos e que frequentemente estão presentes num tradicional sistema de informação. O objetivo é que se possa priorizar os controlos mais importantes na mitigação do risco, e por essa forma racionalizar numa perspetiva de custo vs. benefício quais os controlos que deverão ser primeiramente implementados, considerando que o atual modelo não permite esta visão uma vez que é orientado à conformidade com a implementação dos requisitos de segurança.

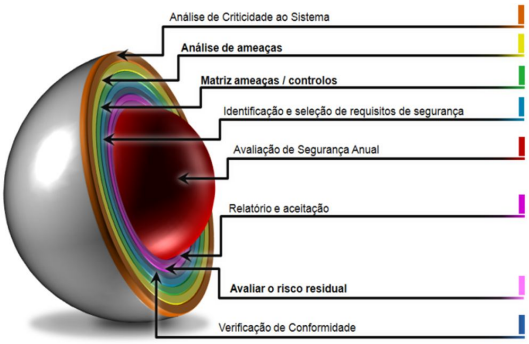


Figura 11 - Proposta de novo modelo (IRMv3) adaptado de documentação interna.

Seguidamente serão descritos detalhadamente cada uma das fases da metodologia a ser proposta, tendo em consideração que as imagens referenciadas em cada uma das fases da metodologia são os exemplos da prova de conceito que foi utilizada para testar a aplicabilidade do modelo.

Tabela 2: Proposta de alteração ao Processo de gestão de risco para os SI

	Fase 1: **Avaliação da criticidade do Sistema**	**Fase 2:** **Análise de ameaças**	**Fase 3:** **Matriz de Ameaças/ controlos**	**Fase 4:** **Identificação e seleção dos requisitos de segurança**	**Fase 5:** **Verificação de conformidade**	**Fase 6:** **Avaliar o risco residual**	**Fase 7:** **Relatório e Aceitação**
Objetivo	Adquirir um entendimento comum sobre o risco do negócio e acordar o nível básico necessário de proteção.	Determinar os riscos relevantes do sistema de informação em conformidade com o seu desenho.	Assegurar que os valores de efetividade dos controlos são os apropriados para contra-atacar as ameaças relacionadas.	Identificar os requisitos de segurança e chegar a um compromisso sobre eles. **Seleção da solução de segurança** Elaborar a solução de segurança em conformidade com os requisitos de segurança e chegar a um compromisso.	Verificar se a implementação está em conformidade com os requisitos de segurança identificados.	Determinar as ameaças não mitigadas, que constituem um risco.	Aceitação do nível de segurança do sistema e os riscos remanescentes e / ou elaborar um plano de ação.
Atividade chave	**Avaliação da criticidade do Sistema** Reunir com os responsáveis do negócio para avaliar o impacto no negócio da perda de confidencialidade, integridade ou disponibilidade da informação e avaliar a probabilidade e as ameaças.	**Análise de ameaças** Identificar os riscos que o sistema de informação é suscetível de estar exposto a, respeitando o âmbito de aplicação do sistema de informação.	**Matriz de controlo/ ameaça** Adaptar os valores de efetividade dos controlos. Os valores representam a efetividade relativa dos controlos para contra-atacar as ameaças.	**Identificação dos requisitos de segurança** Reunir com os responsáveis do negócio para selecionar os requisitos de segurança e as medidas com base no catálogo de segurança. Medidas adicionais, podem ter de ser definidas com a ajuda de uma análise de risco mais detalhada. **Seleção e implementação das medidas de segurança** Reunir com especialistas para desenhar uma solução detalhada que inclua a segurança e informar o negócio sobre os	**Verificação de conformidade** Reunir com a equipa de projeto, negócio e as operações para verificar a implementação (conformidade) de todos os requisitos de segurança e medidas. Realizar avaliação (pré-produção) de segurança (possivelmente suportada por testes de penetração), adicionalmente, se necessário uma análise de risco.	**Avaliar os riscos residuais** Com base na probabilidade inicial, a efetividade dos controlos, a efetividade da matriz de controlo/ ameaça a probabilidade de sucesso pode ser derivada. O impacto e a probabilidade de sucesso representarem o risco.	**Relatório e aceitação** Reportar riscos remanescentes e, em certos casos, ações de mitigação adicionais. Aprovação dos riscos remanescentes e das medidas de segurança sugeridas
Input	Descrição do trigger, por exemplo um novo sistema de informação e / ou business case novo ou modificado, pedidos de alteração, incidentes, uma nova ameaça ou o resultado de uma avaliação de vulnerabilidade.	Lista de ameaças (catálogo ameaça ISF); fronteiras do sistema de informação; desenho e arquitetura do sistema de informação.	As ameaças relevantes e os controlos. A efetividade relativa está dependente do juízo/ opinião do especialista.	**Output da fase 1**: Limites e âmbito do sistema ou da alteração, a avaliação de criticidade de sistema de alto nível com a identificação dos principais riscos em termos de perda de confidencialidade, integridade ou disponibilidade **Output da Fase 2:** Lista dos requisitos e medidas (necessidades de proteção) de segurança definidos, e adicionalmente normas de conformidade (políticas específicas, conceitos de segurança e orientações).	**Output da fase 3:** Proposta da arquitetura e medidas de segurança, bem como especificações de segurança.	**Output da fase 2,3,5:** As ameaças relevantes, efetividades dos controlos avaliada, a matriz de ameaça/ controlo é combinada de acordo com uma função matemática para determinar em larga escala as ameaças não mitigadas.	**Output da fase 6:** Avaliação dos riscos remanescentes e das medidas de segurança propostas.
Output	Os **limites** do sistema e o **âmbito do trigger** claramente definidos, para estabelecer o âmbito da avaliação do risco. Validar o trigger (por ex, pedido de alteração, documento de início de projeto (PID)). Identificação da criticidade com base na CIA (por exemplo, o que acontece se o sistema está indisponível por um período x?).	As ameaças relevantes claramente definidas e o sistema de informação deverá ser protegido em conformidade.	Matriz de controlo/ ameaça	Definição dos **requisitos de segurança** e das **medidas** (de proteção necessárias) com base em riscos de negócio e análises de impacto. Proposta de **arquitetura de segurança** e medidas. **Especificações de segurança**, por exemplo, Especificação de segurança Windows 2008.	**Riscos remanescentes** e as medidas de **segurança associadas** (com uma visão gráfica sobre a situação de risco, se possível).	**Documentar a avaliação de risco: Riscos remanescentes** (visão gráfica da situação de risco se possível) e propostas / planos de ação para resposta aos riscos.	Validação da avaliação de segurança, incluindo um plano de ação com outras medidas de mitigação. Lista de riscos remanescentes aprovados e medidas de mitigação recomendada.
Quem?	Negócio (proprietário do sistema) com o apoio do analista de negócio & IS especialista em segurança.	IS especialistas em segurança	IS especialistas em segurança	Negócio (proprietário do sistema) com o apoio do analista de negócios & IS especialista em segurança.	IT e IS especialistas em segurança, IT operações e negócio (proprietário do sistema).	IT e IS especialistas em segurança, IT operações e negócio (proprietário do sistema).	Negócio (proprietário do sistema) com o apoio da IS especialistas em segurança.

3.3.1. Análise de criticidade do sistema

A avaliação da criticidade do sistema é uma maneira simples de identificar os riscos de negócio associados a um sistema de informação através da determinação do impacto para o negócio em relação aos três aspetos de segurança confidencialidade, integridade e disponibilidade de uma forma estruturada. Este passo só é realizado para aplicações de negócio.

Descrição: o primeiro passo é avaliar a criticidade do sistema novo ou atualizado através da identificação dos riscos de negócio associados ao uso de sistemas de informação, ou seja, ao determinar o impacto para o negócio em relação aos três aspetos de segurança confidencialidade, integridade e disponibilidade.

Isto deve ser feito o mais cedo possível, ou seja, no pedido de fase de iniciação do projeto ou alteração. Os resultados vão mostrar as necessidades básicas em termos de proteção, o que, por sua vez, vai dar uma orientação para a definição de requisitos de segurança mais detalhados e a seleção das medidas de segurança apropriadas.

Um benefício adicional, é que será garantido uma compreensão comum por todas as partes envolvidas. Coerência com a classificação ORM (Gestão de Risco Operacional) para os processos de negócio que dependem do sistema de IT deverá ser garantida.

Quando: após a definição do âmbito do projeto ou alteração.

Input: para os projetos, descrição do business case, incluindo os processos de negócio de alto nível e descrição do modelo concetual de informação e o âmbito.

Para pedidos de alteração, descrição e âmbito do pedido de alteração (PA) com a documentação disponível do sistema.

Atividade: para os projetos, no que se refere à segurança da informação, a avaliação da criticidade do sistema é a primeira atividade. Deve ser realizada preferencialmente sob a forma de um workshop com presença de representantes da área de negócio e um analista de negócio, a segurança é facilitada por um especialista. O objetivo é determinar a criticidade de um sistema novo ou atualizado a partir de uma perspetiva de negócio. Este é um exercício que não vai ser muito demorado e pode ser facilmente posto em prática em três etapas:

1. ***Verificar o âmbito de aplicação do sistema de informação***, limites e interdependências: o primeiro passo é verificar o business case pela compreensão do âmbito do pedido projeto ou alteração, os processos de negócio de alto nível, o modelo de informação concetual (ativos de informação) e os limites e as interdependências com outros sistemas.
2. ***Identificar o impacto de negócio*** (insignificante, baixo, médio, alto, muito alto) em termos de confidencialidade, integridade e disponibilidade (ver anexo 4): o segundo passo é identificar os riscos de negócio e fazer uma avaliação da criticidade com base em questões orientadas para o negócio, descrita num questionário standard, com relação ao potencial impacto causado por uma perda de confidencialidade, integridade e disponibilidade. A avaliação geral para disponibilidade deve representar o impacto de uma interrupção prolongada (por exemplo

cinco dias). Em linha com o rating de disponibilidade, o período aceitável de não disponibilidade deve ser definido, deve ser dada uma indicação sobre se o sistema é fundamental para o SEBC, e se acordos adicionais relativos a procedimentos de recuperação de desastre ou sites de contingência são necessários. Também deve ser dada uma indicação da probabilidade destes riscos se materializarem, já que os controlos de compensação (por exemplo, controlos de integridade organizacional) poderem estar implementados.

3. Discutir e chegar a acordo sobre as ***necessidades básicas de proteção***: como terceiro passo, as necessidades de proteção básicas devem ser discutidas e acordadas. A proteção precisa em termos de confidencialidade, integridade e disponibilidade são, em princípio, a maior pontuação de uma das respostas para as oito perguntas sobre a confidencialidade, integridade e disponibilidade. Durante este passo, é particularmente importante considerar as características específicas do sistema novo ou atualizado.

Para pedidos de alteração, deve ser efetuada uma análise de impacto direcionada aos impactos da alteração na segurança. Dependendo do âmbito da alteração (por exemplo, alteração numa funcionalidade do negócio), pode ser necessário para atualizar a avaliação da criticidade do sistema para projetos, como descrito acima.

Output: para projetos, um questionário de avaliação de criticidade do sistema preenchido com identificação dos principais ativos de informação e a criticidade em termos de confidencialidade, integridade e disponibilidade. Os resultados devem ser documentados num relatório estruturado, que descreva a criticidade e o impacto potencial no negócio, específicos para o sistema estudado, e esta informação deve ser incorporada no documento de início de projeto (PID).

Para pedidos de alteração, a avaliação de impacto de segurança deve ser documentada como parte do registo e início da alteração. Dependendo do âmbito e impacto da mudança, a avaliação de criticidade do sistema existente pode ser atualizado e, posteriormente aceite pelo proprietário do sistema (SO).

A avaliação de criticidade nova ou atualizada do sistema deve ser aceite pelo proprietário do sistema (SO). O pedido de alteração incluindo a análise de impacto de segurança precisa de ser aceite pelo proprietário do sistema e do gestor de alterações (GA).

Avaliações de criticidade do sistema e análises de impacto de alterações devem ser guardadas num repositório central e que possa ser acessível a todas as partes interessadas, incluindo especialistas em segurança.

Categorias de impacto

Esta seção explica o significado das categorias de impacto, mais detalhes e orientação para a classificação é dada no Anexo 3.

Impacto sobre o negócio (em termos de confidencialidade, integridade e disponibilidade)

- **Nenhum** ou **insignificante**: não afetaria os interesses essenciais do SEBC;
- **Baixo**: possa ser desvantajosa para os interesses essenciais do SEBC;
- **Médio**: poderia prejudicar temporariamente os interesses essenciais do SEBC;
- **Alto**: pode prejudicar gravemente os interesses essenciais do SEBC;
- **Muito alto**: prejudicar seriamente os interesses essenciais do SEBC.

O nível dos requisitos é derivado do nível de criticidade (nenhum / baixo, médio, alto / muito alto), o que resulta em mais medidas a serem consideradas para a seleção na próxima etapa.

Tendo em conta os riscos que podem ser induzidos em outros sistemas, os requisitos para sistemas com um nível de criticidade de nenhum / insignificante são definidos para ser o mesmo que para os sistemas de baixo impacto.

3.3.2. Análise de ameaças

Identificar e avaliar as ameaças relevantes para o sistema de acordo com o seu ambiente.

Descrição: A segunda etapa é a chamada etapa de análise de ameaças. A sua função principal é determinar as ameaças relevantes do sistema de informação e dar estimativas sobre as ameaças. Análise de ameaças leva em conta as 54 ameaças da lista de ameaças do ISF listadas no anexo 5.

Quando: Depois de ter realizado a avaliação da criticidade

Input: Para projetos, processos de negócio de alto nível e descrição conceptual do sistema e âmbito do sistema de informação.

Para pedidos de alteração, descrição e âmbito do pedido de alteração (PA) com a documentação disponível do sistema.

Atividade: A análise de ameaças basicamente consiste em três fases:

- Identificação de ameaças importantes;
- Avaliação do impacto da ameaça;
- Avaliação da ameaça probabilidade intrínseca;
- Cálculo de prioridade da ameaça.

Ambas são tarefas executadas manualmente por um especialista em segurança.

Output: Lista com as ameaças relevantes claramente definidas para o sistema de informação que deverá ser protegido em conformidade.

Identificação das ameaças importantes

O objetivo desta fase é identificar as ameaças que o sistema de informação é suscetível de ser exposto a, respeitando o âmbito, o design, bem como a arquitetura do sistema de informação. O output é uma definição clara das ameaças relevantes.

A abordagem proposta é levar em consideração todas as ameaças do ISF e identificar apenas aquelas que não se aplicam com uma explicação. Ameaças adicionais que possam parecer ser relevantes mas ainda não estão abrangidas pela proposta ISF podem ser adicionadas.

Se o âmbito, design e arquitetura do sistema de informação não for clara e objetiva, todas as ameaças devem ser selecionadas.

Se uma aplicação, por exemplo, não possui website ou interface web, pode ser justificado fazer excluir a ameaça E06.

E06	**Defacing web sites**	Unauthorised modification of web site content with the intention of negatively affecting the reputation of the organisation.

Figura 12 - Exemplo de ameaça

Todas as ameaças que foram identificadas de serem relevantes devem então ser avaliadas pelo seu impacto e a sua probabilidade.

Avaliação de impacto da ameaça

Cada uma das ameaças que foram identificadas para que possam serem consideradas relevantes, devem ser avaliadas pelo seu impacto e a sua probabilidade.

A consideração do impacto é determinada com base em que categoria a confidencialidade (C), integridade (I) e disponibilidade (A) é afetada. A respetiva classificação da CIA para a respetiva categoria / categorias pode ser tida como uma suposição inicial, contudo deverá ser efetuado um refinamento. Consequentemente deverá ser efetuada uma estimativa dos danos de acordo com a escala de classificação de gestão de risco operacional (ORM) para cada uma das ameaças. Uma ameaça que afeta apenas as avaliações de disponibilidade é mostrada na imagem infra. A avaliação CIA foi LHH. Como a ameaça afeta apenas a categoria da disponibilidade com o impacto máximo, um VH é atribuído para a disponibilidade.

Impact Assessment		
C	I	A
N/A	N/A	VH

Figura 13 - Avaliação de impacto da ameaça

Fonte: Information Technology Committee, Security Risk Management Working Group (AUG. 2015), ESCB Information Systems Risk Management Methodology – IRMv3. Germany (Frankfurt): ESCB (European Systems of Central Banks).

Para fazer com que o impacto da ameaça seja útil dentro de fórmulas, é atribuído um número a cada nível. Estes números são chamados números de impacto de ameaça (de confidencialidade, integridade e disponibilidade) e representam fatores de multiplicação que serão posteriormente utilizados para medir a prioridade da ameaça. Os multiplicadores refletem a escala de impacto de classificação ORM.

	multiplicator
VH	10000
H	1000
M	100
L	10
VL	1
empty	0

Figura 14 - Legenda para escala de impacto

Como é exigido um impacto total da ameaça, os números de confidencialidade (C), integridade (I) e disponibilidade (A) são adicionados para cada ameaça - sendo então, definido como o impacto ameaça.

#	Threat Name	Threat Description	Impact Assessment			Impact
			C	I	A	
E	**External attack**					
E01	**Carrying out denial of service attacks**	Deliberately attacking a system with the intention of rendering the service unavailable to the legitimate business users.	N/A	N/A	**H**	1000

Figura 15 - Impacto da ameaça

Avaliação da probabilidade intrínseca da ameaça

Dependendo do tipo de ameaça (alguém faz alguma coisa ou alguma coisa acontece), são utilizadas diferentes abordagens para medir a probabilidade intrínseca.

Se "alguém faz algo" uma estimativa é feita para as categorias:

- Motivação;
- Habilidades;
- Conhecimento Sistema;
- Tempo / Custo;
- Colaboração Interna.

Para cada uma destas categorias um número entre 1 e 5 (incluindo 1 e 5) é atribuído de acordo com a seguinte matriz:

	required motivation	required skills	required system knowledge	required time/cost	required internal collaboration
1	Attracting attention	Expertise	Very detailed knowledge	> 1 year > EUR 100 000	Several staff members with specific knowledge
2	Creation of confusion/ delay	Expert skills	Detailed knowledge	<1 year < EUR 100 000	Single member of staff with specific knowledge
3	Damage to the Eurosystem	Everyday skills	Knowledge in the field	<1 month < EUR 10 000	Single member of staff
4	Personal gain or damage to the Eurosystem	Basic skills	General knowledge	<1 week < EUR 1 000	Not required
5	Personal gain	Basic skills sufficient	Knowledge not necessary	<1 day < EUR 100	Not required

Figura 16 - Avaliação das categorias da ameaça "Fraud and attack Oriented"

Para a probabilidade intrínseca a soma de todas as categorias é criada, sendo que a probabilidade da ameaça, pode atingir um máximo de 25 pontos.

Exemplo: Um ataque de negação de serviço afeta apenas a disponibilidade. Neste caso foi avaliado o impacto para um sistema com requisitos de (H) disponibilidade alta, resultando num impacto sobre a disponibilidade com um valor de H.

Neste caso, a ameaça de realizar ataques de negação de serviço é avaliada. As habilidades necessárias como o conhecimento do sistema são insignificantes, bem como o conhecimento do sistema e os custos. Um botnet que executar ataques pode ser alugado por algumas centenas de Euros, um conhecimento sobre o sistema geralmente não é necessário (além da URL ou outros

recursos) e as habilidades exigidas são baixas, como por exemplo através do download de ferramentas da Internet. Nem é necessária uma forte motivação nem a colaboração interna. A probabilidade intrínseca é, portanto, 21, onde um máximo de 25 poderia ser alcançado por este cálculo. Portanto, é uma ameaça que é suscetível de se materializar em caso de falha dos controlos.

#	Threat Name	Threat Description	Impact Assessment			Likelihood Assessment					Inherent Threat Likelihood
						Fraud and Attack Oriented					
			C	I	A	Motivation	Skills	System Knowledge	Time / Cost	Internal collab.	
E	External attack										
E01	Carrying out denial of service attacks	Deliberately attacking a system with the intention of rendering the service unavailable to the legitimate business users.	N/A	N/A	H	4 - Personal gain or damage to the Eurosystem	4 - Basic skills	4 - General knowledge	4 - <1 week < EUR 1 000	5 - Not required	21

Figura 17 - Cálculo da probabilidade intrínseca da ameaça "Fraud and attack Oriented"

Para executar este exercício é disponibilizado uma folha de Excel contendo todas as ameaças ISF, as ameaças irrelevantes podem ser simplesmente eliminadas atribuindo 0 à motivação necessária, habilidades, conhecimento do sistema, o tempo / custo e colaboração interna.

Para as ameaças "Error or Incident Oriented" é efetuada uma estimativa para as categorias:

- Complexidade do negócio;
- Complexidade do meio envolvente.

Para cada uma destas categorias um número entre 1 e 5 (incluindo 1 e 5) é atribuído de acordo com a matriz seguinte:

	Business Complexity	Environmental Complexity
1	5 - Extremely complex and/or changing	5 - Extremely complex and changing
2	4 - Very complex and/or changing	4 - Very complex and changing
3	3 - Complex and/or changing	3 - Complex and changing
4	changing	2 - Little complexity and quite stable
5	1 - Simple and/or exceptionally changing	1 - Simple and stable

Figura 18 - Avaliação das categorias da ameaça "Error or Incident Oriented"

A soma destas duas colunas é multiplicada pelo fator 2,5 para alcançar o mesmo resultado alvo de domínio como o da “Fraud and attack Oriented”, atingindo valores de 5-25. As ameaças irrelevantes podem simplesmente ser eliminadas através da atribuição de 0 à coluna “Inherent Threat Likelihood” da respetiva ameaça, sobrescrevendo a fórmula.

Exemplo:

A ameaça de uma falha na manutenção do sistema de informação é apresentada. Neste caso, o impacto de um sistema com elevado (H) em confidencialidade, integridade e disponibilidade requisito que foi estimado, resultando num impacto sobre a confidencialidade, integridade e disponibilidade de H.

É assumido que a complexidade do negócio é "4 - muito complexo e / ou alterações" e que a complexidade do meio envolvente é "5 - extremamente complexa e alterações". A soma destes valores é de 9, a qual é então multiplicado com 2,5, resultando numa probabilidade inerente de 23 para esta ameaça.

#	Threat Name	Threat Description	Impact Assessment			Likelihood Assessment Error or Incident Oriented		Inherent Threat Likelihood
			C	I	A	Business Complexity	Environ-mental complexity	
M01	**Breach of information system maintainability**	Breach of information system maintainability possibly leading to the business service being unavailable to the legitimate business users and/or rendering it possible to gain unauthorised access to or manipulate business information.	**H**	**H**	**H**	4 - Very complex and/or changing	5 - Extremely complex and changing	23

Figura 19 - Cálculo da probabilidade intrínseca da ameaça ““Error or Incident Oriented””

No final deste passo, é determinado em resultado do cálculo uma estimativa da probabilidade intrínseca de cada uma das ameaças.

Quanto à probabilidade inerente também pode ser determinada empiricamente, em alguns casos, é possível definir diretamente este valor fazendo “um atalho” e configurar o valor para um número de frequências já conhecido de acordo com a escala de classificação ORM. Se esse valor estiver definido, então a probabilidade inerente é calculada em conformidade a partir da frequência definida e uma indicação visual é feita sobre isso, como os itens individuais são negligenciados e, portanto, exibidos em cinza claro.

#	Threat Name	Threat Description	Impact Assessment			Likelihood Assessment						Inherent Threat Likelihood	Inherent Threat Priority Top 10 Top 20
						Fraud and Attack Oriented							
			C	I	A	Motivation	Skills	System Knowledge	Time / Cost	Internal collab.	Frequency		
E	External attack												
E01	Carrying out denial of service attacks	Deliberately attacking a system with the intention of rendering the service unavailable to the legitimate business users.	N/A	N/A	H	5 - Personal gain	4 - Basic skills	4 - General knowledge	4 - <1 week < EUR 1 000	5 - Not required	5 - Almost certain	25	25.000

Figura 20 - Cálculo da probabilidade intrínseca da ameaça

Cálculo da prioridade da ameaça

O objetivo deste passo é calcular a importância de uma ameaça. A ideia básica é a de atribuir uma prioridade maior a uma ameaça, se mais categorias (confidencialidade, integridade, disponibilidade) são afetadas. Se uma ameaça afeta apenas disponibilidade e outra ameaça afeta confidencialidade e disponibilidade e ambas têm a mesma probabilidade intrínseca, deve ser atribuída uma prioridade mais elevada a uma ameaça que afeta mais categorias.

Uma fórmula simples é aplicada:

Prioridade da Ameaça = Probabilidade da Ameaça * (número de impacto da ameaça Confidencialidade + Número impacto ameaça Integridade + número Impacto ameaça disponibilidade)

Os números de impacto da ameaça são tomadas a partir da secção 6.2.2. Por conseguinte, a prioridade da ameaça dá uma indicação sobre quais as ameaças que devem ser mitigadas pela primeira vez. Quanto maior a probabilidade mais categorias são afetadas, maior a prioridade da ameaça será.

3.3.3. Matriz de Ameaças / Controlos

O primeiro passo desta fase é identificar onde é necessário fazer os ajustes aos controlos, na medida em que mitigam as ameaças, isto é, ao valor atribuído ao requisito na mitigação da ameaça.

A teoria por detrás deste passo é a convicção, de que diferentes controlos têm um impacto diferente em mitigar as ameaças em relação entre si.

Enquanto uma política de gestão de passwords é identificado que não dá nenhuma proteção contra “Undertaking malicious probes or scans” ou "desastres naturais", mas que pode proteger contra "Hacking", "cracking de passwords" ou "ter acesso não autorizado a sistemas ou redes".

Mecanismos técnicos de filtragem podem proteger contra a ““Undertaking malicious probes or scans” ou até mesmo "realizar ataques de negação de serviço”. Supõe-se que com base nos controlos disponíveis uma ameaça pode ser completamente mitigada.

Quando: depois da avaliação das ameaças.

Input: conhecimento do especialista acerca da efetividade dos controlos para mitigar as ameaças.

Atividade: esta metodologia utiliza a seguinte abordagem para o bem da simplicidade:

A matriz ameaças / controlos representa o nível de proteção dos controlos corretamente implementados em relação entre si para mitigar as ameaças. Quanto maior o valor, maior é o nível de proteção.

No exemplo que se segue, tendo uma visão da ameaça E01 "Carrying Denial of Service attacks" foi identificado como sendo três vezes mais mitigante ter políticas de segurança da informação do que ter contato com as autoridades.

		Threat Priority	External attack	Carrying out denial of service attacks	Hacking	Undertaking malicious probes or scans	Cracking passwords	Cracking keys
			E	E01	E02	E03	E04	E05
			0	25000	24000	25	30000	900
5	**Information security policies**							
5.1	***MANAGEMENT DIRECTION FOR INFORMATION SECURITY***							
5.1.1	Policies for information security			1	10	10	5	2
5.1.2	Review of the policies for information security						10	10
6	**Organization of information security**							
6.1	***INTERNAL ORGANISATION***							
6.1.1	Information security roles and responsibilities				5			
6.1.2	Segregation of duties				10		2	
6.1.3	Contact with authorities			3	3	3	3	3
6.1.4	Contact with special interest groups				5	5	5	5

Figura 21 - Matriz de Ameaças / Controlos

Um valor entre 0 e 20 (incluindo 0 e 20) é proposto para indicar o nível de proteção de um controlo corretamente implementado para combater uma ameaça. A soma de todos os controlos contrariando uma ameaça pode variar, uma vez que apenas os níveis de proteção relativos estão indicados.

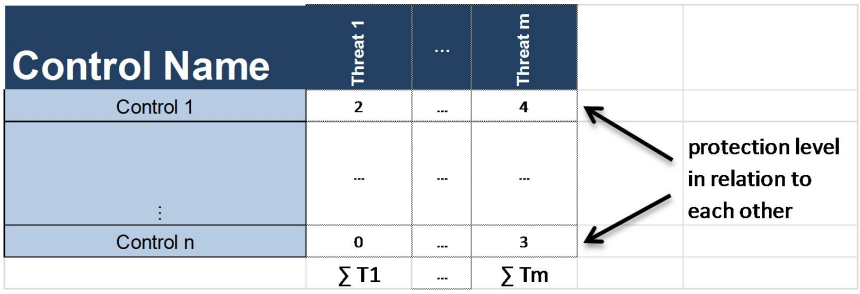


Figura 22 - Priorização do Controlo

No caso dos valores pré-definidos dos controlos, se o especialista identificar que os mesmos não são aplicáveis, estes podem ser modificados/ajustados.

Sempre que sejam identificadas novas ameaças, na análise de ameaças, os níveis de proteção de todos os controlos têm que ser determinados e documentados na folha de Excel.

Output: Matriz de ameaças / controlos.

3.3.4. Identificação e seleção de requisitos de segurança

Identificar os requisitos eelaborar a solução de segurança em conformidade com os requisitos de segurança e chegar a um compromisso.

Definir ou atualizar os requisitos de segurança da baseline em conformidade com a criticidade identificada.

Descrição: o quarto passo é a identificação e seleção de requisitos de segurança. O objetivo é refletir a proteção potencial dos controlos para mitigar as ameaças e para dar aos projetos não apenas uma lista de controlos para implementar. Além disso também a priorização destes requisitos de segurança é entregue, a fim de ser capaz de se concentrar em controlos que são altamente eficazes. Um controlo que mitiga muitas ameaças com impactos elevados e altas probabilidades devem ser priorizados com elevado.

Quando: depois de elaborada a Matriz de Ameaças / Controlos.

Input: conhecimento do especialista e os resultados das fases anteriores.

Atividade: para os projetos:

Para cada um dos controlos a importância relativa para o projeto pode ser calculada. A teoria básica desta fase é indicar para cada controlo quão eficaz é na mitigação das ameaças identificadas na análise de ameaças. O resultado é um valor numérico único para cada controlo, para que a importância relativa dos controlos possa ser comparada e priorizada.

Sendo s <i, j> a força relativa de um controlo i para mitigar a ameaça j. Para cada controlo i a força relativa s <i, j> desse controlo é multiplicado com a prioridade de ameaças relevantes pj e estes valores são somados. O resultado é considerado como sendo a priorização do controlo.

Control Name	Threat 1	...	Threat m	Control Priority		
	priority p1 = 2400		priority pm = 1600			
Control 1	s11	...	s1m	∑ s1i*pi, i=1..m ←	generic formula	
⋮	...	...	...		relative priority of controls	
Control n	0	... 0 ...	3	0*2400+...3*1600 = 4800 ←	Example	

Figura 23 - Formula priorização do controlo

De acordo com a ponderação dos controlos que teve lugar, é possível ordenar os controlos pela sua prioridade numa ordem decrescente, que é suportada pela folha de Excel fornecida. Na folha de Excel, o top 10 e top 20 dos controlos são destacados nas cores, vermelha e laranja. O número de ameaças mitigadas por certos controlos é fornecido para informação, bem como uma indicação sobre se este é considerado para ser um controlo genérico ou um específico.

#	Control objective	Control description	G/S	Control Priority Top 10 Top 20	Number of threats mitigated
6.1.5	Information security in project management	Ensure that all types of projects address information security.	S	12,398,650	52
16.1.6	Learning from information security incidents	Analyze information security incidents and study your responses. Learn from your information security incidents and responses. Use your knowledge to reduce the likelihood that incidents will occur in the future and to moderate their impact when they occur.	G	8,272,545	36
12.4.1	Event logging	Establish logs to record user activities and events. Use event logs to record information security events, activities, exceptions, and faults. Maintain your organization's event logs. Monitor your organization's event logs. Retain logs to support future investigations. Review your event logs on a regular basis.	G	7,713,540	30
18.2.2	Compliance with security policies and security requirements	Ask your organization's managers to carry out regular security compliance reviews within their own areas of responsibility. Review how well your organization's information processing activities and procedures comply with security requirements. Review compliance with appropriate security policies. Review compliance with appropriate security standards.	G	7,393,045	32

Figura 24 - Lista de controlos TOP 10 e 20

Os requisitos de segurança ao nível dos controlos também podem ser alterados por requisitos de segurança adicionais que já são óbvios nesta fase para o sistema.

A equipa (analista de negócio e IS especialista em segurança) deve sanear todos os requisitos de segurança e verificar se os requisitos são adequados, suficientes e eficazes em termos de custos e, assim, encontrar um equilíbrio entre a segurança (mitigação de riscos), os custos e usabilidade / facilidade de uso. Esta deve, preferencialmente, ser feita sob a forma de um workshop.

Estes representam os requisitos de segurança num nível elevado e pode ser encaminhado para a equipa de arquitetura de sistema que cria a partir da lista de controlos de segurança um desenho detalhado da aplicação, as tecnologias utilizadas, os protocolos, a localização na rede, de mecanismos de controlo de autenticação e acesso etc. Os controlos de segurança são, portanto, traduzidos em medidas de segurança. A conformidade com todas as políticas de segurança do SEBC deve ser verificada e, sempre que adequado, os requisitos específicos devem ser adicionados aos requisitos do sistema. A equipa de arquitetura de sistema documenta a arquitetura, bem como a arquitetura de segurança com medidas de segurança (para implementar os requisitos de segurança) no chamado documento de arquitetura de sistema (SAD). É explicitamente declarado que a criação de uma SAD está fora do âmbito de aplicação da metodologia IRMv3.

Para pedidos de alteração: dependendo do âmbito e impacto de segurança da alteração (por exemplo, alteração de funcionalidade do negócio), pode ser necessário atualizar os requisitos de segurança, arquitetura de sistema ou medidas de segurança, como descrito acima. As alterações à arquitetura do sistema e ao conceito de segurança, deve respeitar os requisitos de segurança.

Output: Requisitos de segurança novos ou atualizados e a nova ou atualizada arquitetura de IT (segurança).

3.3.5. Verificação de Conformidade

Avaliar a conformidade com os requisitos de segurança e identificar os riscos remanescentes (documento com os riscos esperados).

Descrição: a verificação deverá ser efetuada:

- Antes da alteração ser aprovada;
- Quando o documento da arquitetura do sistema estiver concluído;
- Antes do sistema entrar em produção;
- A efetividade das medidas de proteção planeadas/ implementadas;
- As medidas e controlos de segurança (documentados no SAD);
- A verificação do estado da segurança do sistema e da qualidade em todas as áreas e aspetos relevantes, devendo ser documentado no PPSA (ver figura 27).

Em relação às alterações, esta avaliação só pode ser relevante para parte do sistema de informação e requisitos de segurança. As avaliações de eficácia, podem portanto ser acionadas a qualquer momento entre a avaliação da criticidade e a avaliação de risco residual quando há uma necessidade de demonstrar os controlos ineficazes ou requisitos de segurança, ou seja, após a criação do documento de arquitetura de segurança ou no meio da execução de um projeto.

Para os sistemas de avaliação com uma criticidade de "muito elevado", deve ser efetuada uma verificação de conformidade mais aprofundada a qual deve ser realizada por especialistas em segurança independentes da equipa do projeto.

Quando: As verificações de conformidade podem ser acionadas a qualquer momento entre a avaliação da criticidade e a avaliação de risco residual, sempre que há uma necessidade de destacar controlos ineficazes ou requisitos de segurança (ou seja, após a criação do documento de arquitetura de segurança ou no meio da execução de um projeto).

Input: requisitos de segurança e medidas selecionadas, documento de arquitetura do sistema.

Atividade: para os projetos:

Com base nos requisitos de segurança e nas medidas acordadas, uma verificação cruzada deve ser realizada pelo especialista em segurança, com o apoio da equipa de trabalho, a área do projeto / negócio e operações de TI, para verificar se as medidas de segurança propostas são executadas de forma adequada.

A efetividade dos controlos é normalmente avaliada controlo a controlo. Informações genéricas disponíveis sobre a efetividade dos controlos, em geral podem ser reutilizadas quando aplicável. Quando necessário, os controlos genéricos têm de ser reavaliados para um projeto, onde o nível de eficácia genérico não se encaixa com o nível de efetividade específico do projeto.

Para cada um dos controlos de segurança aplicáveis, a eficácia do controlo é determinada por pareceres de peritos. Para cada um dos controlos, diferentes níveis de conformidade podem ser atribuídos, de acordo com:

[0] Não é efetiva - poucas ou nenhuma das medidas de proteção estão implementadas e o sistema é extremamente vulnerável com uma elevadíssima probabilidade das ameaças se materializarem, o nível de conformidade é considerado ineficaz quando menos de 30% das medidas de proteção são cumpridas;

[1] Parcialmente efetiva - um pequeno número de medidas de proteção estão implementadas e o sistema é altamente vulnerável com uma alta probabilidade de as ameaças se materializarem, o nível de conformidade é considerada parcialmente eficaz quando estiverem reunidas medidas de proteção entre 30% e 60%;

[2], Grande medida efetiva - significa que um grande número de medidas de proteção estão implementadas e o sistema é moderadamente vulnerável com uma probabilidade média das ameaças se materializarem, o nível de conformidade é considerada muito eficaz quando estiverem reunidas medidas de proteção entre 60% e 90%; e

[3] Efetiva - significa que a maioria das medidas de proteção estão implementadas e o sistema tem algumas vulnerabilidades com uma baixa probabilidade das ameaças se materializarem, o nível de conformidade é considerado efetivo quando superior a 90% das medidas de proteção estejam implementadas.

5.1.1	Policies for information security	Define your organization's information security policies. Ask your management to approve your security policies. Publish your organization's information security policies. Communicate your security policies to relevant parties. Communicate your security policies to employees. Communicate your security policies to external parties.	25,708,570	3

Figura 25- Avaliação da eficácia do Controlo

Para todas as avaliações que tenham sido identificadas com um valor inferior a 3 deve ser efetuada uma explicação.

Para auxiliar o IS especialista em segurança nesta tarefa podem ser definidas perguntas de suporte sobre o nível objetivo, bem como questões norteadoras a serem usadas como uma ferramenta de apoio.

No entanto, não só a existência, mas a efetividade dos controlos têm de ser avaliada. Isto também inclui os procedimentos de teste (por exemplo, recolhendo evidências testes de penetração) para fundamentar os resultados, bem como medidas genéricas fora do sistema (por exemplo, presença de facilidades de reconciliação de contas de utilizador gerais) que podem afetar a segurança de um sistema.

Em algumas ineficácias gerais específicas (por exemplo, desenhos ineficazes para aplicações - ou seja, aplicações 2-tier com ligações a bases de dados e requisitos de alto nível) podem apresentar riscos para a aplicação, portanto atributos ineficazes (como desenho) podem ser destacados.

Para alterações aos sistemas existentes, apenas a parte dos requisitos de segurança e as medidas afetadas pela alteração deverão ser verificadas. Para grandes alterações, é aconselhável realizar uma verificação de conformidade de todos os requisitos e medidas.

Output: como um resultado deste passo, os controlos ineficazes e os requisitos de segurança implementados ineficazes são resumidos. Os resultados são preparados de tal forma que eles podem ser ainda processados no passo de avaliação do risco residual.

Para sistemas de alta criticidade, a verificação de conformidade deve incluir uma avaliação da situação de cumprimento dos requisitos e medidas.

3.3.6. Avaliar o risco residual

Descrição: A avaliação de riscos residuais envolve toda a informação recolhida nas etapas anteriores e resume o resultado com um valor único por ameaça.

Quando: As avaliações de risco podem ser realizadas pelo menos até à entrada em produção ou quando haja alterações aos requisitos de segurança e controlos.

Input: o resultado da avaliação da eficácia dos controlos, os requisitos de segurança ineficazes implementados e potenciais efeitos sobre outros sistemas e conhecimentos adquiridos

Atividade: para projetos e pedidos de alteração:

Com base na análise de ameaça (passo 2), a eficácia da matriz ameaça / controlo a probabilidade (passo 3) e a verificação de conformidade (passo 5), a avaliação de riscos residuais (passo 6) mapeia cada ameaça para a matriz.

Uma ameaça que não foi mitigada por/ através dos controlos constitui definitivamente um risco residual.

Se algum dos controlos de segurança não foram corretamente executados durante o projeto roll-out, então há uma situação de risco remanescente associado que deve ser descrito. Passo 6 refere-se à avaliação deste risco residual, o resultado da etapa 6 é a atribuição de um valor numérico (e correspondente cor visual) da escala à ameaça correspondente. A última coluna do quadro seguinte representa um exemplo de um resultado do passo 6; cada ameaça acabará por ter um "nível de risco" associado:

#	Threat Name	Threat Description	Impact Assessment			Residual Threat Priority	Threat ORM Mapping
			C	I	A		
E	External attack						
E01	Carrying out denial of service attacks	Deliberately attacking a system with the intention of rendering the service unavailable to the legitimate business users.	N/A	N/A	VH	120000	3
E02	Hacking	Gaining unauthorised access to business systems and the data contained therein.	N	H	N/A	12012	2
E03	Undertaking malicious probes or scans	Performing technical information gathering on a business system with the aim of attacking it to gain unauthorised access to the business applications and data contained therein.	N	N/A	N/A	12	1
E04	Cracking passwords	Determining passwords for legitimate users in order to gain unauthorised access to business applications and data contained therein.	N	H	N/A	12012	2
E05	Cracking keys	Determining encryption keys for legitimate connections to a business service in order to gain unauthorised access to business applications and data contained therein.	N	N/A	N/A	12	1
E06	Defacing web sites	Unauthorised modification of web site content with the intention of negatively affecting the reputation of the organisation.	N/A	M	N/A	1200	2
E07	Spoofing web sites	Intentionally redirecting legitimate business users to unauthorised web sites.	N	M	N/A	1212	2
E08	Spoofing user identities	Gaining unauthorised access to business systems and the information contained therein by impersonating legitimate users (e.g. stealing valid user names and passwords).	N	H	VH	132012	3
E09	Modifying network traffic	Intercepting network traffic and rendering a service unavailable to legitimate business users and/or manipulating business data.	N/A	H	VH	132000	3
E10	Eavesdropping	Intercepting information in transit between legitimate business users and the application to gain unauthorised access to the business data contained therein.	N	N/A	N/A	12	1
E11	Introducing malicious code	Introducing malware (malicious code, virus, spyware or adware) in order to gain unauthorised access to the application and/or to manipulate the business data contained therein.	N	H	N/A	12012	2
E12	Carrying out social engineering	Deliberately eliciting information from staff that can be used to gain unauthorised to a business system and the data contained therein.	N	H	N/A	12012	2
E13	Distributing SPAM	Excessive distribution of unsolicited messages (including e-mail, instant messaging and telephony) negatively affecting the performance of a business service rendering it unavailable to legitimate users.	N/A	N/A	L	120	1

Figura 26 - Avaliação de Risco Residual

O "risco inerente" e "prioridade da ameaça" já foram quantificados no passo 2. O "risco efetivo" é o resultado da etapa 5. A "probabilidade do Risco" é calculado, dentro da atual etapa 6, através do mapeamento da "probabilidade efetiva" para o ORM nas cinco fases da escala de classificação. O "impacto do Risco" retorna o maior valor de um conjunto de valores do passo 2 da avaliação CA. As ameaças relevantes, a avaliação da eficácia dos controlos, matriz de ameaças / controlos são combinados de acordo com uma função matemática para determinar em grande parte as ameaças não mitigadas.

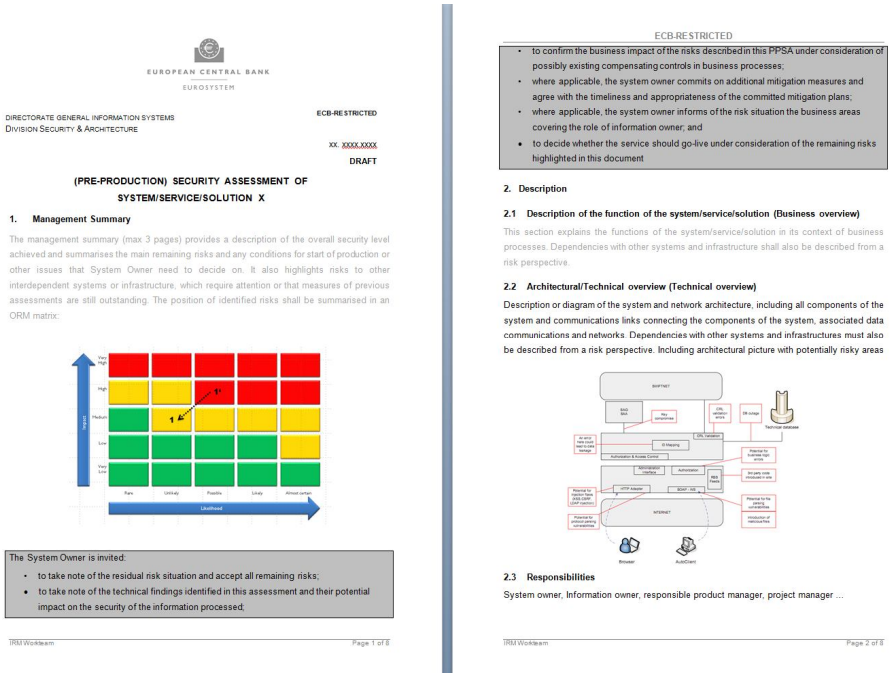
Passo 5 produto final é a Avaliação de Segurança de Pré-Produção (PPSA). Os resultados PPSA em uma "fotografia" a situação de risco remanescente antes de o sistema entrar em produção. O PPSA também poderia documentar medidas de segurança adicionais (se houver) que ainda estão

para ser implementadas, quer antes, ou depois, de entrar em produção.O PPSA baseia-se nos resultados e na verificação do estado da segurança do sistema realizado através dos primeiros seis passos. Dependendo da criticidade do sistema o resultado analítico PPSA pode ser apoiado com uma contribuição técnica suplementar apresentada por um teste de penetração.

Antes da entrada em produção o proprietário do sistema assume a responsabilidade por quaisquer riscos remanescentes, ao aceitar o risco remanescente (se houver) e compromete-se com a implementação de medidas de proteção adicionais adequadamente previstas no plano de follow-up do PPSA (se houver). Em suma:

1. O proprietário do sistema toma conhecimento da situação de risco residual e aceita todos os riscos remanescentes;
2. Se for caso disso, o proprietário do sistema compromete-se em medidas adicionais de mitigação e / ou concorda com um plano de ação; e
3. Se for caso disso, o proprietário do sistema informa sobre a situação de risco as áreas de negócio, abrangendo o papel do proprietário da informação.

A figura seguinte representa um exemplo de um PPSA:



EUROPEAN CENTRAL BANK
EUROSYSTEM

DIRECTORATE GENERAL INFORMATION SYSTEMS
DIVISION SECURITY & ARCHITECTURE

ECB-RESTRICTED

xx xxxx.xxxx
DRAFT

(PRE-PRODUCTION) SECURITY ASSESSMENT OF SYSTEM/SERVICE/SOLUTION X

1. Management Summary

The management summary (max 3 pages) provides a description of the overall security level achieved and summarises the main remaining risks and any conditions for start of production or other issues that System Owner need to decide on. It also highlights risks to other interdependent systems or infrastructure, which require attention or that measures of previous assessments are still outstanding. The position of identified risks shall be summarised in an ORM matrix:

The System Owner is invited:
- to take note of the residual risk situation and accept all remaining risks;
- to take note of the technical findings identified in this assessment and their potential impact on the security of the information processed;

IRM Workteam Page 1 of 8

ECB-RESTRICTED

- to confirm the business impact of the risks described in this PPSA under consideration of possibly existing compensating controls in business processes;
- where applicable, the system owner commits on additional mitigation measures and agree with the timeliness and appropriateness of the committed mitigation plans;
- where applicable, the system owner informs of the risk situation the business areas covering the role of information owner; and
- to decide whether the service should go-live under consideration of the remaining risks highlighted in this document

2. Description

2.1 Description of the function of the system/service/solution (Business overview)

This section explains the functions of the system/service/solution in its context of business processes. Dependencies with other systems and infrastructure shall also be described from a risk perspective.

2.2 Architectural/Technical overview (Technical overview)

Description or diagram of the system and network architecture, including all components of the system and communications links connecting the components of the system, associated data communications and networks. Dependencies with other systems and infrastructures must also be described from a risk perspective. Including architectural picture with potentially risky areas

2.3 Responsibilities

System owner, Information owner, responsible product manager, project manager ...

IRM Workteam Page 2 of 8

Figura 27 – Pre-Production Security Assessment (PPSA)

Agora que os riscos remanescentes foram identificados e classificados de acordo com, com base no seu impacto potencial, os riscos de IT já foram traduzidos para riscos de negócio e uma classificação de risco foi atribuída de acordo com a escala de classificação de

probabilidades ORM, e (quando aplicável) medidas de proteção adicionais identificadas, o próximo passo será fazer face aos riscos remanescentes. Este é exatamente o que acontece com o último passo da metodologia.

Output: Riscos associados aos sistemas e a alterações de forma agregada e um plano de ação.

3.3.7. Relatório e aceitação

Aceitar os riscos remanescentes e, se for caso disso, implementar medidas adicionais.

Descrição: Finalmente, o proprietário do sistema deve assumir a responsabilidade por quaisquer riscos remanescentes antes de o sistema passar a produção, e para a aplicação das salvaguardas ou medidas adicionais apropriadas antes e / ou após a data da entrada em produção.

Para sistemas com uma avaliação de criticidade "muito elevado", a avaliação de segurança de pré-produção (PPSA) deve ser efetuado por um especialista em segurança que seja independente da equipa de projeto e do proprietário do sistema.

Quando: O proprietário do sistema assume a responsabilidade por quaisquer riscos residuais antes do sistema entrar em produção ou alterado de forma significativa, e para a implementação de medidas adicionais adequadas ou medidas antes e / ou após a data da entrada em produção.

Input: a avaliação de segurança de pré-produção descrevendo a situação de risco, que consiste nos riscos remanescentes e, quando aplicável, uma lista de medidas de segurança adicionais e o calendário proposto para a sua implementação.

Atividade: para projetos e pedidos de alteração:

1. O proprietário do sistema deve tomar nota da situação de risco residual e aceitar todos os riscos remanescentes;
2. Se for caso disso o sistema deve priorizar as propostas medidas adicionais de mitigação;
3. Se for caso disso, o proprietário do sistema deve informar essas áreas de negócio que possuem informação no sistema sobre a situação de risco.

Output: como resultado desta etapa, tem-se a situação de risco final aprovado, que compreende os riscos remanescentes aceites, as medidas de mitigação adicionais propostas e o necessário Plano de execução, devem estar documentados.

Esta etapa documenta a situação de risco final aprovada, a aceitação dos riscos remanescentes e a proposta de medidas adicionais de mitigação e o comprometimento num plano de acompanhamento. Dois resultados são produzidos na etapa 7 e ambos são um inputpara o IRMv3:

- "Plano de tratamento de riscos" (PTR) - com o PTR um risco tanto pode ser aceite ou

reduzido (ou seja eliminado) ou partilhado (ou seja transferido) ou evitado. O especialista em segurança pode, nesta fase, fazer uma sugestão para melhoria ou implementação de novos controlos, um cenário “what-if” pode ser considerado e o especialista em riscos de IT pode reorganizar o plano em termos de relevância e risco. A PTR enumera todas as situações de risco e os níveis de risco associados com base na escala de classificação ORM, identifica ações e retoma o compromisso da equipa de projeto para a sua conclusão num período de tempo definido;

• "Aceitação do risco formal" - o proprietário do sistema pode aceitar riscos residuais. Estes dois resultados finais completam a metodologia e encerram todas as informações recolhidas até agora.

CONCLUSÕES

O trabalho desenvolvido, aplicado ao contexto do sector financeiro, nomeadamente o Sistema Europeu de Bancos Centrais, e que se apresenta nesta forma escrita, envolveu uma diversidade de temáticas, nomeadamente as áreas (Pessoas, SI, TIC, informação, risco e segurança da informação e SI), teve como objetivo analisar a atual metodologia de Information Risk Management (IRMv2), utilizada pelos bancos centrais na gestão da segurança dos sistemas de informação. De modo a poder atingir-se os objetivos identificados tornou-se necessário considerar as implicações da implementação da componente de gestão de risco e como a mesma era percecionada pelas partes interessadas.

Como principais conclusões da análise destaca-se as seguintes oportunidades de melhoria:

- Atualização do standard da ISO27002:2005 para ISO27002:2013;
- Conceptualizar a metodologia com uma vertente de gestão de risco;
- Relacionar os sistemas de informação com os processos de negócio, pela identificação como o negócio é impactado pelos riscos dos sistemas de informação;
- A metodologia atual é baseada num catálogo de segurança, que remonta a 2005, e entretanto os riscos de IT e as ameaças evoluíram de forma significativa e rapidamente.

De forma breve estes foram os principais resultados, e os mesmos tornam-se críticos quando o sector financeiro nomeadamente no âmbito do Sistema Europeu de Bancos Centrais, os processos de negócio tem uma grande dependência dos SI, e nesse sentido considera-se crítico uma adequada gestão do risco associado.

Considerando a necessidade enunciada e de modo a que se possa gerir os riscos para a organização que estão associados com os sistemas de informação, uma avaliação global do risco será necessário para:

- Sistemas novos; ou
- Atualizações relevantes para sistema existentes.

Com base nos resultados foi identificado que a atual metodologia carecia de uma componente de gestão risco, constatando-se que havia a necessidade de identificar e definir 3 novas fases para uma adequada gestão do risco associado aos sistemas de informação.

De modo sucinto passa-se a descrever cada uma das fases da metodologia proposta:

A avaliação da criticidade [Passo 1] não é substancialmente inalterada quando comparada com a anterior metodologia; contínua a ser uma classificação de confidencialidade, integridade e disponibilidade de acordo com uma escala de cinco níveis.

A análise de ameaças [passo 2] faz uma mudança disruptiva quando comparada com a metodologia anterior:

- Agora, a criticidade do sistema é efetuada para cada ameaça individual;
- Uma nova lista de ameaças está disponível;
- Estima-se o impacto de cada ameaça individual;
- Estima-se uma probabilidade de ameaça intrínseca, da atribuição de pesos a cada ameaça;
- Eventualmente, as ameaças são priorizadas a partir da mais relevante para a menos relevante.

A matriz de ameaça / controlo [passo 3] também contém pelo menos duas inovações, a lista de controlos vem da versão 2013 da norma ISO 27002 (enquanto o anterior foi uma versão de 2005), e os controlos agora são medidos em termos de capacidade de mitigar uma ameaça específica de acordo com uma matriz predefinida.

A identificação e seleção de requisitos de segurança [Passo 4] serão agora priorizadas, enquanto antes não eram; os controlos selecionados e priorizados são, então, entregues à equipa de projeto para a implementação.

A verificação da conformidade [passo 5] tanto apresenta semelhanças com a versão anterior da metodologia como introduz novos elementos; a mesma será executada quando a equipa de projeto tenha concluído a implementação; será utilizado a mesma grelha de pontuação (entre 0 e 3); enquanto a lista de controlos em relação ao qual o exercício é executado deriva da lista atualizada introduzida com a etapa 4.

A avaliação de riscos residuais [etapa 6] contínua a ser uma finalização de toda a informação recolhida nas etapas anteriores, mas agora assentará numa base muito diferente, agora é concetualmente focada na ameaça. O Relatório e aceitação [passo 7] segue a mesma linha da versão anterior.

A principal vantagem desta nova abordagem, revela-se no facto de que a metodologia estará agora muito mais em sintonia com ameaças chave de IT e os riscos, e proporciona um sistema de gestão de segurança de informação mais eficaz. De um modo geral, trata-se de um processo global de mitigação de riscos em relação aos ativos de SI que são melhorados.

O seu objetivo será assegurar que a segurança da informação é tratada adequadamente em cada fase do ciclo-de-vida do sistema. Desenvolver a segurança em sistemas durante o seu desenvolvimento é mais eficaz e seguro, do que quando realizadas numa fase posterior ao seu desenvolvimento.

REFERÊNCIAS

Committee Draft for Vote. (2008). *IEC 31010 Ed. 1.0: Risk Management - Risk Assessment Techniques.* International Electrotechnical Commission.

Gaivéu, J. (2008). *As Pessoas nos Sistemas de Gestão da Segurança da Informação.* Tese de Doutoramento em Informática. Setúbal: IPS - Escola Superior de Ciências Empresariais.

IT Governance Institute. (2003). *Board Briefing on IT Governance* (2nd ed.). United States of America: ITGI.

IT Governance Institute. (2006). *IT Control Objectives for Sarbanes-Oxley: The Role of IT in the Design and Implementation of Internal Control Over Financial Reporting* (2nd ed.). United States of America: ITGI.

IT Governance Institute. (2006). IT Control Objectives for Sarbanes-Oxley: The Role of IT in the Design and Implementation of Internal Control Over Financial Reporting. United States of America: ITGI.

IT Governance Institute. (2007). *COBIT 4.1: Framework Control Objectives Management Guidelines Maturity Models.* United States of America: ITGI.

IT Governance Institute. (2007). *IT Control Objectives for Basel II: The Importance of Governance and Risk Management for Compliance.* United States of America: ITGI.

Metcalfe, J. (2014). *IRAM2 - The next generation of assessing information risk.* Information Security Forum Limited.

PricewaterhouseCoopers. (2014). *IT Governance, Alinhar as Tecnologias de Informação com o negócio.* Lisboa: Academia da PwC.

PricewaterhouseCoopers LLP. (2004). *Enterprise Risk Management Framework - Executive Summary.* Committee of Sponsoring Organizations of the Treadway Commission (COSO).

PricewaterhouseCoopers LLP. (2005). *Internal Control Integrated Framework: Guidance for Smaller Public Companies Reporting on Internal Control over Financial Reporting - Executive Summary Guidance.* Committee of Sponsoring Organizations of the Treadway Commission (COSO).

Risk Management Group. (2001). *Sound Practices for the Management and Supervision of Operational Risk.* Basel Committee on Banking Supervision.

SRM TF. (2014). *ESCB Information Systems Risk Management Methodology.* Frankfurt: ESCB.

Stoneburner, G., Goguen, A., & Feringa, A. (2002). *Risk Management Guide for Information Technology Systems NIST SP 800-30.* Gaithersburg: National Institute of Standards and Technology.

Subcommittee SC 27, IT Security techniques. (2002). *Risk management – Vocabulary Guidelines for use in standards ISO/IEC Guide 73:2002.* Switzerland: ISO (the International Organization for Standardization) and IEC (the International Electrotechnical Commission).

Subcommittee SC 27, IT Security techniques. (2005). *Information technology - Code of pratice for information security management ISO/IEC 27002:2005.* Switzerland: ISO (the international Organization for Standardization) and IEC (the International Eletrotechnical Commission).

Subcommittee SC 27, IT Security techniques. (2005). *Information technology – Information security management systems – Requirements ISO/IEC 27001:2005.* Switzerland: ISO (the International Organization for Standardization) and IEC (the International Electrotechnical Commission).

Subcommittee SC 27, IT Security techniques. (2008). *Information Technology - Information security risk management ISO/IEC 27005:2008.* Switzerland: ISO (the International Organization for Standardization) and IEC (the International Electrotechnical Commission).

Subcommittee SC 27, IT Security techniques. (2013). *Information technology – Code of practice for information security management ISO/IEC 27002:2013* (2nd ed.). Switzerland: ISO (the International Organization for Standardization) and IEC (the International Electrotechnical Commission).

Subcommittee SC 27, IT Security techniques. (2013). *Information technology – Information security management systems – Requirements ISO/IEC 27001:2013* (2nd ed.). Switzerland: ISO (the International Organization for Standardization) and IEC (the International Electrotechnical Commission.

Whitepaper:

A Pathfinder Technology Solutions Whitepaper. (2004). *Regulatory Compliance - Needs Process Management.*

Silva, I., Veloso, A., & Keating, J. (2014). *Focus group: Considerações teóricas e metodológicas.* Revista Lusófona de Educação.

Links

AON. (s.d.). Disponível em www.aon.com

Committee of the Sponsoring Organizations of the Treadway Commission. (n.d.). Disponível em www.coso.org

Ernst & Young. (s.d.). Disponível em www.ey.com

Gartner. (s.d.). Disponível em http://www.gartner.com/it-glossary/it-governance

Information Security Forum. (s.d.). Disponível em https://www.securityforum.org/

Information Systems Audit and Control Association. (s.d.). Disponível em www.isaca.org

International Organization for Standardization. (s.d.). Disponível em www.iso.org/

IT Governance Institute. (s.d.). Disponível em www.itgi.org
PricewaterhouseCoopers. (n.d.). Disponível em www.pwc.pt
Public Company Oversight Board. (s.d.). Disponível em www.pcaobus.org

Anexos

Anexo 1: Termos e definições

Asset	Anything that is of value to the organisation, such as **information** (e.g. databases, data files), **software** (e.g. system software, application software), **physical assets** (e.g. processors, tapes, power supply), **services** (e.g. computing services, heating, air-conditioning) and **people** (e.g. users, consultants).
Awareness	Rasining consciousness regarding potential risks and threats to information systems which target human behaviour.
COBIT4.1	COBIT é um acrónimo constituído pelas letras Control Objectives for Information and related Technology. Tendo como Missão – Investigar, desenvolver, publicar e promover a autoridade, é um conjunto internacionalmente aceite de objetivos de controlos de IT aplicáveis diariamente no desempenho das suas funções pelos gestores de negócio e pelos auditores. O CobIT está em conformidade com o COSO e é uma Framework de IT internacionalmente aceite.
Control	Any action taken by management, the board, and other parties to manage risk and increase the likelihood that established objectives and goals will be achieved. Controls include any plan, process, policy, device, practice, or other actions which modify risk, and organize and direct the performance of sufficient actions to provide reasonable assurance that objectives and goals will be achieved. Controls may not always exert the intended or assumed modifying effect.
Control Catalogue	The catalogue containing a list of security controls and control enhancements for protecting information systems and managing IT security risks.
Control Effectiveness	The measure of correctness of implementation (i.e., how consistently the control implementation complies with the security plan) and how well the security plan meets organizational needs in accordance with current risk tolerance.
Control strength adjustment	A mapping of security controls against threats and control enhancements for protecting information systems and managing IT security risks.
Criticality	In business terms, something is deemed to be “critical” when it is urgently needed and/or absolutely necessary to achieve the business goals. All ESCB information systems have been put in place to support business functions and processes. Hence, it can be concluded that all ESCB information systems are important for the success of the ESCB’s business. Further, it can be assumed that most, if not all, of the information systems deployed are reliant upon the continued functioning of other information systems, especially the IT infrastructure such as the network, mail system, internet connection, telephone lines, etc. However, some are more crucial than others, and require a greater attention and better protection. For example, a business process may be able to continue more or less normally if the e-mail system has to be closed, but would come to a complete halt if a certain information system crashes, e.g. the core network.
Criticality Assessment (CA)	To identify the criticality of the IT solution to be implemented by the project, a criticality assessment reflecting the business impact of a potential loss of confidentiality, integrity or availability should be provided.
Effectiveness assessments	The measure of correctness of implementation (i.e., how consistently the control implementation complies with the security plan, security architecture document) and how well the security plan meets organizational needs in accordance with current risk tolerance.
Effective threat	The likelihood that a threat materialises after controls have been implemented.

likelihood	
Event	Occurrence or change of a particular set of circumstances. An event can be one or more occurrences, and can have several causes. An event can consist of something not happening. An event can sometimes be referred to as an "incident" or "accident".
Horizontal Services	Services what do not apply to specific solution but rather cover or can be adopted by a wider range of solutions
Impact	The result of an unwanted incident. The result of an unwanted incident. represents the potential effects and consequences that a given event could have on an entity and its objectives. An event can lead to a range of consequences. A consequence can be certain or uncertain and can have positive or negative effects on objectives. Events that have positive effects represent opportunities and those with negative effects represent risks. Consequences can be expressed qualitatively or quantitatively. Entities often describe events based on severity, effects, or monetary amounts. Initial consequences can escalate through knock-on effects.
Impact analysis	The process of identifying threats to the assets, and the impact such threats could have if it were to result in a genuine incident. Such analysis should quantify the value of the assets being protected, so as to enable a decision on the appropriate level of safeguards.
Information	The meaning that is currently assigned to data by means of the conventions applied to those data.
Inherent risk	The risk that remains before risk treatment.
Inhertited Criticality Requirement (ICR)	Criticality requirement derived based on criticality of a depending service.
Key risk indicator (KRI)	A management information indicator that provides continuous insight into the level of risk in the group/business. KRIs enable management to manage and monitor risk proactively on an ongoing basis. KRIs may be leading, concurrent or lagging indicators. (Note: It is preferable to focus on leading indicators proactively to prevent a risk from materialising).
Likelihood	Chance of something happening. In risk management terminology the word “likelihood” is used to refer to the chance of something happening, whether defined, measured or determined objectively or subjectively, qualitatively or quantitatively, and described using general terms or mathematically (such as a probability or a frequency over a given time period).
Intrinsic Likelihood	The likelihood belonging to a service or asset by its very nature.
Likelihood of Initiation	The likelihood of a weakness being initiated.
Likelihood of Success	The liklihood of a weakness being realized and thus causing an impact.
Maximum Tolerable Outage (MTO)	Defines the maximum tolerable outage of service. The MTO should be defined on the situation of normal operations and can be different for crisis situations.

Operational risk	The risk of loss resulting from inadequate or failed internal processes, people or systems or from external events. This includes legal risk, but excludes strategic risk and reputational risk. The subrisks of operational risk are: • business disruption and system failures; • clients, products and business practices; • damage to physical assets; • employment practices and workplace safety; • execution, delivery and process management; • external fraud; • internal fraud; • legal risk (legal risk is a subcategory of the subrisk clients, products and business practices); and • model risk (for economic capital purposes, model risk is a subcategory of the subrisk clients, products and business practices).
Pre-Production Security Assessment (PPSA)	Risk assessment which is prepared by the ITC's security experts.. The PPSA including a recommendation from the ITC are forwarded to the System Owner for approval. The recommendation may include mitigating measures to be implemented and an invitation to accept the residual risks.
Priority calculation	Priority calculation is a predefined set of values that automatically set a priority level for the different controls to be implemented.
Residual Risks assessment	Risk assessment which is prepared by the ITC's security experts following the development of an IT system and the risks that remains after risk treatment, but before it goes live
Residual risk	The risk that remains after risk treatment.
Resilience	The abbility to recover from an incident or to maintain adequate level of service.
Risk	The possibility of an event occurring that will have an effect on the achievement of objectives. An effect is a deviation from the expected (positive and/or negative). Objectives can have different aspects (such as financial, health and safety, and environmental goals) and can apply at different levels (such as strategic, organization-wide, project, product and process). All activities of an organization involve risk. Organizations manage risk by identifying it, analysing it and then evaluating whether the risk should be modified by risk treatment in order to satisfy their risk criteria. Risk is often characterized by reference to potential events and impact, or a combination of these. Risk is measured in terms of impact (including changes in circumstances) and likelihood of occurrence. Uncertainty is the state, even partial, of deficiency of information related to, understanding or knowledge of an event, its consequences, or likelihood.
Risk analysis	Systematic use of information to identify sources of, and to estimate, risk
Risk appetite	Amount and type of risk that an organization is willing and prepared to accept as it tries to achieve its goal and provide value to stakeholders. Risk appetite is a higher level statement that considers broadly the levels of risks that management deems acceptable. It reflects the enterprise's risk management philosophy, and in turn influences the entity's culture and operating style. Many entities define their risk appetite qualitative, while other take a more quantitative approach.
Risk assessment	The overall process of risk analysis and risk evaluation.
Risk evaluation	Process of comparing the estimated risk against risk criteria to determine the

	significance of risk.
Risk identification	Process of finding, recognizing and describing risks. Risk identification involves the identification of risk sources, events, their causes and their potential consequences. Risk identification can involve historical data, theoretical analysis, informed and expert opinions, and stakeholder's needs.
Risk Level	The level that results from the product of the likelihhod that a weakness is being exploited multiplied by the impact of the materilization of that weakness.
Risk management	Coordinated activities to direct and control an organisation with regard to risk, i.e. the ongoing process of risk assessment (evaluation of the impact or system criticality, and the likelihood of loss/damage occurring), leading to the definition of security requirements and the additional mitigation (by safeguards) and/or acceptance of residual risks.
Risk owner	Person or entity with the accountability and authority to manage the risk.
Risk tolerance	The acceptable level of variation relative to achievement of a specific objective. This variation is often measured using the same units as its related objective. In setting risk tolerance, management considers the relative importance of the related objective and aligns risk tolerances with risk appetite. Therefore, an entity operating with its risk tolerances, narrow boundaries, is operating within its risk appetite, wide boundaries
Risk treatment	Means by which an organization elects to manage individual risks. Risk treatments can also be called risk responses. As part of enterprise risk management, for each significant risk an entity considers potential responses from a range of response categories. Risk treatment can involve: • Avoidance/Terminating is a response where you exit the activities that cause the risk. Some examples of avoidance are exiting product line, selling a division, or deciding against expansion. • Treating/Reduction is a response where action is taken to mitigate the risk likelihood and impact, or both. • Transferring/Sharing is a response that reduces the risk likelihood and impact by sharing or transferring a portion of the risk. An extremely common sharing response is insurance. • Tolerance/Acceptance is a response where no action is taken to affect the risk likelihood or impact. • Risk treatments that deal with negative consequences are sometimes referred to as "risk mitigation", "risk elimination", "risk prevention" and "risk reduction". Risk treatment can create new risks or modify existing risks.
Risk Register	The document containing the results of the qualitative risk analysis, quantitative risk analysis, and risk response planning. The risk register details all identified risks, including description, category, cause, probability of occurring, impact(s) on objectives, proposed responses, owners, and current status. The risk register is a component of the project management plan.
Risk Report	The document containing the results of the qualitative risk analysis, quantitative risk analysis, and risk response planning.
Threat	A potential cause of an unwanted incident, which may result in harm to the system or the organisation.
Threat Analysis	An evaluation of the type, scope and nature of events or actions that can result in adverse consequences; identification of the threats that exist against enterprise assets Scope Note: The threat analysis usually defines the level of threat and the

	likelihood of it materializing.
Threat-Control Matrix	A mapping of security controls against threats and control enhancements for protecting information systems and managing IT security risks.
Threat Impact	The impact of a threat on a information system or services
Trigger	An event that activates the risk management process, such as a new or changed business case, a change request, an incident, a new threat, etc.
Recovery Time Objective (RTO)	Service Operation) The maximum time allowed for recovery of an IT Service following an interruption. The Service Level to be provided may be less than normal Service Level Targets. Recovery Time Objectives for each IT Service should be negotiated, agreed and documented.
Vulnerability	A weakness of an asset, or a group of assets, that can be exploited by a threat.

Anexo 2: Avaliação da Criticidade do Sistema

General Information			
System Name			
System Owner		MTO	
Project Name		Project Code	

System Description			
End Users			
Connection to Internet		Non Repudation	
Does the system store personal data?		What is the highest classification of stored documents?	
General Desription			

Document Information			
Name(s) of staff member(s) filling in the form		Document Status	
Approval Name		Approval Date	

	Area	Confidentiality		Integrity		Avalability	
		if information is disclosed?		if information is erroneous or manipulated?		if information is not available when required?	
		Maximum Impact	Comment	Maximum Impact	Comment	Maximum Impact	Comment
Business Impact	Could there be an impact on market stability?						
	How damaging would it be for the ESCB's business objectives?						
	Could there be a breach of legal, regulatory or contractual obligations?						
	Where applicable, would there be a competitive disadvantage?						
Reputation Impact	What damage could there be to public confidence and reputation of the ESCB or the Euro?						
	Could financial gain be achieved on the market?						
Financial Impact	Could costs be incurred?						
Overall Rating		N/A		N/A		N/A	

Anexo 3: Tabela - Classificação de Risco de Impacto

A avaliação da criticidade do sistema deve ser executada pela respostas às perguntas infra. A tabela faculta as orientações para determinar a criticidade de um sistema de informação.

Impact	Area	Very High	High	Medium	Low	Negligible
Business Impact	Could there be an impact on market stability?	Unwanted adverse market reactions and significant market movement over a period > 1 week	Unwanted adverse market reactions and significant market movement between one day to one week	Market irritation and unwanted significant market movements during one day	Temporary market irritation and limited unwanted market movements during less than one day	No noticeable market reaction
	How damaging would it be for the ESCB's business objectives?	Failure to deliver on statutory tasks	Partial failure to deliver on statutory tasks or failure to deliver on advisory functions or complete failure to achieve strategic objective	Unsatisfactory quality or significant delays in delivery on statutory tasks or partial failure to meet strategic objectives	Statutory tasks and strategic objectives still may be achieved, however internal business expectations not being met due to a delay in delivery, or deterioration in quality	Internal tasks and business processes affects, however statutory tasks or strategic objectives not affected
	Could there be a breach of legal, regulatory or contractual obligations?	Serious sanctions imposed. Breach or legal action leading to significant impact on multiple other criteria	Sanctions imposed. Breach or legal action leading to significant impact on one of the other criteria	Regulations breached. Breach leading to serious impact on one of the other criteria	Little regulatory or legal impact. Breach leading to little impact on one of the other criteria	No legal, regulatory or contractual impact
	Where applicable, would there be a competitive disadvantage?	More than 25% loss of transactions/users or more than €10.000.000, whichever is higher	Between 10% and 25% loss of transactions/users or up to €10.000.000, whichever is higher	Between 1% and 10% loss of transactions/users or up to €1.000.000, whichever is higher	Less than a 1% loss of transactions/users or up to €50.000, whichever is higher	Negligible loss of transactions/users or up to €1.000
Reputation impact	What damage could there be to public confidence and reputation of the ESCB or the Euro?	Credibility affected over 3 years	Credibility affected between 1 year up to 3 years	Credibility affected between 3 months up to 1 year	Credibility affected between 1 week up to 3 months	Credibility affected below 1 week
	Could financial gain be achieved on the market?	More than €1.000.000	Between €100.000 up to €1.000.000	Between €1.000 up to €100.000	Less than €1.000	None
Financial impact	Could costs be incurred?	Above €10.000.000	Between €1.000.000 up to €10.000.000	Between €100.000 up to €1.000.000	Between €10.000 up to €100.000	Less than €10.000

Anexo 4: Lista de Ameaças

A lista de ameaças do Information Security Forum (ISF) pode ser utilizado para identificar riscos relacionados com situações de não conformidades na avaliação de segurança de pré-produção.

Threat ID	Threats	Business View
External Attack		
E01	Carrying out denial of service attacks	Deliberately attacking a system with the intention of rendering the service
E02	Hacking	Gaining unauthorised access to business systems and the data contained therein.
E03	Undertaking malicious probes or scans	Performing technical information gathering on a business system with the aim of attacking it to gain unauthorised access to the business applications and data contained therein.
E04	Cracking passwords	Determining passwords for legitimate users in order to gain unauthorised access to business applications and data contained therein.
E05	Cracking keys	Determining encryption keys for legitimate connections to a business service in order to gain unauthorised access to business applications and data contained therein.
E06	Defacing web sites	Unauthorised modification of web site content with the intention of negatively affecting the reputation of the organisation.
E07	Spoofing web sites	Intentionally redirecting legitimate business users to unauthorised web sites.
E08	Spoofing user identities	Gaining unauthorised access to business systems and the information contained therein by impersonating legitimate users (e.g. stealing valid user names and passwords).
E09	Modifying network traffic	Intercepting network traffic and rendering a service unavailable to legitimate business users and/or manipulating business data.
E10	Eavesdropping	Intercepting information in transit between legitimate business users and the application to gain unauthorised access to the business data contained

Threat ID	Threats	Business View
		therein.
E11	Introducing malicious code	Introducing malware (malicious code, virus, spyware or adware) in order to gain unauthorised access to the application and/or to manipulate the business data contained therein.
E12	Carrying out social engineering	Deliberately eliciting information from staff that can be used to gain unauthorised to a business system and the data contained therein.
E13	Distributing SPAM	Excessive distribution of unsolicited messages (including e-mail, instant messaging and telephony) negatively affecting the performance of a business service rendering it unavailable to legitimate users.
I01	Gaining unauthorised access to systems or networks	Gaining unauthorised access to business systems and the data contained therein (e.g. through password theft or other covert actions).
I02	Changing system privileges without authorisation	Changing system privileges without authorisation in order to negatively affect the performance of a business service rendering it unavailable to legitimate business users and/or to manipulate the data contained therein.
I03	Changing or adding software without authorisation	Modifying or adding software without authorisation in order to produce unwanted system behaviour resulting in rendering the business service unavailable to legitimate business users or manipulating the data contained therein.
I04	Modifying or inserting transactions, files or databases without authorisation	Modifying or adding transactions, files or databases without authorisation in order to produce unwanted system behaviour resulting in rendering the business service unavailable to legitimate business users or manipulating the data contained therein.
I05	Misusing systems to cause disruption	Misusing systems and negatively affecting the performance of a business service rendering it unavailable to legitimate business users (e.g. uploading or downloading high volume of .mp3/.mpeg files causing poor network response times).
I06	Misusing systems to commit fraud	Deliberately misusing business applications to defraud the organisation (e.g. diverting goods to different address, diverting funds to personal accounts, etc.)
I07	Denial of actions	Denial of actions leading to a lack of proof (person who denies having received a message or having carried an

Threat ID	Threats	Business View
		action)
I08	Installing unauthorised software	Installing software without authorisation and negatively affecting the performance of a business service rendering it unavailable to legitimate business users and/or manipulating the data contained therein.
I09	Disclosing authentication information	Disclosure of user authentication details (e.g. sharing user profile and password) leading to unauthorised access to business systems and data contained therein.
I10	Disclosing business information	Disclosure of business information by unauthorised personnel (e.g. confidential financial information) leading to a breach in confidentiality.
T01	Software piracy	The unauthorised copying of software rendering the organisation liable to legal action.
T02	Theft of business information	Theft of business information (e.g. customer lists, product designs, intellectual property) rendering the organisation liable to legal action.
T03	Theft of identity information (eg as a result of Phishing)	Theft of personally identifiable information (e.g. credit card numbers, employment IDs, personal health details) rendering the organisation liable to legal action.
T04	Theft of physical assets	Theft of physical assets (e.g. computer equipment, communications equipment and other devices) in order to render the business service unavailable to the legitimate business users.
T05	Theft of portable computers and storage devices	Theft of portable computers and storage devices (e.g. laptops, PDAs, mobile phones, removable media) in order to render the business service unavailable to the legitimate business users and/or to gain unauthorised access to business information.
T06	Theft of authentication information	Theft of authentication information (e.g. user IDs, passwords and PINs) in order to gain unauthorised access to business information.
T07	Theft of software	Theft of software (e.g. programs and methodologies) in order to render the business service unavailable to the legitimate business users and/or to gain unauthorised access to business information.

Threat ID	Threats	Business View
System Malfunction		
M01	Breach of information system maintainability	Breach of information system maintainability possibly leading to the business service being unavailable to the legitimate business users and/or rendering it possible to gain unauthorised access to or manipulate business information.
M02	Malfunction of business application software developed in-house	Malfunction of business application software developed in-house (e.g. a software "bug") possibly leading to the business service being unavailable to the legitimate business users and/or rendering it possible to gain unauthorised access to or manipulate business information.
M03	Malfunction of business application software acquired from an external party	Malfunction of business application software acquired from a third party (e.g. SAP R/3, Baan IV, Oracle Financials) possibly leading to the business service being unavailable to the legitimate business users and/or rendering it possible to gain unauthorised access to or manipulate business information.
M04	Malfunction of system software	Malfunction of system software (e.g. operating system software or utilities) possibly leading to the business service being unavailable to the legitimate business users and/or rendering it possible to gain unauthorised access to or manipulate business information.
M05	Malfunction of computer/network equipment	Malfunction of computer/network equipment (e.g. servers or routers) possibly leading to the business service being unavailable to the legitimate business users and/or rendering it possible to gain unauthorised access to or manipulate business information.
Service interruption		
S01	Damage to or loss of information processing facilities	Damage to or loss of information processing facilities (e.g. data centres, computer/network rooms, trading floors or process control systems) leading to the business service being unavailable to the legitimate business users.
S02	Damage to or loss of communications links/services.	Damage to or loss of communications links/services (e.g. SWIFT, Internet service provider (ISP), CoreNet network) leading to the business service being unavailable to the legitimate business users.
S03	Damage to or loss of external services	Damage to or loss of external services (e.g. IAM, PKI) leading to the business service being unavailable to the legitimate business users.
S04	Damage to or loss of	Damage to or loss of general utilities (e.g. heating,

Threat ID	Threats	Business View
	general utilities	lighting, air-conditioning) leading to the business service being unavailable to the legitimate business users.
S05	Loss of power	Failure of mains electricity or back-up power supply leading to the business service being unavailable to the legitimate business users.
S06	Natural disasters or major accident	The occurrence of natural disasters (e.g. earthquakes, fires and extreme weather) leading to the business service being unavailable to the legitimate business users.
S07	Physical terrorist attack	The occurrence of a physical terrorist attack (e.g. bomb attack) leading to the business service being unavailable to the legitimate business users.
S08	System overload	Excessive system activity causing performance degradation or failure, thus leading to the business service being unavailable to the legitimate business users.
S09	Disturbance due to radiation	Disturbance physical systems due to radiation leading to business service being unavailable to the legitimate business users.
Human error		
H01	Operational staff errors	Mistakes made by system users (e.g. input errors, incorrect operation of workstations, sending material to the wrong address) causing unwanted changes to the business information and/or rendering the business service unavailable to the legitimate business users.
H02	Technical staff errors	Mistakes made by staff responsible for operating and maintaining computers or networks causing unwanted changes to the business information and/or rendering the business service unavailable to the legitimate business users.
Unforeseen effect of changes		
U01	Unforeseen effects of introducing new/upgraded business processes	Introducing new/upgraded processes could potentially lead to unforeseen effects, such as, rendering the business application unavailable to legitimate business users, gaining unauthorised access to the system and/or allowing the manipulation of data contained therein.
U02	Unforeseen effect of	Changes in the software could potentially lead to unforeseen effects, such as, rendering the business

Threat ID	Threats	Business View
	changes to software	application unavailable to legitimate business users, gaining unauthorised access to the system and/or allowing the manipulation of data contained therein.
U03	Unforeseen effect of changes to business information	Changes in business information (e.g. customer lists, product designs and other intellectual property) could potentially lead to unforeseen effects, such as, rendering the business application unavailable to legitimate business users, gaining unauthorised access to the system and/or allowing the manipulation of data contained therein.
U04	Unforeseen effect of changes to computer/communications equipment	Changes in computer/communications equipment could potentially lead to unforeseen effects, such as, rendering the business application unavailable to legitimate business users, gaining unauthorised access to the system and/or allowing the manipulation of data contained therein.
U05	Unforeseen effects of organisational changes	Organisational changes (e.g. mergers, acquisitions, outsourcing or internal reorganisation) could potentially lead to unforeseen effects, such as, rendering the business application unavailable to legitimate business users, gaining unauthorised access to the system and/or allowing the manipulation of data contained therein.
U06	Unforeseen effects of changes to user processes or facilities	Changes in user processes or facilities (e.g. user/operating procedures, staffing, etc.) could potentially lead to unforeseen effects, such as, rendering the business application unavailable to legitimate business users, gaining unauthorised access to the system and/or allowing the manipulation of data contained therein.
Lawsuit		
L01	Repudiation of sent/received message	Users claiming not to have sent/received certain messages in order to undermine the integrity of (and confidence in) the business system or to render the organisation liable to legal action.
L02	Non-compliance with legal requirements within the scope of information security	Breaches of any law, statutory, regulatory or contractual obligations, and of any security requirements.

Anexo 5: Guião de Entrevista Semiestruturado

Caracterização do Entrevistado:

Focus Group – constituído por um grupo de especialistas em segurança da informação de bancos centrais do Sistema Europeu de Bancos Centrais (SEBC).

A resposta a este guião de entrevista semiestruturado, foi possível através da criação de um focus group em que os diversos intervenientes foram reunidos numa reunião de brainstorming, e com a ajuda das questões encadeadas foi possível reunir um conjunto de informação percecionada através das iterações ao longo de uma sessão de 3 dias que teve lugar em Estugarda.

Cada um dos intervenientes dava um input que era depois afixado num quadro para análise e discussão da sua pertinência e relevância, sendo que no final esse itens foram todos organizados por workstream e sua complexidade de realização (fácil, médio e ambicioso).

No anexo 7 é possível verificar como esse quadro foi organizado.

Caracterização da Empresa:

SEBC-Bancos Centrais - Zona geográfica: Zona Euro

Questões:

1. A metodologia atual responde às necessidades?
   - A metodologia atual não responde às necessidades, uma vez que a mesma é orientada à conformidade não transmitindo a necessidade de implementação dos requisitos de segurança na forma em que mitigam o risco.
   - O cliente (dono da aplicação) e a equipa de projeto não conseguem percecionar os benefícios que advêm da mitigação dos riscos, uma vez que a segurança de alguma forma é vista como um entrave/ custo ao desenvolvimento do sistema e com a atual metodologia não é possível percecionar os riscos que qualquer projeto de sistemas de informação incorre.

2. Quais as oportunidades de melhoria que identificaria?
   - Considerando as atuais fases da metodologia é possível constatar que falta a componente de gestão de risco, seria importante integrar numa proposta de novo modelo as componentes identificação de risco, análise de impacto e avaliação de risco residual.
   - A definição de uma lista de ameaças pré-definida genérica o suficiente para que seja aplicável a todos os projetos e possa de alguma forma mitigar o esforço necessário a identificar as ameaças para cada projeto.
   - Clarificação dos requisitos de segurança e relacionar com as ameaças que os mesmos mitigam.

- Existe a necessidade de o negócio e a equipa de desenvolvimento ter perceção de como a implementação dos requisitos ajudam a mitigar os riscos.
- Clarificação da linguagem utilizada, termos e definições.
- Definição de um glossário.
- Clarificação na forma de reportar os riscos críticos.

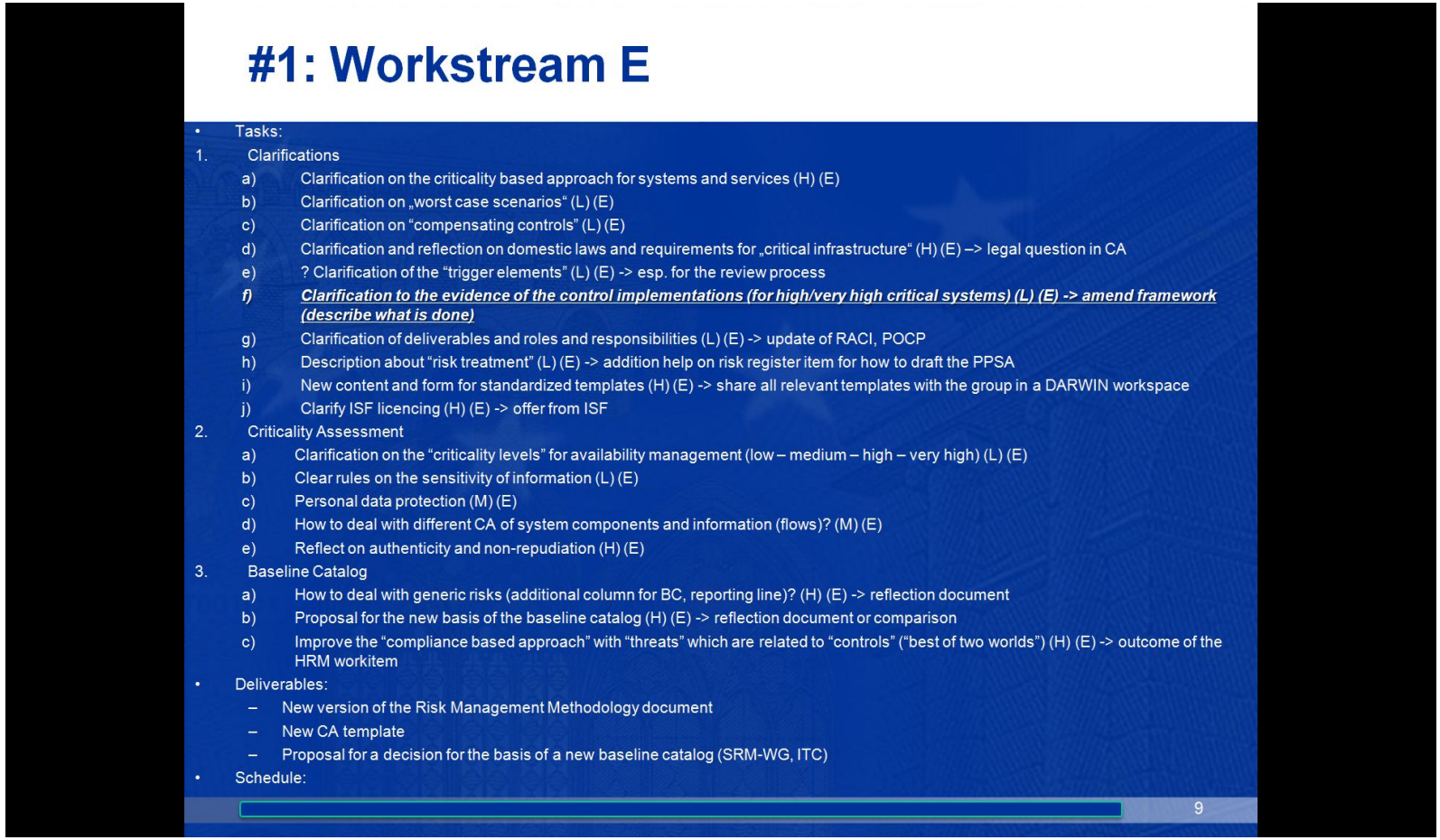
3. A metodologia encontra-se atualizada de acordo com a ISO27002:2013?
A atual metodologia está baseada na ISO27002:2005, considerando a importância de ter uma metodologia em conformidade, foi identificada a necessidade de que a proposta esteja à luz do novo standard.

4. Como é identificada a relação entre os sistemas de informação com os processos de negócio?
- Foi identificado que de momento não existe relacionamento entre os sistemas de informação com os processos de negócio. Nesse sentido, é possível constatar que com a definição de uma lista de ameaças será possível relacionar o SI com o processo de negócio que é afetado.
- Isto é, ao fazer o levantamento da criticidade do sistema, aproveita-se a oportunidade para identificar os processos de negócio que utilizam o sistema e como são afetados, desta forma é possível fazer esse relacionamento, pela identificação da ameaça e definição do impacto no sentido em que afeta o processo de negócio.

5. Quem deverá ser o público-alvo desta metodologia?

Com base nas iterações foi identificado que deverão ser todos aqueles que participam em atividades de gestão de risco, além do proprietário do sistema, o gestor de operações de TI, o gestor de projetos e restantes membros da equipa, especialistas em sistemas e colaboradores de segurança (peritos e operacionais), incluindo todos os colaboradores dentro da organização, que estejam envolvidos em atividades de desenvolvimento ou operação dos sistemas. Para facilitar o trabalho, mas também para garantir a qualidade comparável, especialistas em segurança devem ser envolvidos na execução das tarefas chave ou devem ser consultados sempre que necessário.

Anexo 7: Resultados da entrevista semiestruturada ao focus group



#1: Workstream E

- Tasks:

1. Clarifications
   - a) Clarification on the criticality based approach for systems and services (H) (E)
   - b) Clarification on „worst case scenarios“ (L) (E)
   - c) Clarification on “compensating controls” (L) (E)
   - d) Clarification and reflection on domestic laws and requirements for „critical infrastructure“ (H) (E) –> legal question in CA
   - e) ? Clarification of the “trigger elements” (L) (E) -> esp. for the review process
   - ***f) Clarification to the evidence of the control implementations (for high/very high critical systems) (L) (E) -> amend framework (describe what is done)***
   - g) Clarification of deliverables and roles and responsibilities (L) (E) -> update of RACI, POCP
   - h) Description about “risk treatment” (L) (E) -> addition help on risk register item for how to draft the PPSA
   - i) New content and form for standardized templates (H) (E) -> share all relevant templates with the group in a DARWIN workspace
   - j) Clarify ISF licencing (H) (E) -> offer from ISF
2. Criticality Assessment
   - a) Clarification on the “criticality levels” for availability management (low – medium – high – very high) (L) (E)
   - b) Clear rules on the sensitivity of information (L) (E)
   - c) Personal data protection (M) (E)
   - d) How to deal with different CA of system components and information (flows)? (M) (E)
   - e) Reflect on authenticity and non-repudiation (H) (E)
3. Baseline Catalog
   - a) How to deal with generic risks (additional column for BC, reporting line)? (H) (E) -> reflection document
   - b) Proposal for the new basis of the baseline catalog (H) (E) -> reflection document or comparison
   - c) Improve the “compliance based approach” with “threats” which are related to “controls” (“best of two worlds”) (H) (E) -> outcome of the HRM workitem

- Deliverables:
  - New version of the Risk Management Methodology document
  - New CA template
  - Proposal for a decision for the basis of a new baseline catalog (SRM-WG, ITC)
- Schedule:

9

#2: Workstream H

- Participants:
  - No participants

- Tasks:

1. Link the technical systems to business process (IRM and ORM) (H) (H)
2. Link with Availability Management: Responsibility for Availability (SLAs) (H) (H)
3. 3 levels of control severity (A – B – C) (H) (H)
4. Findings and risk review process (incl. risk register) must be improved (H) (H)
5. Speak the same language – Definition of terms, roles and responsibilities (H) (H)
6. Improve the compliance check (M) (H)
7. Reporting and compliance with processes and systems in operations (H) (H)
8. Business language for reporting (for threats) (H) (H)
9. How to report the relevant risks for shared services (regularly) to the system owner? (H) (H)
10. Risk classification (temp. / regularly reviewed / permanent) (M) (H)
11. Risk reporting and register (review) (H) (H)

- Deliverables:
  - Proposal for the new basis of the baseline catalog
  - The new baseline catalog

- Schedule:

#3: Workstream C

- Participants:
  - No participants

- Tasks:

1. Alignment of Baseline Catalog and Policies (H) (C)
2. Improve the content of the baseline catalog (H) (C)
3. Measures and controls should not be interpretable (“clear understanding”) (H) (C)
4. Improvement of the tool (“baseline catalog”, reporting, history) (H) (C)

- Deliverables:
  - Proposal for the new basis of the baseline catalog

- Schedule:
  - Start after the decision of the baseline basis