CONCEITOS DE SISTEMAS DE INFORMAÇÃO APLICADOS A GESTÃO DE RISCOS

José Barateiro[1,2] e José Borbinha[2]

[1] Laboratório Nacional de Engenharia Civil,
Lisboa, Portugal
jbarateiro@lnec.pt

[2] Instituto de Engenharia de Sistemas e Computadores Investigação e Desenvolvimento,
Lisboa, Portugal
jlb@ist.utl.pt

Resumo

O objetivo das atividades de gestão de risco consiste em definir um conjunto de mecanismos para controlar os riscos associados a atividades e recursos valiosos. Verifica-se que grande parte das atividades de gestão de risco opera em silos, conduzindo a uma visão fragmentada de riscos, na qual cada atividade usa a sua linguagem, princípios e métricas. Este facto limita a obtenção de uma perceção global, onde riscos interdependentes nem sempre são antecipados, controlados ou geridos. De forma a otimizar a visão global de riscos numa organização, este artigo propõe a aplicação à gestão de risco de conceitos já estabelecidos na governação dos sistemas de informação. Analisamos o exemplo da preservação digital, que é reconhecida como uma preocupação em gerir conteúdos valiosos ao longo do tempo, assegurando que a informação digital pode ser lida e usada num futuro imprevisível. Este é assim um problema interdisciplinar, no qual desafios tecnológicos intersetam objetivos organizacionais, requerendo a gestão de riscos a múltiplos níveis. Este artigo propõe uma solução integrada de gestão de risco que providencia uma visão holística de riscos com o objetivo de permitir que uma organização possa antecipar e gerir riscos de uma forma global.

1 Introdução

A gestão de risco é uma área em constante desenvolvimento, na qual o principal objetivo consiste em definir mecanismos de controlo para proteger

bens valiosos. A rápida identificação de riscos permite criar planos para reduzir o potencial impacto adverso dos mesmos (Software Engineering Institute, 2010). Um processo de gestão de risco define um conjunto de atividades para suportar a identificação e mitigação de riscos num contexto específico. Este artigo baseia-se na norma ISO 31000 (ISO 31000, 2009) e nas suas normas de suporte, considerando risco como a "…combinação entre a probabilidade de um evento (ameaça) e as suas consequências na exploração de uma vulnerabilidade de um bem ou recurso."

Analisar e modelar riscos constitui umas das tarefas mais críticas no processo de gestão de riscos. Dependendo do contexto ou do interesse, os riscos podem ser analisado de várias perspetivas, desde riscos de negócio, de mercado, de crédito, operacionais, tecnológicos (Barry Bohem, 1991, K. Lytinen et al, 2000), de engenharia, etc. Deste modo, várias estratégias e processos de gestão de risco têm sido desenvolvidos, como por exemplo em gestão de projetos, tecnologias de informação (incluindo segurança de informação), engenharia de segurança, etc. Áreas específicas como a militar (Neil Trewin et al, 2010), aviação, seguros e banca (David Shirre, 2004), focam-se principalmente nos métodos analíticos para analisar e quantificar riscos (Paul R. Garvey, 2008).

Existem várias definições de risco, que dependem, essencialmente, da área de conhecimento a que se aplica. Por exemplo, em engenharia de software, (Ian Sommerville, 2010) define-se risco como:

> "Um resultado indesejável que coloca uma ameaça para a obtenção de um determinado objetivo. Um risco de processo ameaça a execução ou custo do processo, um risco de produto significa que um conjunto de requisitos de sistema não serão cumpridos".

Da mesma forma, a norma ISO Guide 73 (ISO Guide 73, 2009) define risco como:

> "…a combinação da probabilidade de um evento (ameaça[1]) e das suas consequências quando explora uma vulnerabilidade[2]".

Na perspetiva das ciências sociais, risco é visto como uma situação ou evento em que o valor humano está em perigo e o resultado é incerto, ou seja, risco é visto como uma incerteza de um evento ou atividade em relação aos valores humanos (Terje Aven and Ortwin Renn, 2009).

---

[1] Ameaça é uma circunstância ou evento com o potencial de afetar negativamente um recurso, através de acesso não autorizado, divulgação de informação privilegiada, destruição e modificação de dados (ISO Guide 73, 2009).

[2] Vulnerabilidade é a existência de uma debilidade, ou erro de desenho ou de implementação que pode levar a um evento inesperado e indesejado, comprometendo a segurança de um sistema, rede, aplicação ou protocolo (ISO Guide 73, 2009).

Apesar de várias comunidades usarem diferentes definições e terminologia para gestão de risco, podemos assumir que partilham os mesmos conceitos básicos. A figura 1 apresenta um mapa conceptual com os conceitos usados neste artigo.

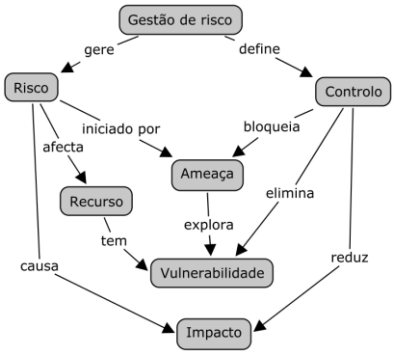

Figura 1- Conceitos de gestão de risco

O objetivo da gestão de risco consiste em definir um conjunto adequado de controlos para bloquear ameaças, eliminar vulnerabilidades ou reduzir o impacto da ocorrência de um risco, assumindo que um risco ocorre quando uma ameaça consegue explorar uma vulnerabilidade associada a um recurso com valor. O tipo de recurso a proteger depende da natureza da organização e dos objetivos de negócio, mas pode incluir, entre outros, entidades físicas (pessoas, edifícios), entidades informacionais e processos. Quando uma vulnerabilidade é explorada, é introduzido um impacto na obtenção de objetivos da organização, reduzindo-lhe o valor.

A base de conhecimento associada à gestão de risco tem vindo a ganhar especial atenção, estando relacionada com várias áreas de investigação e incluindo aspetos de julgamento empírico, normativo e quantitativo no processo de decisão.

Analisar e modelar riscos é uma das tarefas mais críticas em todo o processo de gestão de risco. Por exemplo, métodos tradicionais como *Fault Tree Analysis, Event Tree Analysis* (M. Stamatelatos, 2002) ou *Failure Mode Effect And Criticality Analysis* (MIL-STD1692A, 1980) são usados na área de segurança. No entanto, estes métodos não se adequam à modelação dos riscos iminentes que as organizações atuais enfrentam a múltiplos níveis, tanto internos como externos.

A área de gestão de riscos empresariais pretende endereçar riscos ao nível organizacional. No entanto, um dos principais problemas deve-se ao facto de que as tarefas de gestão de risco são normalmente muito específicas, operando em silos (Stephanie Maziol, 2009). Este facto resulta numa vista fragmentada de riscos, usando-se modelos e linguagens de representação

diferentes (por exemplo, riscos tecnológicos e riscos de projeto representados de forma distinta).

Um exemplo com que temos lidado e que requer gestão de riscos a nível organizacional é o problema da preservação digital. A preservação digital é reconhecida como um mecanismo para manter conteúdos valiosos ao longo do tempo, assegurando que a informação digital possa ser lida e usada no futuro. Este é um problema interdisciplinar, no qual desafios tecnológicos intersetam objetivos organizacionais.

Este artigo propõe abordar a preservação digital como um cenário específico de gestão de risco no qual os níveis físico, lógico e semântico da informação digital são constantemente ameaçados, propondo uma solução integrada de gestão de risco que providencia uma visão holística de riscos. Esta solução pretende reduzir as barreiras existentes entre a área de gestão de riscos e a área de sistemas de informação, suportando assim um processo colaborativo entre diferentes processos de gestão de risco que possam ser executados de forma não integrada.

Este artigo organiza-se da seguinte forma: a secção 2 apresenta o trabalho relacionado nas áreas de governos de tecnologias de informação, gestão de risco, arquitetura empresarial e preservação digital. Em seguida, a secção 3 apresenta a abordagem proposta neste artigo, propondo uma colaboração entre as áreas de governo de tecnologias de informação, arquitetura empresarial e gestão de risco, com o objetivo de providenciar uma visão holística da informação de risco. Na secção 4, propõe-se um modelo conceptual para representação de informação de risco e na secção 5 ilustra-se uma arquitetura para gerir essa informação. Finalmente, concluímos na secção 6.

2 Trabalho relacionado

2.1 Governo de tecnologias de informação

O governo de tecnologias de informação inclui "liderança, estrutura organizacional e processos que garantam a sustentabilidade dos recursos de tecnologias de informação no suporte aos objetives e estratégias organizacionais" (IT Governance Institute, 2007).

O COBIT (IT Governance Institute, 2007) é visto como uma referência no governo de tecnologias de informação, organizando as atividades num modelo de processos que identifica os recursos que devem ser aplicados para atingir os objetivos de governo de tecnologias de informação. O COBIT propõe um modelo de processos organizado em quatro domínios:

planeamento e organização; aquisição e implementação; suporte; e monitorização e avaliação. Define também relações entre os diferentes processos através da especificação de artefactos de entrada e de saída e modela a relevância de cada processo em vários critérios de avaliação (efetividade, eficiência, confidencialidade, integridade, disponibilidade, conformidade e confiança). Finalmente, o COBIT inclui um modelo de maturidade baseado no Capability Maturity Model Integration for Development (Software Engineering Institute, 2010) e na norma ISO 15504 (ISO 15504-1, 2004), para integrar as boas práticas de modelos de maturidade, providenciando um mecanismo de melhoramento de processos, com o objetivo de auxiliar as organizações a gerir e controlar os complexos processos de manutenção e de desenvolvimento em tecnologias de informação.

2.2 Gestão de risco

Os processos genéricos de gestão de riscos preocupam-se, essencialmente, com a definição de um conjunto de princípios e fundamentos para orientar a conceção e implementação de atividades de gestão de risco em qualquer tipo de organização. Uma vez que não se focam numa área ou domínio de aplicação específicos, os processos de gestão de risco genéricos não providenciam qualquer recomendação sobre os métodos e técnicas adequadas para cada uma das atividades, nem mesmo uma base de conhecimento com riscos comuns e planos de tratamento adequados para os riscos identificados.

A norma ISO 31000 (ISO 31000, 2009) baseia-se no princípio de que a gestão de riscos é um processo que opera em diferentes níveis, conforme ilustra a figura 2. O processo caracteriza-se pela combinação de políticas e procedimentos aplicados às atividades de estabelecer o contexto, identificação, análise, avaliação, tratamento, consulta e comunicação e, monitorização e revisão dos riscos.

Em primeiro lugar, definir o contexto é crucial para identificar os objetivos estratégicos e definir critérios (internos e externos) para determinar as consequências aceitáveis para cada contexto específico. Em segundo lugar, as organizações estão continuamente expostas a diversas ameaças e vulnerabilidades que podem afetar o seu comportamento normal. A identificação de riscos reconhece a existência de riscos, a atividade de análise examina a natureza e gravidade dos riscos identificados e, finalmente, a avaliação de riscos compara a gravidade dos riscos com os critérios definidos na determinação do contexto, para decidir se os riscos são aceitáveis e para definir se é necessário definir técnicas e controlos adequados para mitigar esses riscos.

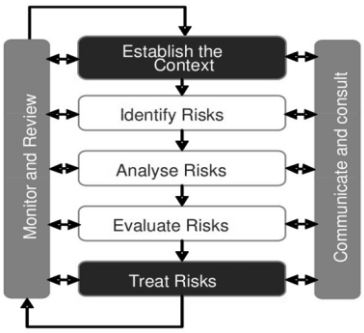

Figura 2 – Processo de gestão de risco (ISO 31000, 2009)

A identificação de ameaças, vulnerabilidades e riscos baseia-se em eventos que possam inviabilizar a realização de objetivos organizacionais (identificados na definição de contexto). Depois disso, a análise e avaliação de risco estimam a probabilidade, o impacto e a severidade dos riscos em comparação com os critérios estratégicos, a fim de ser capaz de decidir sobre as técnicas apropriadas para lidar com esses riscos (tratamento de riscos). O processo de gestão de risco requer assim uma atividade de monitorização e revisão contínua, a fim de auditar o comportamento de todo o ambiente permitindo, por exemplo, a identificação de alterações nos riscos, ou a adequação dos procedimentos de risco implementados ao seu tratamento. Finalmente, as atividades de consulta e comunicação de riscos são cruciais para se envolver e dialogar com as diferentes partes interessadas.

A norma ISO/IEC 31010 (ISO/IEC 31010, 2009) analisa 31 técnicas para realizar avaliação de risco, mostrando a sua aplicação nas etapas do processo de avaliação de risco da seguinte forma: (*i*) identificação do risco, (*ii*) análise de risco - análise das consequências, (*iii*) análise de risco - estimando probabilidades de forma qualitativa, semi-quantitativa ou quantitativa, (*iv*) análise de risco - avaliar a eficácia de controlos existentes; (*v*) análise de risco - estimando o nível (severidade) de risco, e (*vi*) avaliação de risco.

A gestão de riscos empresariais é um processo de identificação e análise de riscos, a partir de uma perspetiva integrada de toda a organização (Committee of Sponsoring Organizations of the Treadway Commission, 2004), em que considera que: "as entidades existem para fornecer valor às partes interessadas". Na verdade, todas as entidades podem enfrentar vários tipos de incerteza, levantando desafios para a gestão sobre como lidar com tal incerteza de uma forma que maximiza os valores dessas entidades para as partes interessadas

Em 2004 foi proposto o “COSO ERM Framework” (Committee of Sponsoring Organizations of the Treadway Commission, 2004) com o objetivo de criar um modelo comum para avaliar e alinhar, de forma eficaz,

todas as abordagens de gestão de risco de uma organização, definindo os componentes essenciais da gestão de riscos empresariais e discutindo os princípios e conceitos básicos com o objetivo de criar uma linguagem de riscos comum.

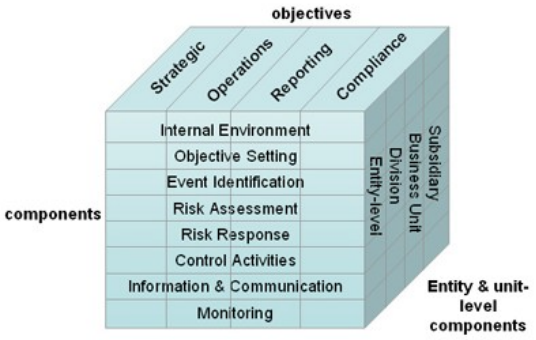

Figura 3 – COSO: gestão de riscos empresariais (Committee of Sponsoring Organizations of the Treadway Commission, 2004)

A figura 3 ilustra o "COSO ERM Framework", que se organiza em três dimensões: Objetivos, Organização (incluindo as unidades organizacionais) e componentes da gestão de risco empresarial (que definem o processo de gestão de risco). Note-se que já aqui a gestão de riscos empresariais não pode ser vista como um conjunto de processos independentes, mas sim como um disciplina iterativa e multidimensional em que existem várias dependências entre os vários componentes.

2.3 Arquitetura empresarial

As descrições de arquitetura fornecem descrições rigorosas de sistemas complexos com diferentes preocupações, sendo uma abordagem recomendada para lidar com a complexidade dinâmica e crescente desses sistemas. De acordo com a norma ISO/IEC/IEEE 42010 (ISO/IEC/IEEE 42010, 2011), arquitetura é "a organização fundamental de um sistema, incorporada nos seus componentes, relações entre si e com o meio ambiente, e os princípios que regem a sua conceção e evolução". A norma considera que um sistema tem uma missão e habita num ambiente que pode influenciá-lo. O sistema tem uma ou mais partes interessadas que têm preocupações relacionadas com o sistema e sua missão. As preocupações são "os interesses que dizem respeito ao desenvolvimento do sistema, ao seu funcionamento, ou a quaisquer outros aspetos críticos para uma ou mais partes interessadas".

Um sistema deve ter a sua arquitetura representada por descrições que ilustrem as diferentes vistas, de acordo com os pontos de vista de cada uma

das partes interessadas (incluindo aspetos funcionais e não). As descrições de arquitetura fornecem assim uma "imagem completa" do sistema e devem refletir as constantes variações impulsionadas pela evolução do ambiente que rodeia o sistema (T. Mens et al, 2010).

A arquitetura empresarial é uma abordagem holística para a definição arquiteturas de sistemas, que tem como objetivo modelar o papel da tecnologia e dos sistemas de informação na organização, providenciando um alinhamento global entre a tecnologia e sistemas de informação com os processos de negócio. Suporta o planeamento de mudança sustentável e proporciona autoconhecimento da organização, forncendo uma vista completa da organização (P. Sousa et al, 2006).

A "Zachman Framework" é uma "forma de representar a arquitetura empresarial" com a finalidade de "dar uma visão holística da organização" (J. Zachman, 1997). Também é vista como uma "teoria de classificação sobre a natureza de uma organização" representado os tipos de entidades que existem na organização. A figura 4 ilustra a organização da "Zachman Framework", que se apresenta como uma tabela onde cada célula pode estar relacionada com o conjunto de modelos, princípios, normas e serviços necessários para atender às preocupações de uma parte interessada

Perspective / Role	DATA What	FUNCTION How	NETWORK Where	PEOPLE Who	TIME When	MOTIVATION Why
Planner (Objective/Scope - Contextual)	Things important for the business	Business Processes	Business Locations	Important Organizations	Events	Business Goals and Strategies
Owner (Enterprise Model – Conceptual)	Conceptual Data / Object Model	Business Process Model	Business Logistics System	Workflow Model	Master Schedule	Business Plan
Designer (System Model –Logical)	Logical Data Model	System Architecture Model	Distributed Systems Architecture	Human Interface Architecture	Processing Structure	Business Rule Model
Builder (Technology Model – Physical)	Physical Data/Class Model	Technology Design Architecture	Technology Architecture	Presentation Architecture	Control Structure	Rule Design
Programmer (Detailed Representation – Out of Context)	Data Definition	Program	Network Architecture	Security Architecture	Timing Definition	Rule Speculation
User (Functioning Enterprise)	Usable Data	Working Definition	Usable Network	Functioning Organization	Implemented Schedule	Working Strategy

Figura 4 – Zachman framework (J. Zachman, 1997)

Cada linha representa um diferente ponto de vista da organização, enquanto as colunas expressam diferentes perspetivas sobre cada um dos pontos de vista (dados, funções, rede, pessoas, tempo e motivação). Devido à sua representação e simples visualização, a "Zachman Framework" é muito útil na análise do âmbito de modelos específicos, facilitando a conciliação de pontos de vista potencialmente contraditórios.

2.4 Preservação digital

A preservação digital pretende manter o conhecimento contido nos objetos digitais, por longos períodos de tempo, enfrentando os desafios relacionados com falhas e evolução tecnológica, garantindo a autenticidade e integridade dos objetos digitais (Maggie Jones e Neil Beagrie, 2008). A complexidade da preservação digital aumenta com o facto de que cada cenário contém diferentes tipos de objetos digitais com exigências específicas. Estes objetos digitais são ameaçados por diferentes eventos, desde erros operacionais, desastres naturais, ataques de dentro ou fora da organização, falhas de gestão, falhas de natureza económica ou organizacional, ou novos requisitos de negócios ou atualizações de natureza jurídica ou impostas pelas partes interessadas (José Barateiro et al, 2010).

Uma referência relevante na área da preservação digital é o modelo OAIS (ISO 14721, 2003), que combina um modelo de informação com um modelo de entidades funcionais. O modelo OAIS determina um contexto de alto nível para uma organização de arquivo de objetos digitais e define as principais partes interessadas. A grande vantagem desta referência foi ter estabelecido uma linguagem comum para este domínio, sendo por isso usado na conceção de sistemas de preservação.

Outra referência relevante é o modelo de metadados PREMIS, que relaciona entidades intelectuais, objetos, direitos, eventos, e agentes para fornecer um dicionário de dados para a preservação digital preservação (PREMIS Editorial Committee, 2011).

3 Proposta

Com o objetivo de suportar a estratégia global de qualquer organização, capacitando-a para associar os riscos identificados com artefactos empresariais, este artigo propõe a necessidade de um alinhamento entre processos e atividades de gestão de risco, governo de tecnologia de informação e arquitetura empresarial, para suportar cenários complexos (em que o caso da preservação digital tem sido usado para validação). Os processos de governo de tecnologias de informação pretendem assegurar o controlo na transição do planeamento estratégico para a implementação operacional. Esta tarefa exige orientação e transparência que pode ser suportada pelos processos arquitetura empresarial. De facto, a arquitetura empresarial pode ser usada para revelar deficiências, mostrando interações complexas entre as estratégias, processos de negócio, serviços e infraestrutura, fornecendo uma base de análise complexa, que pode ser usada em atividades de governo de tecnologias de informação ou em atividade de gestão de risco. Desta forma, propomos uma visão integrada de governo de

tecnologias de informação, gestão de riscos e arquitetura empresarial para apoiar as organizações na melhoria da sua eficiência, eficácia e confiança, já que a tomada de decisão deve ser capaz de fazer as coisas certas da maneira certa, com um risco controlado.

As organizações podem ser descritas através da sua arquitetura. A existência de artefactos de arquitetura empresarial (por exemplo, modelos de dados, modelos de negócio, estratégias, planos de infraestrutura, hardware, funções, estrutura organizacional, etc.) denota a consciência da organização acerca da sua arquitetura. Tal como para os edifícios, a arquitetura empresarial existe sempre, quer seja reconhecida, planeada e apoiada por modelos precisos, quer em cenários onde não é reconhecia pelas organizações.

Quando se considera a relação entre governo de tecnologias de informação e arquitetura empresarial, a arquitetura empresarial fornece informação transparente como base para a tomada de decisão e controle de atividades. No entanto, esta relação não pode ser vista de forma estática, uma vez que é fundamental atualizar a representação atual para permitir um governo de tecnologias de informação adequado que estabeleça a ponte entre o planeamento estratégico e as operações reais (alinhamento estratégico).

A relação entre governo de tecnologias de informação e gestão de risco já é reconhecida pela área de *Governance, Risk and Compliance* (GRC). De facto, a disseminação de regulamentações como *Basel* II e *Sarbanes-Oxley*, juntamente os recentes eventos económicos e financeiros, fez aumentar a consciência das organizações para estabelecer atividades de GRC (M. Frigo e R. Anderson, 2009).

O fundamento para propor uma relação entre risco e arquitetura empresarial baseia-se no facto de se verificar que as atividades de risco serem, normalmente, realizadas em silos, sem uma clara associação entre os riscos e os componentes da organização potencialmente afetados. O alargamento das atividades de risco para associar riscos com componentes da arquitetura empresarial, suporta a análise da propagação de riscos que podem afetar diretamente apenas um componente mas que potencialmente podem contaminar um conjunto maior de bens valiosos. Por outro lado, as atualizações da arquitetura empresarial são refletidas na informação de risco, o que melhora a precisão e capacidade de atualização das informações de risco.

4 Conceitos de gestão de risco

Na figura 5 propomos um modelo de domínio (em UML[3]) resultante da nossa análise do problema em causa. A gestão de riscos é um conjunto coordenado de atividades para dirigir e controlar uma organização no que diz respeito ao risco. Neste contexto, o risco é visto como o efeito, positivo ou negativo, de uma incerteza e expressa-se pela combinação da probabilidade de um evento e as suas consequências, ao explorar uma vulnerabilidade de um recurso. O recurso deve ter um valor para a organização. Não se considera por isso a existência de riscos para recursos que não tenham valor.

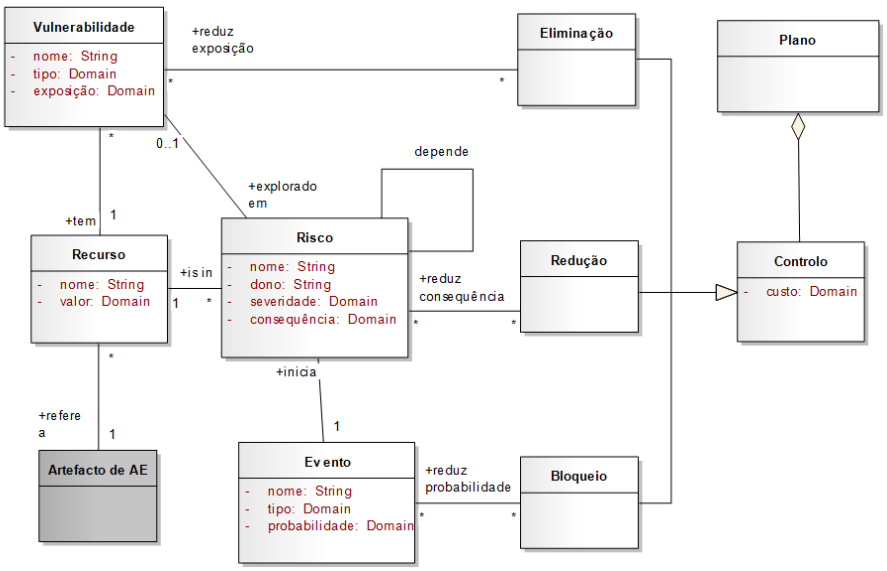

Figura 5 - Modelo de domínio para os conceitos de risco

As vulnerabilidades de um recurso têm uma exposição que quantifica a extensão à qual o recurso está sujeito a eventos devido a esta vulnerabilidade. Os recursos devem estar associados a artefactos de arquitetura empresarial (por exemplo, processos, entidades de informação, infraestrutura tecnológica). A razão para esta proposta prende-se com o facto de aproveitar a separação de interesses, bem como a representação estruturada e precisa do contexto de risco global previsto pelos modelos de arquitetura empresarial, melhorando, desta forma, a identificação de dependências e relações entre os riscos.

Dependendo do domínio de negócio, a severidade do risco (ou o nível de risco), que representa a magnitude deste risco, pode ser calculada por diferentes métodos e fórmulas de cálculo. Tipicamente, a severidade do risco

[3] http://www.uml.org/

expressa-se em função da combinação das consequências e da probabilidade do evento, mas pode também ter em conta o valor do recurso e a sua exposição relativamente a um conjunto vulnerabilidades. O plano de risco representa um conjunto de controlos aplicados para modificar os riscos, onde os controlos podem reduzir a exposição de uma vulnerabilidade, bloquear um evento, reduzir as consequências do risco, transferir/partilhar o risco com um terceiro (exemplo dos seguros), ou aceitar o risco.

5 Representação de riscos

Com o objetivo de controlar aspetos de interoperabilidade e normalização nas tarefas de gestão de riscos e suportar a colaboração de atividades relacionadas com o governo de tecnologias de informação, arquitetura empresarial e preservação digital, propomos uma linguagem de domínio para gestão de riscos, baseada em XML[4] (*Risk-DL*). Esta linguagem, especifica os conceitos definidos na secção 4 através da definição de um esquema de XML (na forma de um ficheiro .xsd[5]), que deve ser usado para validar especificações de riscos em XML.

A utilização de XML para modelar riscos pretende apoiar a interoperabilidade entre diferentes fontes de informação de risco. Além disso, XML usa uma linguagem legível que pode ser facilmente compreendida por pessoas e computadores, sendo altamente portável e independente de plataforma (é também altamente extensível, o que simplifica a evolução da linguagem, bem como a manutenção da compatibilidade entre as diferentes versões da linguagem).

A figura 6 ilustra uma arquitetura conceptual de negócio para suportar um sistema de gestão integrada de informação de risco (como diagrama de componentes, em UML[6]).

O operador é responsável por interagir com o sistema, providenciando uma descrição de risco que é transformada numa representação em *Risk-DL*, através do serviço modelador de riscos. Esta transformação é suportada pelo componente de gestão de esquemas permitindo, desta forma, suportar diferentes versões da linguagem *Risk-DL*, bem como outras representações que sejam geridas pelo componente de gestão de esquemas. Em seguida, o analisador de risco deve decifrar a especificação *Risk-DL* e gerar uma

[4] http://www.w3.org/XML
[5] http://www.w3.org/XML/Schema
[6] Perfil UML para modelos de negócio, em que um ator (Operador) lê ou edita entidades informacionais (e.g., descrição de risco), que são produzidas ou consumidas por serviços (e.g., analisador de risco) http://www.ibm.com/developerworks/rational/library/5167.html.

representação interna (conjunto de objeto *Java*), que será processada pelo gerador de planos para produzir opções de tratamento de riscos.

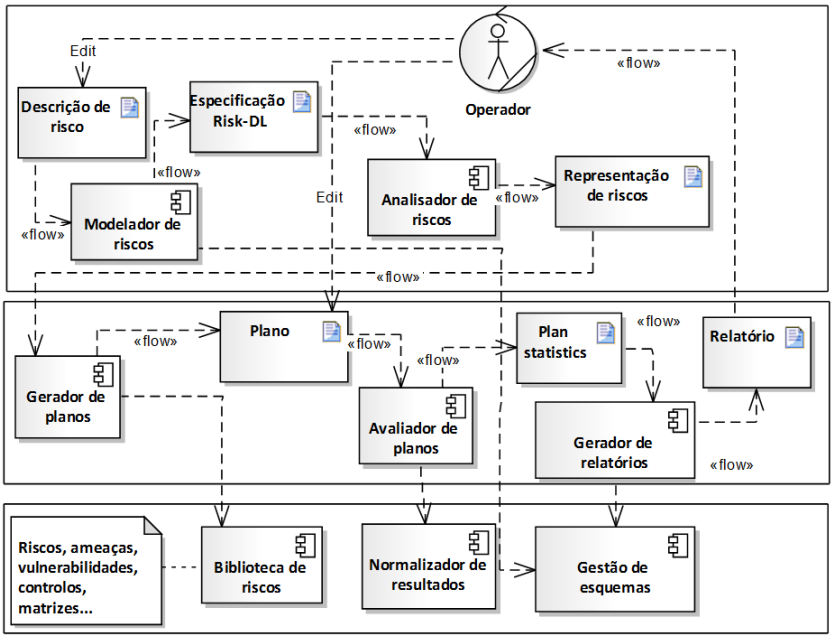

Figura 6 – Arquitetura de negócio de um sistema de gestão de risco

O gerador de planos usa o conhecimento armazenado na biblioteca de riscos para enriquecer a informação de suporte à decisão. Posteriormente, o avaliador de planos gera um conjunto de estatísticas (e.g., rácios custo/benefício) que podem ser usadas para comparar diferentes alternativas. Quando os riscos usam tipos métodos diferentes para determinar resultados (por exemplo, um resultado qualitativo e um quantitativo), o serviço normalizador de resultados transforma os diferentes valores para uma escala normalizada, permitindo comparar resultados apurados por diferentes métodos e técnicas. Finalmente, o gerador de relatórios fornece visualizações da informação de risco que pretendem suportar as necessidades das diferentes partes interessadas.

Note-se que esta solução se foca na dimensão de gestão de riscos da proposta apresentada na secção 3. A relação com arquitetura empresarial e governo de tecnologias de informação deriva do facto de que os recursos devem estar associados a artefactos da arquitetura empresarial. Por outro lado, a representação de riscos proposta suporta interoperabilidade e integração da informação de risco que pode provir de diferentes unidades organizacionais, suportando, desta forma, uma visão holística e integrada da informação de risco.

Este modelo pode ser instanciado por várias soluções tecnológicas. Como exemplo, desenvolveu-se um protótipo assente em tecnologias *Java* e soluções da comunidade *JBoss*[7], usando uma base de dados *PostGreSQL*[8] para garantir a persistência dos dados.

6 Conclusão

Os riscos são uma constante das atividades diárias de qualquer pessoa ou organização, mesmo que não sejam reconhecidos pelas partes interessadas. Um dos principais desafios na área de gestão de risco, relaciona-se com a modelação e representação da informação de risco relevante. De facto, além de outras dificuldades, a gestão de riscos envolve um conjunto heterogéneo de recursos, eventos, métodos, partes interessadas de responsabilidades, requerendo um conjunto adaptável de modelos para representar e comunicar esta informação. Por outro lado, as tarefas de gestão de risco e, em particular, as tarefas de análise de risco, tendem a ser executada em silos, por equipas diferentes com potencialmente diferentes visões sobre a mesma informação de risco. Este tipo de desafios é endereçado pelos métodos de arquitetura empresarial em que as organizações são modeladas a partir de múltiplas vistas que representam as preocupações das diferentes partes interessadas.

Para potenciar as capacidades de cada organização, recomenda-se que, nos casos em que já existam práticas de arquitetura empresarial, se usem os artefactos produzidos para auxiliar processos de gestão de risco, fornecendo, desta forma, informação detalhada e atualizada sobre vários componentes da organização. Esta ligação não deve ser feita sob a forma de extensão das práticas de arquitetura empresarial, por forma a evitar dependências em relação aos formalismos usados e, ao mesmo tempo, manter a separação de preocupações entre os dois processos. Por outro lado, para as organizações que ainda não tenham quaisquer práticas de arquitetura empresarial, o processo de gestão de risco pode ser visto como motivador e desbloqueado dessas práticas, já que, por exemplo, várias descrições e modelos de representação do contexto têm que ser detalhados neste processo. Note-se que a colaboração e integração entre arquitetura empresarial e gestão de risco, potencia a capacidade de reação à mudança (alteração ao estado atual captada pela arquitetura empresarial; perceção e análise de eventos futuros por parte da gestão de risco), tanto ao nível operacional, como estratégico e de planeamento das organizações.

[7] http://www.jboss.org
[8] http://www.postgresql.org

Este artigo propõe tirar partido das boas práticas de sistemas de informação em geral e arquitetura empresarial em particular para facilitar a troca de informação de risco e providenciar uma vista global e uniformizada da informação de riscos organizacionais. Consequentemente, os riscos podem ser associados a artefactos da arquitetura empresarial, permitindo uma análise precisa da disseminação e dependências de riscos entre os diversos componentes organizacionais. Propõe-se ainda uma solução de representação de risco, desligada dos formalismos utilizados em arquitetura empresarial, de forma a não depender de qualquer formalismo de representação de risco e de arquitetura. Propomos assim uma representação baseada em XML que suporta a comunicação entre diferentes representações de risco, bem como a comunicação com outros artefactos.

Esta abordagem foi validada no domínio da preservação digital, no âmbito do projeto nacional GRITO[9] e dos projetos internacionais SHAMAN[10] e TIMBUS[11], cofinanciados pela União Europeia.

Referências:

Barry Bohem, 1991, "Software risk management: Principles and practices", *IEEE Software*, Vol. 8(1), pp 32-41.

Committee of Sponsoring Organizations of the Treadway Commission, 2004, "Enterprise Risk Management - Integrated Framework".

David Shirre, 2004, "Dealing With Financial Risk". The Economist in association with Profile Books Ltd, 214pp.

Ian Sommerville, 2010, Software Engineering (9th Edition), Pearson Education, 792pp.

ISO 14721, 2003, "Open archival information system – Reference model", ISO, Genebra, Suiça.

ISO/IEC 15504-1, 2004, "Information technology - Process assessment - Part 1: Concepts and vocabulary", ISO, Genebra, Suiça.

ISO 31000, 2009, "Risk Management - Principles and guidelines", ISO, Genebra, Suiça.

ISO/IEC 31010, 2009. "Risk Management – Risk assessment techniques", ISO, Genebra, Suiça.

[9] http://www.fct.mctes.pt/projetos/pub/2006/Painel_Result_Especif/vglobal_projeto.asp?r_idp=81872&r_idec=938

[10] http://shaman-ip.eu

[11] http://timbusproject.net

ISO Guide 73, 2009, “Risk Management – Vocabulary”, ISO, Genebra, Suiça.

ISO/IEC/IEEE 42010, 2011, “Systems and software engineering - Architecture description”, ISO, Genebra, Suiça.

IT Governance Institute, 2007. “COBIT 4.1. Framework”.

J. Zachman, 1997, “A Framework for Information Systems Architecture”, *IBM Systems Journal*, Vol. 6(12), pp. 276-292.

José Barateiro, Gonçalo Antunes, Filipe Freitas e José Borbinha, 2010, “Designing digital preservation solutions: A risk management-based approach”, *International Journal of Digital Curation*, Vol. 5(1), pp. 4-17.

K. Lytinen, L. Mathiassen e J. Ropponen, 2000, “Attention shaping and software risk: A categorical analysis of four classical approaches”, *Information Systems Research*, Vol. 9(3), pp. 233-255.

M. Frigo e R. Anderson, 2009, “A strategic framework for governance, risk, and compliance,” *Strategic Finance*, Vol. 90(8).

M. Stamatelatos, W. Vesely, J. Dugan, J. Fragola, J. Minaric e J. Railsback, 2002, “Fault tree handbook with aerospace applications”, NASA.

Maggie Jones e Neil Beagrie, 2008, “Preservation Management of Digital Materials: A Handbook”, *Digital Preservation Coalition.*

MIL-STD1692A, 1980, “DoD: Military Standard, Procedures for Performing a Failure Mode, Effects, and Critical Analysis”. US Department of Defense.

Neil Trewin, Udechukwu Ojiako e Johnnie Johnson, 2010. “Risk management and its practical application: lessons from the british army”, Journal of Risk Research, Vol. 13(5), pp. 669-686.

Paul R. Garvey, 2008, “Analytical Methods for Risk Management: A Systems Engineering Perspective”, *Statistics: a Series of Textbooks and Monographs*, Chapman and Hall-CRC Press, 208pp.

Pedro Sousa, Artur Caetano, André Vasconcelos, Carla Pereira e José Tribolet, 2006, “Enterprise Architecture Modeling with the Unified Modeling Language”, *Enterprise Modeling and Computing with UML*, IGI Global.

PREMIS Editorial Committee, 2011. “PREMIS Data Dictionary for Preservation Metadata”, Version 2.1.

Software Engineering Institute, 2010, “Capability Mautiry Model Integration for Development”, Version 1.3, Carnegie Mellon University.

Terje Aven and Ortwin Renn, 2009. “On risk defined as an event where the outcome is uncertain”, Journal of Risk Research, Vol. 12(1), pp. 1-11.

Stephanie Maziol, 2009, “Risk management: Protect and maximize stakeholder value”, *Technical report, Oracle Governance, Risk, and Compliance, Oracle Corporation.*

T. Mens, J. Magee e B. Rumpe, 2010, “Evolving Software Architecture Descriptions of Critical Systems”, *Computer, IEEE Computer Society*, vol. 43, pp. 42-48.