Instituto Universitário de Lisboa

Departamento de Ciências e Tecnologias da Informação

Implementação de uma *Framework* para Gestão da *Compliance* nos SI/TIC - Estudo de Caso no Sector Bancário

Carlos Alberto Fernandes Macias

Dissertação submetida como requisito parcial para obtenção do grau de

Mestre em Gestão de Sistemas de Informação

Orientador:

Doutor José Cordeiro Gomes, Professor Associado,

ISCTE – Instituto Universitário de Lisboa

Co-Orientador:

Doutor Manuel José Vilares, Professor Catedrático,

Univ. Nova de Lisboa

Setembro, 2011

AGRADECIMENTOS

Em primeiro lugar quero agradecer ao Prof. Cordeiro Gomes por ter acedido ao meu pedido para orientar a minha dissertação de mestrado, bem como ao Prof. Manuel Vilares, pelo apoio prestado ao longo destes meses, pois sem eles seria impossível atingir os objectivos a que me tinha proposto.

Um agradecimento muito especial para a minha esposa Maria das Dores pelo constante incentivo e apoio, bem como no garantir da minha disponibilidade suficiente para me dedicar a este projecto.

Um agradecimento carinhoso aos meus filhos Marco, Anabela, Vítor pelo apoio e compreensão pela minha indisponibilidade.

Um agradecimento aos meus pais, Maria do Céu e Eduardo pelo incentivo que me deram ao longo deste projecto.

Agradeço ao Hélder Gonçalves pelo apoio e no empenho e profissionalismo demonstrado na implementação do estudo de caso.

Agradeço aos meus colegas de trabalho pela adesão e empenho na implementação do estudo de caso.

Finalmente agradeço aos professores do Mestrado em Gestão de Sistemas de Informação e aos colegas pelo apoio e incentivo.

RESUMO

Este trabalho propõe uma *Framework* para a Gestão da *Compliance* nos SI/TIC (Sistemas de Informação / Tecnologias de Informação e Comunicação), tendo sido verificada a sua aplicabilidade numa Entidade Gestora dos SI/TIC do BANCO que presta serviços a um dos maiores grupos do Sector Financeiro Português. A *Compliance* relaciona-se com a aderência das Organizações às exigências impostas pelos reguladores da sua actividade. As Organizações ao não atenderem a estas exigências incorrem no denominado Risco de *Compliance*.

O desenvolvimento da *framework* resultou da sistematização das orientações e boas práticas identificadas e estudadas dos vários modelos propostos por vários autores e pelo ISACA, para a gestão da *Compliance*. O estudo de caso foi realizado em três fases: (i) Auditoria à Situação Inicial; (ii) Implementação da *Framework* para a Gestão da *Compliance* dos SI/TIC; (iii) Auditoria da Situação Pós Implementação. Através deste estudo de caso foi possível analisar a adequação da *framework,* para assegurar uma das exigências impostas pelo Banco de Portugal à Entidade Gestora dos SI/TIC do BANCO.

Apesar de, durante o estudo de caso, não ter sido possível a recolha de indicadores para a medição da eficiência e eficácia da utilização da *framework*, foi entendimento dos vários colaboradores, nomeadamente pela administração da Entidade Gestora dos SI/TIC do BANCO, que a sua utilização permite uma melhoria para já qualitativa através da sistematização e normalização das várias actividades associadas à Gestão da *Compliance* nos SI/TIC.

Palavras-chave: *Compliance*, Gestão, Sistemas de Informação, *Framework*

Classificação ACM: K.6 Management of Computing and Information Systems

ABSTRACT

This master thesis proposes a Framework for the IS/ICT *Compliance* Management, having been checked their applicability in the SI/TIC Bank Entity Management that provides services to one of the largest groups in the Portuguese financial sector. The *Compliance* is related to adherence of the organizations to the requirements imposed by regulators of their activity. Failing to meet these requirements, Organizations will incur the so-called *Compliance* Risk.

The framework has been developed from the systematization of orientations and good practices of the IS/ICT *Compliance* Management identified and studied from the various models proposed by multiple authors and by ISACA. The case study was conducted in three phases: (i) the Initial Situation Audit, (ii) the Implementation of Framework for the IS/ICT *Compliance* Management, (iii) Post-Implementation Audit Status.

Through this case study we could analyze the adequacy of the framework to ensure the requirements imposed by Bank of Portugal to the SI/TIC Bank Entity Management. Although during the case study, has not been possible the capture of indicators for the efficiency measuring and effectiveness of framework used, was understood by multiple collaborators, including top management of the SI/TIC Bank Entity Management that its use allows a qualitative improvement through the systematization and standardization of the various activities associated with the IS/ICT *Compliance* Management.

Keywords: *Compliance*, Management, Information System, *Framework*

Classificação ACM**:** K.6 Management of Computing and Information Systems

ÍNDICE

ÍNDICE DE FIGURAS

ÍNDICE DE TABELAS

1 Introdução

1.1 Enquadramento

O progresso tecnológico, a globalização das economias, a forte competitividade e a concorrência no mercado, constituem factores de mudança e desenvolvimento económico e social, trazendo consigo novos serviços financeiros e novas formas de relacionamento entre os diversos agentes económicos. No entanto, nem todas as mudanças ou os seus efeitos são positivas. Sucessivos escândalos financeiros têm imposto aos governos e parlamentos nacionais a necessidade de reforçar as medidas regulatórias, que pretendem dissuadir ou pelo menos minimizar os efeitos negativos sobre a economia e sobre a confiança dos cidadãos nos Sistemas Financeiros[1] e na acção dos reguladores, decorrentes de eventuais crises sistémicas devido ao não controlo dos riscos. Devido à complexidade e risco da sua própria actividade - a financeira, o Sector Bancário é um dos sectores económicos mais regulados. A regulação do Sector Bancário[2] em Portugal está estreitamente ligada à actividade regulatória dos outros países da comunidade europeia e enquadrada pela regulamentação comunitária, sendo que um número crescente de questões é tratado e decidido a nível comunitário. Na União Europeia (UE) existem três tipos básicos de legislação[3]: Regulamentos[4], Directivas[5] e Decisões[6].

No caso de Portugal os regulamentos são criados pelas entidades reguladoras, supervisionadas pelos respectivos governos. São exemplos dessas entidades o Banco de Portugal (BdP)[7] que tem como responsabilidade velar pela estabilidade do sistema financeiro nacional, e a CMVM (Comissão do Mercado de Valores Mobiliários) tem como missão supervisionar e regular os mercados de valores mobiliários e instrumentos financeiros derivados, bem como as actividades de todos os agentes que neles operam. A supervisão realizada por estas entidades é decomposta em prudencial[8] e

[1] Para maior detalhe sobre o Sistema Financeiro consultar o Anexo – Caracterização e Funções do Sistema Financeiro.
[2] A actividade deste sector centra-se em receber depósitos e outros fundos reembolsáveis do público para os aplicarem na concessão de crédito. Para maior detalhe consultar o Anexo –Caracterização e Funções do Sistema Financeiro.
[3] "EUROPA > European Commission > Legislation", consultado em 2010-10-16, em http://ec.europa.eu/legislation/index_en.htm
[4] Os regulamentos são actos jurídicos não precisam de ser incorporados nas leis nacionais, para se tornarem efectivos.
[5] As directivas em geral têm uma maior área de aplicação, são mais poderosas que as decisões e regulamentos da UE e são o instrumento mais utilizado ao nível legal, e para terem efeito precisam de ser incorporados nas leis nacionais, para se tornarem efectivas. Uma vez transpostas para o direito nacional, servem para harmonizar os sistemas jurídicos nacionais dos Estados-Membros da UE.
[6] As decisões são actos administrativos em geral, que são destinadas a indivíduos específicos, empresas ou governos e, como tal, tem impacto limitado.
[7] Para maior detalhe sobre as competências do BdP consultar o Anexo – Caracterização e Funções do Sistema Financeiro.
[8] A supervisão prudencial refere-se a normas com regras de prevenção e de salvaguarda caracterizadas estas pela introdução de critérios de prudência quanto à segurança e solidez na gestão dos bancos.

comportamental[9]. Como referimos anteriormente, o risco é um dos factores inerentes à Actividade Bancária[10], principalmente em momentos de incerteza e suspeições, pois esta encontra-se mais exposta a falhas e incorrecções processuais podendo acarretar prejuízos.

A disponibilização dos SI/TIC ao Negócio desempenha um papel chave para suportar as actividades bancárias, sendo necessário assegurar as exigências dos reguladores. O não assegurar dessas exigências podem resultar em perdas decorrentes da falha ou da não adequação dos meios - processos internos, pessoas, sistemas da Organização e ainda dos eventos externos a que esta está exposta. Neste contexto as Organizações precisam de encontrar modelos que garantam uma gestão efectiva quanto aos seus riscos.

1.2 Estrutura da Dissertação

Este documento encontra-se estruturado em seis capítulos que materializam todo o trabalho desenvolvido e realizado.
O primeiro capítulo apresenta o enquadramento e a estrutura da dissertação.

O segundo capítulo apresenta, de forma sucinta, a conformidade no Sector Bancário e as orientações e boas práticas apresentadas por vários autores e pelo ISACA (Information Systems Audit and Control Association), para o tratamento dos Requisitos de Conformidade para a *Compliance* dos SI/TIC bem como o seu contexto nos SI/TIC.

O terceiro capítulo apresenta a metodologia adoptada para este trabalho.

O quarto capítulo apresenta a *framework* desenvolvida para a Gestão da *Compliance* dos SI/TIC.

O quinto capítulo apresenta o estudo de caso realizado numa Entidade Prestadora dos Serviços de SI/TIC para o Sector Bancário Português, para validação da Framework para a Gestão da *Compliance* dos SI/TIC.

No sexto capítulo apresentam-se as conclusões e trabalhos futuros.

[9] A supervisão comportamental refere-se a normas que focam a conduta do mercado, localizam as assimetrias de informação e outros aspectos relacionados com as actividades bancárias, como os deveres de informação quanto ao conteúdo e clareza dos contratos associados aos produtos e serviços financeiros (e.g. Aviso n.º 8/2009 e a Instrução n.º 21/2009), e pela adopção de códigos de conduta pelos bancos.
[10] Para maior detalhe sobre a Actividade Bancária consultar o Anexo – Caracterização e Funções do Sistema Financeiro.

2 Enquadramento da *Compliance*

Neste capítulo é abordada de forma sucinta a *Compliance* no Sector Bancário, as várias abordagens no tratamento dos Requisitos de Conformidade, as orientações e boas práticas para a *Compliance* dos SI/TIC.

2.1 A Conformidade no Sector Bancário

2.1.1 Requisitos de Conformidade

A Conformidade[11] das exigências impostas ao Sector Bancário que é um dos componentes do Sistema Financeiro poderá apresentar-se de três formas distintas embora relacionadas (BACE e ROZWELL, 2006, pp.4-5):

- A Conformidade Regulamentar preocupa-se em compreender e cumprir com a legislação, regulamentação, normas e acordos contratuais a que uma Organização do Sistema Financeiro está sujeita, sendo imposta pelos reguladores e legisladores;
- A Conformidade do Negócio está relacionada com os princípios de ética propostos a uma Organização do Sistema Financeiro pelos seus parceiros comerciais, clientes e organizações internacionais e intergovernamentais, promovendo a responsabilidade social e ecológica, através da implementação de orientações e boas práticas nos seus processos;
- A Conformidade Organizacional resulta da necessidade de preservar o património bem como da responsabilidade social corporativa que se traduz na indicação de objectivos e directrizes para a produção de políticas[12], normas[13] e procedimentos internos de uma Organização do Sistema Financeiro.

No âmbito desta dissertação são considerados como Requisitos de Conformidade as "*leis, regulamentos, contratos, códigos de conduta, práticas instituídas ou princípios éticos*" como definido pelo Banco de Portugal no Modelo de Avaliação do Risco (MAR) (BANCO DE PORTUGAL, 2007, p.17).

Os Requisitos de Conformidade impostos à Actividade Bancária[14] pretendem manter o regular funcionamento das Organizações, tendo-se tornado uma fonte de preocupação para a Gestão. A questão crítica para a Gestão é a Organização incorrer em sanções de carácter civil, penal e de

[11] A palavra Conformidade é a condição para algo estar conforme (do lat., com - "junto" + *formare* "formar", "dar forma" = com a mesma forma) pretendido ou previamente estabelecido.

[12] Dado que os SI/TIC são vitais para a operacionalidade de muitas organizações, deverão existir Políticas escritas relativas a todo o âmbito dos SI/TIC, devidamente aprovadas pela Gestão e divulgadas por toda a Organização.

[13] As normas servem para suportar os requisitos das Políticas e definem formas de operar na organização, compatíveis com os objectivos desta. Permitem à organização manter a totalidade do ambiente operacional dos SI/TIC de forma mais eficiente.

[14] Para maior detalhe sobre a Actividade Bancária consultar o Anexo – Caracterização e Funções do Sistema Financeiro.

reputação, financeiro ou de mercado, em resultado de não ter cumprido com os Requisitos de Conformidade (TARANTINO, 2008, pp.21-22).

2.1.2 Risco e Controlo da *Compliance*

A *Compliance*[15] no contexto desta dissertação refere-se ao estado do cumprimento das exigências dos Requisitos de Conformidade (Secção 2.1.1) impostos às actividades de uma Organização.

O não atendimento aos Requisitos de Conformidade pela Organização faz com que uma Organização fique sujeita ao Risco de *Compliance*, principal risco a considerar nesta dissertação. Genericamente, o risco é inerente à própria actividade das Organizações, independentemente do sector, e a única forma de o evitar totalmente seria estas deixarem de exercer a sua própria actividade (TARANTINO, 2008, p.15). O risco pode ser considerado como qualquer evento que possa afectar a capacidade de uma Organização alcançar os seus objectivos.

A caracterização do Risco de *Compliance,* que é parte integrante da categoria de Riscos Não Financeiros, encontra-se redigida no MAR[16], como sendo a "*Probabilidade de ocorrência de impactos negativos nos resultados ou no capital, decorrentes de violações ou desconformidades relativamente às leis, regulamentos, contratos, códigos de conduta, práticas instituídas ou princípios éticos. Pode traduzir-se em sanções de carácter legal ou regulamentar, na limitação das oportunidades de negócio, na redução do potencial de expansão ou na impossibilidade de exigir o cumprimento de obrigações contratuais*" (BANCO DE PORTUGAL, 2007, pp.17-18). No contexto do MAR e como abordado por Cascarino (CASCARINO, 2007, p.37), as Organizações ao não assegurarem as exigências dos Requisitos de Conformidade, além de incorrerem no Risco de *Compliance*, podem incorrer noutros riscos, como: (i) perda de clientes, reputação e confiança das partes interessadas; (ii) perda de foco nas metas e objectivos da Organização; (iii) penalizações significativas a nível pessoal e organizacional; (iv) acesso limitado aos mercados de capitais; (v) limitação de realizar a sua actividade em jurisdições específicas; (vi) aumento da fiscalização por parte dos reguladores.

O Banco de Portugal, na sua Instrução nº 20/2005 (BANCO DE PORTUGAL, 2005, p.2) relativamente ao risco, onde se inclui o Risco de *Compliance*, indica que as instituições deverão mostrar a sua aderência às recomendações do Comité de Supervisão Bancária de Basileia. Estas recomendações estão relacionadas com a difusão das boas práticas no Sector Bancário, potenciando o desenvolvimento de um conjunto de incentivos que premeia a capacidade do sector em medir e gerir o risco, provocando, inevitavelmente, adaptações nas estruturas organizativas, processos internos e na própria cultura das Organizações. Neste contexto Cascarino (CASCARINO, 2007, p.33) refere que

[15] A palavra *Compliance* vem do verbo em inglês "*to comply*", que significa "cumprir", "executar", "satisfazer", "realizar o que foi imposto".

[16] A caracterização do risco é parte integrante da taxonomia uniformizadora para a classificação dos riscos da Organização, proposta na matriz de riscos anexa ao Decreto-Lei n.º 104/2007[16], de 3 de Abril, na qual são indicadas nove categorias de risco divididas em dois grupos: Riscos Financeiros e Riscos Não Financeiros onde se inclui o Risco de *Compliance*. A definição da taxinomia de risco está consistente com as "*Guidelines on the Application of the Supervisory Review Process under Pillar 2*" publicada pelo CEBS (Committee of European Banking Supervisors) em 2006.

o controlo, ou seja, a mitigação do risco, engloba todos os elementos de uma Organização (incluindo os seus recursos, sistemas, processos, cultura, estrutura e actividades) suportados por todos os seus colaboradores, para que sejam alcançados os objectivos da Organização. O controlo pode ser considerado como um conjunto de procedimentos e métodos, executados de forma manual ou automática, cuja finalidade é vigiar as funções e atitudes das organizações, permitindo verificar se as operações são realizadas conforme os programas adaptados e as directrizes e princípios estabelecidos. A primeira finalidade do controlo é o de prevenir quanto ao Risco de *Compliance* e posteriormente o de vigiar a efectividade da *Compliance* dos SI/TIC.

O Risco de *Compliance* pode decorrer da inexistência de Controlos de *Compliance* na detecção ou prevenção de processos ou mecanismos inadequados ou da ineficiência dos controlos instituídos pela Organização. Cascarino (CASCARINO, 2007, pp.61-62) indica que os controlos podem ter objectivos de prevenção (*controlo preventivo)*, detecção (*controlo detectivo*), correcção (*controlo correctivo*), orientação (*controlo orientador*) e de compensação (*controlo compensatório*)[17]. Esta classificação facilita distinguir se um determinado controlo actua sobre a probabilidade da ocorrência de um evento de risco ou sobre a severidade do mesmo. Os controlos aplicáveis à *Compliance* pretendem ajudar a eliminar ou mitigar o Risco de *Compliance*, embora per si não constituam uma garantia absoluta na mitigação total do risco.
O COSO (COSO, 2007, p.3) [18] indica quatro tipos de estratégia para a mitigação do risco na qual se inclui o Risco de *Compliance*: Evitar, Transferir, Aceitar e Tratar. A escolha da estratégia dependerá dos critérios estabelecidos pela Organização para a implementação dos controlos necessários para mitigar os riscos, devendo estes critérios estar alinhados com a missão e a estratégia da Organização e serem consistentes com a sua apetência ao risco.

As Organizações com o objectivo de garantirem a efectividade da mitigação do Risco de *Compliance* devem implementar um Sistema de Controlo Interno. Cascarino (CASCARINO, 2007, pp.59-61) indica que os objectivos do Controlo Interno numa Organização podem passar pela: (1) confiabilidade e integridade da informação; (2) o cumprimento das políticas, planos, procedimentos e Requisitos de Conformidade; (3) a salvaguarda dos seus activos; (4) a eficácia e eficiência das suas operações. O ISACA através COBIT 4.1 (Control Objectives for Information and Related Technology) (ITGI, 2007,

[17] Um Controlo Preventivo tende a agir sobre a probabilidade de ocorrência de um determinado evento, impedindo nunca a 100% que este aconteça. Um Controlo Detectivo pretende mitigar a severidade de um evento já ocorrido e podem envolver menos custos do que os *controlos preventivos*. Um Controlo Correctivo pretende assegurar a correcção de anomalias identificadas. Um Controlo Orientador pretende assegurar que as directrizes da Gestão são executadas na Organização, o COBIT 4.1 (ITGI, 2007, p.15) define-o como Controlo de Entidade. Um Controlo Compensatório tende a existir para colmatar uma fraqueza num determinado controlo, podendo este ser compensado por outro Controlo ou através de outros elementos como, a título de exemplo, apólice de seguro, cláusulas contratuais com direito a indemnização (CASCARINO, 2007, pp.61-62).

[18] A estratégia de Evitar ou Eliminar o risco encontra-se subjacente à não execução das actividades que possam ter risco. A estratégia de Transferir o risco significa partilhar os riscos com parceiros através de contractos específicos ou contratar seguro apropriado a troco de uma retribuição. A estratégia de Aceitar o risco é assumir as eventuais perdas que sejam consequência de um risco, devendo esta opção ser criteriosamente documentada. A estratégia de Mitigar o risco envolve a implementação de Controlos de *Compliance*, estando a sua eficácia dependente de os riscos estarem identificados, avaliados e controlados.

p.191)[19] define Controlo Interno como as políticas, os procedimentos, as práticas e as estruturas organizacionais concebidos para dar uma garantia razoável de que os objectivos de Negócio serão atingidos e de que serão prevenidos ou detectados e corrigidos quaisquer acontecimentos indesejados. Neste contexto poderemos caracterizar o Controlo Interno como uma forma de gerir um risco, que garanta a obtenção dos objectivos de Negócio, sendo um sistema posto em prática para regular, orientar e monitorizar os riscos.

A Instrução nº 20/2005 do Banco de Portugal (BANCO DE PORTUGAL, 2005, p.1), sobre Controlo Interno, refere: "A crescente complexidade das actividades conduzidas pelas instituições de crédito e sociedades financeiras, bem como a dinamização da actividade internacional de algumas e as consequentes alterações ao nível da estrutura dos grupos bancários, exigem o reforço dos sistemas e procedimentos de controlo interno". No caso português o Banco de Portugal, como supervisor do Sector Bancário, adoptou o "Internal Control – Integrated Framework" do COSO (Commitee of Sponsoring Organizations of the Treadway Comission) (COSO, 1994), que foi escolhido pela Comissão Europeia, como modelo de avaliação dos Sistemas de Controlo Interno no Sector Bancário. Tendo como base o COSO (COSO, 1994), o Banco de Portugal indica que as Organizações deste sector devem promover "uma sistematização dos princípios básicos que devem nortear a implementação de um sistema de controlo interno, seguindo os conceitos, reconhecidos e aceites a nível internacional, definidos no "Internal Control - Integrated Framework" publicado pelo Committee of Sponsoring Organizations of the Treadway Commission (COSO) " (BANCO DE PORTUGAL, 2008, p.1).

É neste contexto que os Controlos de *Compliance* devem ser monitorizados, podendo esta monitorização assumir várias formas, incluindo auto-avaliação, o uso de auditorias regulares, e a introdução de programas de melhoria contínua. Controlos devem ser revistos frequentemente de modo a aferir a sua relevância e eficácia, devendo estes ser alterados ou adaptados quando necessário (CASCARINO, 2007, p.27). O Banco de Portugal como regulador indica que deve haver uma auditoria interna adequada à complexidade das actividades conduzidas pela entidade, capaz de proceder, de forma eficaz, à revisão independente dos sistemas e procedimentos implementados de controlo (BANCO DE PORTUGAL, 2005, p.1). Os auditores internos devem constituir uma função de avaliação independente, embora pertençam à própria Organização, pois desempenham um papel importante ao avaliar a eficácia dos sistemas de controlo. Como complemento poderão existir auditorias externas que terão uma maior objectividade relativamente à auditoria interna, resultante do maior distanciamento entre auditores e auditados.

2.1.3 Função *Compliance*

O BIS (Bank for International Settlements) (BIS, 2005) refere que as Organizações do Sector Bancário devam criar a Função *Compliance*, para a gestão das matérias relacionadas com *Compliance* propondo mesmo um princípio (*Principle 7: Compliance function responsibilities*) que define as responsabilidades específicas associadas a esta função. Esta função tem como

[19] Para maior detalhe sobre o COBIT 4.1 consultar o Anexo – COBIT 4.1.

responsabilidade o de proactivamente identificar e avaliar a aderência aos Requisitos de Conformidade, controlar os Riscos de *Compliance* afectos à actividade bancária, aconselhar e informar a gestão sobre esses riscos (BIS, 2005, p.7).

O Banco de Portugal (BANCO DE PORTUGAL, 2010, p.12) e o BIS (BIS, 2005) referem-se à Função *Compliance* e não a uma estrutura fixa como uma área ou departamento, devendo esta função estar descentralizada. Neste contexto poderá ser criada a Função *Compliance* dos SI/TIC, em concertação com a Função *Compliance* da Organização do Sector Bancário, para o tratamento das matérias de *Compliance* aplicáveis aos SI/TIC. O que se pretende com a Função *Compliance* dos SI/TIC é que desenvolva actividades em matérias de *Compliance* para mitigar os Riscos de *Compliance* (Secção 2.1.2) nos SI/TIC. O objectivo desta função deverá ser a identificação, a análise, a avaliação, o aconselhamento, no que se refere às exigências dos Requisitos de Conformidade (Secção 2.1.1) e da monitorização e comunicação às partes interessadas da efectividade dos Controlos de *Compliance* e estado do tratamento em matérias de *Compliance* nos SI/TIC.

2.2 As várias abordagens no tratamento dos Requisitos de Conformidade

Os SI/TIC suportam a execução das actividades bancárias (Secção 2.1.1) sendo fundamentais para assegurar a *Compliance* da Organização (Secção 2.1.2), sendo necessário proactivamente assegurar as exigências dos Requisitos de Conformidade nesses serviços. O tratamento dos Requisitos de Conformidade nos SI/TIC, na generalidade é reactivo porque é o resultado de uma reacção instintiva a um problema conhecido que precisa de ser resolvido (COX, 2008, p.553). Por outro lado Tarantino (TARANTINO, 2008, p. 13) refere mesmo que a história tem demonstrado que as melhorias na Gestão da *Compliance* normalmente vêm como consequência de escândalos financeiros, tendo resultado em mais Requisitos de Conformidade. A consequência é que as Organizações terão de assegurar as suas exigências. No estudo "*Regulatory compliance is top concern in 2011*" do ISACA (ISACA, 2011, p.10) com base num inquérito realizado a mais de 2.400 membros desta entidade distribuídos por 126 países, constatou-se que para os próximos 12 a 18 meses a principal questão que poderão afectar os SI/TIC, é a *Compliance*. Uma das questões evidenciadas no estudo é que as Organizações são confrontadas com a necessidade de gerirem um crescimento numa economia cada vez mais global e por outro lado assegurar as exigências dos Requisitos de Conformidade. Os novos ou a alteração aos requisitos existentes tem um impacto nos SI/TIC, que precisa de ser gerido. Este contexto sugere mesmo a criação de processos proactivos para o tratamento de tais requisitos.

Ross (ROSS, 2007, p.1) refere que embora a adesão aos Requisitos de Conformidade (Secção 2.1.1) nunca seja total, é necessário uma vigilância sobre a variabilidade destes requisitos bem como sobre as actividades e responsabilidades dos SI/TIC em matérias de *Compliance*. Enquadrado com este argumento para a Gestão da *Compliance* nos SI/TIC (Secção 2.1.3), podemos aplicar três princípios essenciais para a governação de uma Organização: conhecer o estado presente, saber para onde ir e saber como se está a progredir. Aplicando estes princípios à Gestão da *Compliance* nos SI/TIC, a

Função *Compliance* dos SI/TIC (Secção 2.1.3), pode de forma continuada: identificar as necessidades de *Compliance* para se "conhecer o estado presente"; determinar o que será necessário assegurar quanto às exigências dos Requisitos de Conformidade, de modo a "saber para onde ir"; e comunicar o estado da *Compliance* através da informação proveniente dos relatórios de auditoria e monitorização para se saber "como se está a progredir" quanto à efectividade da *Compliance* dos SI/TIC (Secção 2.1.3). Neste contexto os seguintes autores, Ho (HO, 2009), Dameri (DAMERI, 2009) e Annawamy (ANNASWAMY, 2009), referem que para terem uma atitude proactiva as Organizações precisam de estabelecer processos para a gestão do tratamento dos Requisitos de Conformidade nos SI/TIC, no qual os Riscos de *Compliance* devem ser geridos e endereçados**.**

A nível académico só foi possível, até ao momento, identificar um trabalho relacionado com a *Compliance:* "*IT System Regulatory Compliance*" de Hansson (HANSSON, 2008), do Royal Institute of Technology, Stockholm, Sweden, de Junho de 2008. Este autor refere que os SI/TIC da Vattenfall (empresa do sector energético Sueco) estão sujeitos a múltiplos requisitos de conformidade, devido à sua presença em vários países da União Europeia (EU). Esta tese de dissertação fornece uma visão geral dos principais Requisitos de Conformidade, em diversas áreas suportadas pelos SI/TIC. O autor da dissertação concluiu que tais requisitos são bastante semelhantes entre si devido à tradição jurídica semelhante nos países onde está presente e parcialmente pelos esforços da EU, no sentido de harmonizar os sistemas jurídicos. Outra conclusão é a de que os Requisitos de Conformidade não endereçam de uma forma concreta o que é necessário fazer nos SI/TIC.
Os Requisitos de Conformidade impõem Requisitos Aplicacionais[20] que são necessários implementar nos SI/TIC para assegurar as exigências dos Requisitos de Conformidade, como referido por Breaux e Antón (BREAUX e ANTÓN, 2007, p.1). Segundo estes autores a captura dos Requisitos Aplicacionais é complexa porque os Requisitos de Conformidade contêm ambiguidades intencionais e não intencionais e porque a sua rastreabilidade ao longo do texto bem como as referências cruzadas dificultam a sua identificação. Neste contexto propuseram uma metodologia denominada "*Frame-Based Requirements Analysis Method (FBRAM)*" para uma captura sistemática dos Requisitos Aplicacionais dentro dos Requisitos de Conformidade. Este modelo não foi explorado nesta dissertação por se focar em aspectos relacionados com os possíveis conflitos de exigências nos próprios Requisitos de Conformidade.

Após uma consulta a entidades similares do sector bancário Português não foi possível identificar a existência de modelos para a Gestão da *Compliance* nos SI/TIC. No entanto Sants (SANTS, 2007, p.3), num estudo sobre as boas práticas na Gestão dos Riscos de *Compliance* nos maiores bancos de investimentos do Reino Unido, observou as seguintes boas práticas realizadas por esses bancos: (S1) uma definição do risco de *Compliance* que seja acessível a todos os funcionários e articulada de modo que estes a possam entender; (S2) uma mensagem clara dentro da Organização que o risco de

[20] Requisitos Aplicacionais são as condições ou capacidades que as Aplicações precisam de possuir para responder às necessidades ou restrições da actividade bancária. Os requisitos incluem a quantificação e documentação das necessidades, desejos e expectativas do seu patrocinador, dos utilizadores e das partes interessadas (PMI, 2004) Project Management Institute; "A Guide to the Project Management Body of Knowledge- Fourthe Edition"; publicado em 2008 pelo PMI.

Compliance é da responsabilidade de todos os funcionários sendo que estes devem aderir à cultura de *Compliance* da Organização; (S3) o envolvimento de outras funções da Organização (e.g. Controlo Interno, Processos de Trabalho) que em conjunto com a Função *Compliance* (Secção 2.1.3) auxiliem a gerir os riscos de *Compliance*; (S4) a avaliação da *Compliance* e que esta faça parte do relatório de outras funções-chave de controlo da Organização.

2.2.1 Uma perspectiva holística na gestão da *Compliance*

Ho (HO, 2009, p.3) recomenda que o tratamento dos Requisitos de Conformidade (Secção 2.1.1) deve ser feito de modo integrado no que se refere aos "silos funcionais"[21], para que cada silo funcional não tenha diferentes formas de assegurar as exigências dos Requisitos de Conformidade. Recomenda mesmo que deve existir um envolvimento precoce e comunicação contínua entre as partes interessadas a fim de evitar uma abordagem baseada em silos. A normalização deve ser um objectivo de forma a mitigar o aumento dos encargos sobre o Negócio, e reforçar a confiança das partes interessadas em matérias de *Compliance* (Secção 2.1.3). A formação contínua nestas matérias deve ser utilizada por forma a alertar as pessoas, quer internas quer externas (e.g. Fornecedores de Serviços Externos de SI/TIC), para os riscos, custos e impactos do não atendimento às exigências dos requisitos. A tomada de decisões em matérias de *Compliance* deve estar dentro dos critérios de apetência ao risco estabelecidos pela Organização (Secção 2.1.2).

Ho (HO, 2009, pp.1-2) recomenda a utilização COSO-ERM[22] COSO, 2007), do COBIT 4.1 (ITGI, 2007), dos dez princípios dos SI/TIC do Comité de Basileia II[23] (BIS, 2002), e a norma ISO/IEC 27001 (Requisitos do Sistemas de Gestão de Segurança da Informação) (ISO/IEC 27001, 2005). Esta autora refere o COSO-ERM (COSO, 2007) como referência para o Controlo Interno e o COBIT 4.1 (ITGI, 2007) para a governação dos SI/TIC. A norma ISO/IEC 27001 (ISO/IEC 27001, 2005) pertence à família da ISO/IEC 27000[24]. Segundo a autora, estes referenciais facilitam a adopção de uma abordagem holística para a gestão do tratamento dos Requisitos de Conformidade nos SI/TIC, no qual os Riscos de *Compliance* têm de ser geridos e tratados. Para tal Ho (HO, 2009, pp.2-6) propõe os seguintes processos: (H1) A identificação dos Requisitos de Conformidade; (H2) A interpretação e

[21] Os silos funcionais referem-se à segmentação em unidades autónomas das funções de negócio (HO, 2009).

[22] Para maior detalhe sobre o COSO-ERM consultar o Anexo - COSO.

[23] Uma das recomendações do Comité de Basileia expressa em "*Sound Practices for the Management and Supervision of Operational Risk*" (BIS, 2002), define dez princípios para os SI/TIC divididos em quatro práticas: (1) Desenvolvimento de um ambiente apropriado para a gestão do risco[23] – relacionado com a sensibilização para o Risco Operacional,com os requisitos de auditoria interna, com a gestão de políticas, processos e procedimentos. (2) Identificação, avaliação, monitorização e controlo e/ou mitigação do risco – relacionado com a identificação e avaliação do risco; com a monitorização dos riscos e perdas, e com o controlo e mitigação de riscos; com a gestão da continuidade do negócio. (3) O âmbito dos supervisores – relacionado com a *framework* para o controlo de riscos e mitigação da Informação, e com a avaliação independente da informação. (4) O âmbito da divulgação – relacionado com a divulgação de informação às partes interessadas. Para maior detalhe sobre o acordo de Basileia II e sobre os dos dez princípios dos SI/TIC, consultar o Anexo –Basileia II.

[24] Esta família inclui um conjunto de normas relacionadas com a segurança da informação, no contexto de se estabelecer um processo para a gestão do tratamento dos Requisitos de Conformidade nos SI/TIC, no qual os Riscos de *Compliance* têm de ser geridos e tratados**.** Estas normas tratam da gestão da segurança da informação, determinando o nível adequado de segurança da informação. A norma ISO/IEC 27002 dedica o capítulo 15 às questões da *Compliance* fornecendo um conjunto de boas práticas e controlos para a sua gestão e tratamento: A *Compliance* com os Requisitos de Conformidade; A *Compliance* com as políticas e normas de segurança, e conformidade técnica; As considerações de auditoria nos sistemas de informações.

a análise do impacto dos Requisitos de Conformidade; (H3) A determinação do âmbito dos Requisitos de Conformidade; (H4) A recolha de informação e a identificação das questões de *Compliance*; (H5) A análise de risco; (H6) A implementação das acções apropriadas relativas à *Compliance*; (H7) A monitorização e o reporte; (H8) A melhoria contínua.

(H1) Segundo a autora devem ser implementados os meios mais adequados à Organização para assegurar a identificação dos Requisitos de Conformidade (Secção 2.1.1). A interpretação do Requisito de Conformidade deverá determinar se este é obrigatório ou recomendado (e.g. opcional), pois esta constatação afecta os resultados da análise do seu impacto e relevância para a Organização.

(H2) A análise do impacto dos Requisitos de Conformidade deverá facilitar a determinação das prioridades para a *Compliance* no que se refere aos esforços e aos recursos necessários. Para esta análise recomenda que sejam envolvidas e consultadas as partes interessada em matérias de *Compliance* (Secção 2.1.3), nomeadamente os SI/TIC, a Função *Compliance* (Secção 2.1.3), a função Jurídica, a função de Segurança e Risco e a função de Controlo Interno, podendo no entanto, ser envolvidas outras pessoas[25] que, de algum modo, estão relacionadas com as exigências dos requisitos (e.g. reguladores ou legisladores).

(H3) O processo para a determinação do âmbito é fundamental para assegurar as exigências dos Requisitos de Conformidade. Ao nível das aplicações (Domínio Tecnológico[26]) se não for delimitado pode mesmo tornar complexa a implementação das medidas necessárias que assegurem as exigências dos Requisitos de Conformidade.

(H4) Para a identificação das questões de *Compliance* recomenda que seja recolhida informação para determinar a existência e a extensão das lacunas para assegurar as exigências dos Requisitos de Conformidade. O objectivo é determinar até que ponto o que já existe dá resposta total ou parcial, ou não dá resposta.

(H5) Para assegurar as exigências dos Requisitos de Conformidade recomenda que se identifique os requisitos que são obrigatórios em detrimento dos requisitos que são uma boa prática. Que sejam determinados os riscos associados à não implementação dessas exigências. Esta determinação do risco permitirá priorizar os requisitos com maior impacto na Organização. Por outro lado permite determinar os Controlos de *Compliance* (Secção 2.1.2) mais adequados para mitigar os riscos identificados. Caso seja decidido que certos Controlos de *Compliance* (Secção 2.1.2) não devem ser aplicados ou ser aplicados parcialmente, propõe que exista uma aprovação formal da gestão. Este processo deverá contemplar a análise custo-benefício e avaliação dos riscos quanto ao seu impacto

[25] Pessoas - são as pessoas (colaboradores e dirigentes) utilizadas para planear, organizar, adquirir, executar, entregar, suportar, monitorizar e avaliar os SI/TIC e os seus serviços (ITGI, 2007).
[26] São considerados os seguintes componentes: Tecnologia, Aplicações/Sistemas e Infra-estruturas (ITGI, 2007).

na Organização e a identificação dos controlos compensatórios (Secção 2.1.2). A Organização antes de implementar os Controlos de *Compliance* (Secção 2.1.2) deve reflectir sobre a sua adequação e de algum modo acompanhar, e onde possível influenciar os emissores dos Requisitos de Conformidade, ou seja, devem ser realizadas reuniões regulares entre as partes interessadas, sejam internas ou externas (e.g. Reguladores e Legisladores) à Organização em matérias de *Compliance* dos SI/TIC (Secção 2.1.3).Esta autora não refere nenhuma *framework* para a identificação do risco. No contexto desta dissertação também não será sugerida nenhuma framework para a identificação do risco ficando ao critério de cada Organização a adopção da framework que melhor se adaptar à sua realidade.

(H6) A existência de lacunas e os impactos de implementação ou não (e.g. coimas, cessão da actividade, reputação) das medidas para assegurar as exigências dos requisitos devem ser determinadas. A complexidade associada à implementação nas Aplicações (Domínio Tecnológico) bem como a adequação das políticas e procedimentos (Domínio Organizacional) da Organização deve ser analisada. Esta abrangência aos Domínios Organizacional e Tecnológico encontra-se alinhado com o referido por Cascarino (CASCARINO, 2007, p.33) (Secção 2.1.2) quanto à necessidade de controlo.

(H7) A autora recomenda que deve ser desenvolvido um processo de monitorização e reporte sobre a *Compliance* dos SI/TIC, e que as recomendações significativas devem ser escaladas (e.g. CIO, Director de Risco, Director de *Compliance*), numa perspectiva de melhoria contínua, tal como referido por Cascarino (CASCARINO, 2007, p.27) (Secção 2.1.2).

(H8) Quanto à melhoria contínua recomenda que a Gestão poderá incentivar as oportunidades de melhoria dos Controlos de *Compliance* bem como proactivamente estender o âmbito da aplicação dos Controlos a outras partes do Negócio.

2.2.2 Melhorar os benefícios da *Compliance* dos SI/TIC

Dameri (DAMERI, 2009, p.27) refere que historicamente a *Compliance* tem sido vista como um encargo, no entanto recomenda que deve ser vista como uma oportunidade para as Organizações melhorarem os seus processos de negócio e as suas operações.

Segundo esta autora os investimentos na *Compliance* dos SI/TIC devem ultrapassar o âmbito do evitar as sanções decorrentes de não atender aos Requisitos de Conformidade, pois deste modo não haverá retorno. O alinhamento dos SI/TIC com o Negócio em matérias de *Compliance* permitirá a optimização destes investimentos. As iniciativas para a *Compliance* dos SI/TIC devem ser encaradas como oportunidades para explorar o conhecimento sobre os SI/TIC, para reduzir os riscos a que estes estão sujeitos e, deste modo, aumentar o valor da informação reforçando a confiança das partes interessadas na Organização. Tarantino (TARANTINO, 2008, p.15) faz a distinção entre riscos e oportunidades. Os riscos são eventos que podem ter um impacto negativo na Organização podendo

impedir a criação de valor ou mesmo destruir o valor existente. As oportunidades são eventos que podem ter um impacto positivo, podendo estes últimos ser integrados na estratégia da Organização.
Dameri (DAMERI, 2009, p.27) refere que o assegurar da exigência do Requisito de Conformidade nos SI/TIC pode estar relacionado com dois factores: a complexidade e a pouca consistência no seu tratamento. A complexidade advém do modo como geralmente os Requisitos de Conformidade são escritos. Estes são escritos num contexto jurídico e num sentido generalista para terem uma ampla aplicabilidade, raramente dizendo como os SI/TIC devem agir na prática, demonstrando pouca sensibilidade para os impactos de tais requisitos nos SI/TIC, tal como referido por Breaux e Antón (BREAUX e ANTÓN, 2007, p.1) e Hansson (HANSSON, 2008, p.64).

A pouca consistência relaciona-se com a abrangência com que os impactos das exigências dos Requisitos de Conformidade são analisados nos SI/TIC. Tal como o ISACA através do processo COBIT 4.1-ME3 (ITGI, 2007a, p.158), Dameri (DAMERI, 2009, p.27) sugere que em caso de dúvidas sobre o âmbito e objectivos dos Requisitos de Conformidade, seja solicitado aconselhamento independente, para desfazer quaisquer dúvidas. Esta autora foca a sua abordagem na *Compliance* dos sistemas que disponibilizam informação financeira. Tal como HO (HO, 2009, pp.1-2), também Dameri (DAMERI, 2009, pp.29-30) refere que para suportar a *Compliance* dos SI/TIC, as Organizações podem usar o COSO-ERM COSO, 2007) e o COBIT 4.1 (ITGI, 2007) porque ajudam as Organizações a executar de forma mais adequada, por serem referenciais que proporcionam um conjunto de boas práticas que devem servir de orientação para facilitar a gestão e deste modo as Organizações podem poupar dinheiro.

Dameri (DAMERI, 2009, p.28) recomenda os seguintes passos para a *Compliance* dos SI/TIC: (D1) Definir o âmbito da *Compliance* dos SI/TIC; (D2) Identificar, mapear, documentar todas as actividades de SI/TIC que suportam a informação financeira; (D3) Conceber os controlos de mitigação dos riscos; (D4) Avaliar os controlos; (D5) Reportar sobre as actividades da *Compliance* dos SI/TIC.

(D1) Recomenda que todas as aplicações (Domínio Tecnológico) de uma Organização devem ser incluídas no âmbito da *Compliance* dos SI/TIC, devido à sua interligação para assegurar a fiabilidade da informação financeira.

(D2) Após a delimitação do âmbito da *Compliance* dos SI/TIC, a Organização deverá identificar e mapear todas as actividades que compõem os processos (Domínio Organizacional) relacionados com a informação financeira e documentá-los. Tal como Ho (HO, 2009, pp.2-6) (Secção 2.2.1), Dameri (DAMERI, 2009, pp.29-30) para a gestão da *Compliance* abrange os Domínios Organizacional e Tecnológico alinhando-se também ao referido por Cascarino (CASCARINO, 2007, p.33) (Secção 2.1.2) quanto à necessidade de controlo.

(D3) Recomenda que se avalie os riscos existentes e as ameaças, quanto à integridade da informação financeira, e se criem controlos específicos para cada um deles. Estes controlos podem

estar nos sistemas de segurança ou integrados nas Aplicações financeiras. Esta autora indica que todos os controlos devem estar documentados para demonstrar a sua existência bem como permitir que possam ser monitorizados.

(D4) Recomenda que se criem mecanismos de avaliação, para avaliar a efectividade de cada controlo e a solidez de toda a *Compliance* dos SI/TIC, com o objectivo de detectar qualquer mau funcionamento das aplicações e identificar quem deverá ser responsabilizado por esse motivo.

(D5) Recomenda que todas as actividades relacionadas com *Compliance* dos SI/TIC devem ser reportadas e documentadas, e que os resultados devem ser claros e estarem disponíveis para as partes interessadas, quer sejam da Organização ou não.

2.2.3 O ciclo PDCA aplicado à *Compliance*

Annaswamy (ANNASWAMY, 2009, p.1) indica como impulsionadores da *Compliance*: - a actividade constante dos reguladores no reforço e garantia de que os Requisitos de Conformidade existentes são suficientes e integralmente cumpridos; - a pressão das partes interessadas da Organização para que os SI/TIC forneçam mais com menos; - a complexidade do negócio, mesmo que o negócio esteja em desaceleração pois este estará cada vez mais dependente dos SI/TIC.
Neste contexto este autor refere que para sustentar a longo prazo uma abordagem proactiva e flexível para a *Compliance*, esta deverá ser gerida com base no ritmo de mudança incutido pela Organização, através da diferença entre como está e até onde pretende ir. Esta abordagem obriga a um esforço continuado para manter e melhorar a *Compliance* da Organização, sugerindo deste modo a implementação de um Ciclo PDCA[27] para a *Compliance,* porque esta nunca tem fim, tal como referido também por HO (HO, 2009, pp.5-6).

O ciclo PDCA ((P) Planear, (E) Executar, (V) Verificar e (A) Agir) insere-se nas técnicas de gestão da mudança organizacional, que envolve toda a organização (Colaboradores e Gestão) no esforço de melhoria contínua dos processos tendo em vista a qualidade dos serviços, a economia de recursos e de tempo. É neste contexto que Annaswamy (ANNASWAMY, 2009, pp.2-3) propõe o âmbito deste ciclo aplicado à gestão da *Compliance*.

(P) Segundo o autor, a fase de planeamento tem como objectivo uma monitorização constante dos Requisitos de Conformidade, para se antecipar e perceber as exigências dos requisitos. A Organização deve procurar saber o que está no radar dos reguladores e legisladores para o acompanhar e onde possível, influenciar. Deve também perceber o que os reguladores procuram quando exercem a função de supervisores/auditores. Após a identificação devem ser avaliados os riscos associados à não implementação dos Requisitos de Conformidade, bem como do seu potencial

[27] Ciclo PDCA - também conhecido por Ciclo de Deming, é composto por quatro fases: Planear (Plan) – Estabelecer os objectivos; Executar (Do) – Implementar os processos, os procedimentos, os templates e relatórios; Verificar (Check) – Medir os resultados e comparar com o esperado; Agir (Act) – Analisar as diferenças, identificar as causas e implementar medidas correctivas adequadas.

impacto na Organização. (E) Na fase executar, recomenda a implementação de pilotos em pequena escala para minimizar os impactos na Organização. (V) Na fase verificar, recomenda uma avaliação independente ao piloto, quanto à sua eficácia. (A) Na fase agir, recomenda que devem ser analisados e tratados os eventuais pontos fracos do piloto, que depois de sanados permitirão que este seja estendido a toda a Organização.

2.2.4 Os quatro elementos da *Compliance*

Bace e Rozwell (BACE e ROZWELL, 2006, p.3) indicam quatro elementos caracterizadores da *Compliance* que devem ser considerados na aderência aos Requisitos de Conformidade: (B1) Saber o que fazer - interpretar os requisitos; (B2) Saber o que fazemos – compreender os requisitos e documentar suas políticas, processos e controlos; (B3) Fazer como dizemos – monitorizar a *Compliance* e as mudanças ao longo do tempo; (B4) Dizer o que sabemos – reportar quando solicitado.

2.3 Orientações e Boas práticas aplicáveis à *Compliance* dos SI/TIC

O COSO (COSO, 1994), COSO-ERM COSO, 2007) [28] e o COBIT 4.1 (ITGI, 2007) são referenciais que não têm a força de lei, mas muitos Requisitos de Conformidade referenciam-nas para suportar a sua efectivação[29]. Calder (CALDER, 2008, p.164) refere que se pode constatar que nenhuns destes referenciais isoladamente se poderão adequar ao assunto em análise por não serem, per si, uma solução completa. Mas as orientações obtidas da consulta das diferentes *frameworks e* normas permitem obter um resultado mais completo se soubermos aproveitar a complementaridade desses referenciais. No entanto, é importante ter o conhecimento adequado para saber quais os referenciais que se complementam para que, no conjunto, se obtenha uma resposta completa ao assunto em análise.

Dameri (DAMERI, 2009, pp.29-30) recomenda que para implementar o COSO-ERM COSO, 2007) e o COBIT 4.1 (ITGI, 2007) para a Gestão da *Compliance* é necessário em primeiro lugar mapear as duas *frameworks* e depois relacioná-los com as exigências dos Requisitos de Conformidade. Deste modo, os requisitos definem o âmbito da *Compliance*, os componentes do COSO-ERM COSO, 2007) descrevem como fazer, e as práticas de controlo[30] do COBIT 4.1 (ITGI, 2007a) definem o que fazer. Para esta autora o COBIT 4.1 (ITGI, 2007) é um instrumento muito completo para a gestão e controlo

[28] Para maior detalhe sobre o COSO-ERM consultar o Anexo – COSO.

[29] A SEC por exemplo, relativamente à lei de Sarbanes-Oxley refere a utilização pelas organizações de duas frameworks: o COSO-ERM COSO, 2007) e o COBIT 4.1 (ITGI, 2007). A SEC indica que o COBIT 4.1 (ITGI, 2007) complementa o COSO-ERM COSO, 2007), e é referido como um *framework* dos SI/TIC para o cumprimento do SOX (publicado "*IT Control Objectives for Basel II: The Importance of Governance and Risk Management for Compliance*", que disponibiliza orientações para os gestores dos SI/TIC para o Sector Financeiro (LARRY, 2007) Rittenberg Larry consultado em 2 de Dezembro de 2010, em http://www.coso.org/documents/MarioMicallef.pdf. A lei Sarbanes-Oxley Act of 2002 (SOX, 2008) foi aprovada pelo Senado e Câmara de Representantes dos Estados Unidos da América, em 2002. Esta lei torna os gestores de topo das empresas públicas responsáveis pelas falhas em providenciar informação atempada, completa e precisa para os interessados no estado do desempenho das Organizações.

[30] Práticas de Controlo - São mecanismos de controlo que apoiam a realização dos objectivos de controlo através do uso responsável dos recursos, de uma gestão adequada de risco e do alinhamento dos SI/TIC com Negócios (ISACA, 2010).

dos SI/TIC, mas indica que será necessário: - realizar uma reengenharia aos processos do ciclo de vida dos SI/TIC (Domínio Organizacional); - formalizar todas as actividades relacionadas com os processos onde se incluem procedimentos de controlo; - normalizar e adaptar todas as actividades às práticas de controlo do COBIT 4.1 (ITGI, 2007a). Os resultados deste esforço, por um lado, disponibilizam à Organização um sistema de gestão dos SI/TIC, normalizado, formalizado e avaliado, por outro lado é uma estrutura rígida, sem oportunidade de adaptá-la às mudanças ou situações específicas.

Uma das questões referidas por Dameri (DAMERI, 2009) (Secção 2.2.2) tem a ver com a necessidade efectiva de implementar o COSO-ERM COSO, 2007) e o COBIT 4.1 (ITGI, 2007) ou se será possível, com base nas orientações e boas práticas destes referenciais e após analisar as necessidades organizacionais, definir actividades para o tratamento dos Requisitos de Conformidade que se alinhem melhor com a estratégia da Organização.

2.3.1 O contexto da *Compliance* no COBIT 4.1

O COBIT 4.1 (ITGI, 2007, pp.161-164) inclui um processo, no domínio Monitorização e Avaliação, que aborda especificamente para a Gestão da *Compliance* nos SI/TIC, o processo ME3: Garantia de Conformidade com Requisitos Externos (ITGI, 2007), tendo como objectivo possibilitar a garantia da *Compliance* dos SI/TIC alinhada com o Negócio. Os processos a incluir numa *framework* de *Compliance,* propostos pelo ISACA no processo COBIT 4.1 - ME3 (ITGI, 2007) são: (ME3-1) Identificação dos Requisitos de Conformidade; (ME3-2) Optimização da Resposta; (ME3-3) Avaliação da *Compliance*; (ME3-4) Garantia de *Compliance* pela Positiva; (ME3-5) Reporte Integrado.

(ME3-1) Processo de identificação dos Requisitos de Conformidade tem como objectivo a identificação numa base contínua das leis locais e internacionais, dos regulamentos e outras exigências externas de conformidade que devam ser incorporadas nas políticas, nas normas, procedimentos e metodologias dos SI/TIC da Organização.

(ME3-2) Processo de optimização da resposta aos Requisitos de Conformidade tem como objectivo assegurar que a revisão e ajuste das políticas, das normas, dos procedimentos e das metodologias dos SI/TIC da Organização, são realizados para assegurar que as exigências dos Requisitos de Conformidade são endereçadas e comunicadas. Tal como Dameri (DAMERI, 2009) (Secção 2.2.2) o ISACA através do processo COBIT 4.1-ME3 (ITGI, 2007a, p.158) sugere que em caso de dúvidas sobre o âmbito e objectivos dos Requisitos de Conformidade, seja solicitado aconselhamento independente, para desfazer quaisquer dúvidas.

(ME3-3) Processo de avaliação da *Compliance* tem como objectivo garantir de forma continuada que as políticas, normas, procedimentos e metodologias dos SI/TIC da Organização estão *Compliance* com os Requisitos de Conformidade.

(ME3-4) Processo de garantia da *Compliance* pela positiva, tem como objectivo obter e reportar a garantia de *Compliance* e aderência a todas as políticas, derivadas de directivas internas ou Requisitos de Conformidade, confirmando que qualquer acção correctiva efectuada para endereçar qualquer falha na *Compliance* foi tomada sob responsabilidade da Gestão, de uma maneira apropriada.

(ME3-5) Processo de Reporte Integrado tem como objectivo integrar os relatórios da *Compliance* com os relatórios semelhantes de outras funções de Negócio. Esta comunicação tem a pretensão de informar sobre o estado da *Compliance* e o tratamento dos Requisitos de Conformidade. Deverá ser assegurada a completude e consistência da informação disponibilizada às partes interessadas, nomeadamente os supervisores permitindo saber a efectividade ou não da *Compliance*, assim como as respectivas necessidades de melhoria e remediação.

O ISACA através do processo COBIT 4.1-ME3 (ITGI, 2007a, p.158) recomenda a utilização de uma ferramenta de suporte à Gestão da *Compliance* nos SI/TIC, para o registo centralizado de toda a informação sobre a *Compliance* nos SI/TIC, o mesmo é recomendado por Ho (HO, 2009, p.3).

O ISACA propõe um Modelo de Maturidade para processo COBIT 4.1 - ME3 (ITGI, 2007, p.162)[31] com o objectivo de medir o nível de confiança, eficácia e eficiência do processo quanto à gestão dos Requisitos de Conformidade. Em termos práticos, os graus de maturidade mostram até que ponto é que os processos e as actividades da Organização estão documentados, controladas, monitorizadas, optimizadas e disseminadas pela Organização. Quanto maior o nível de maturidade dos processos menor o risco. O ISACA para responder às exigências de Basileia II[32] (BIS, 2002), propõe como objectivo um nível de maturidade "4" (processos geridos e medidos) para o processo COBIT 4.1 - ME3 (ITGI, 2007b, p.69).

2.3.2 O contexto da *Compliance* no COSO

Dameri (DAMERI, 2009, p.29) refere que o COSO-ERM COSO, 2007) é uma framework que tem como objectivo a auditoria interna, mas que também suporta a auditoria aos SI/TIC na qual a *Compliance* se encontra inserida. Esta autora indica que no âmbito da auditoria aos SI/TIC é necessário:

- Avaliar os riscos relativos às infra-estruturas e aplicações, para entender o âmbito do esforço de *Compliance* requerido pelos SI/TIC;
- Conceber, não apenas controlos mas um ambiente de controlo que faça a gestão da Segurança e da *Compliance* dos SI/TIC de forma integrada;
- Definir os controlos e processos de controlo, explicitando as regras a seguir e os objectivos a alcançar;

[31] Para maior detalhe sobre o modelo de maturidade do processo COBIT4.1: ME3 consultar o Anexo - Modelo de Maturidade do processo COBIT 4.1: ME3.
[32] Para maior detalhe sobre o acordo de Basileia II consultar o Anexo –Basileia II.

- Informar as partes interessadas que sejam internas ou externas (e.g. reguladores e mercados financeiros) à Organização sobre as actividades de *Compliance* e comunicar esforços, actividades e resultados obtidos;
- Monitorizar a efectividade dos controlos de SI/TIC e usar a informação daí resultante para rever as avaliações de risco e para a melhoria contínua da framework da *Compliance* dos SI/TIC.

Neste contexto Dameri (DAMERI, 2009) realça a importância dos componentes do COSO (COSO, 1994) e do COSO-ERM (COSO, 2007)[33] Ambiente de Controlo, Informação e Comunicação e a Monitorização da gestão da *Compliance* nos SI/TIC. A componente do Ambiente de Controlo, tem a finalidade de marcar o estilo de uma Organização na forma como os riscos são identificados e abordados pelos colaboradores, incluindo ambiente organizacional, a gestão dos riscos, o apetite de risco, os valores éticos e de integridade (COSO, 1994, p.4) (COSO, 2007, p.22). A componente da Informação e Comunicação tem como finalidade assegurar que as informações relevantes são identificadas, capturadas, armazenadas e comunicadas de forma atempada e adequada, possibilitando que todos os envolvidos as recebam de forma integrada, consistente e apropriada para a execução das actividades (COSO, 1994, pp.4-5) (COSO, 2007, p.22). A componente da Monitorização tem como finalidade verificar a adequação e efectividade dos controlos internos, e se estão alinhados com os objectivos propostos inicialmente (COSO, 1994, p.5) (COSO, 2007, p.22). A monitorização pode ser realizada através de acompanhamento contínuo ou através de avaliações independentes ou de ambas as formas.

2.4 O Contexto para a *Compliance* dos Serviços SI/TIC

Um Serviço de SI/TIC é disponibilizado ao Negócio para apoiar a execução dos seus processos (ITGI, 2007, p.15). Este serviço geralmente é composto pela combinação de pessoas, processos e tecnologias que suportam a execução das actividades do Negócio de uma Organização. Este serviço pode ser fornecido por uma Entidade de SI/TIC a uma ou mais Organizações clientes (ITIL V3, 2007, p.23).

Ho (HO, 2009) (Secção 2.2.1), Dameri (DAMERI, 2009) (Secção 2.2.2) e Annaswamy (ANNASWAMY, 2009) (Secção 2.2.3), Bace e Rozwell (BACE e ROZWELL, 2006) (Secção 2.2.4), e o ISACA através do processo[34] COBIT 4.1-ME3 (ITGI, 2007) (Secção 2.3.1) sugerem que a aderência aos Requisitos de Conformidade pode envolver a implementação de medidas e Controlos de *Compliance* nos SI/TIC. A implementação das medidas e controlos materializa o que é necessário implementar para assegurar as exigências dos Requisitos de Conformidade. A implementação das medidas passa pelas adequações necessárias das políticas, normas internas, processos

[33] Para maior detalhe sobre o COSO consultar o Anexo - COSO.

[34] Processo – Abordagem sistematizada que é realizada para atingir um objectivo específico; Conjunto de actividades inter-relacionadas e interactuantes que transformam entradas (inputs) em saídas (outputs); Conjunto de actividades, encadeadas de forma lógica e sequencial (ISACA, 2010).

(Referenciais de Qualidade), na formação e na redefinição dos papéis e das responsabilidades das pessoas (Domínio Organizacional) e por outro lado, caso se aplique na implementação de funcionalidades nas aplicações (Domínio Tecnológico) através da transformação do Requisito de Conformidade em Requisitos Aplicacionais. A implementação dos Controlos de *Compliance* (Secção 2.1.2) deverá ter em consideração a dimensão da Organização, a sua natureza, a sua complexidade, a diversidade das suas operações, e os Requisitos de Conformidade aplicáveis.

O ISACA através do COBIT 4.1 (ITGI, 2007, p.15) define quatro tipos de Controlos Genéricos que pela sua natureza se podem associar à *Compliance*: - os Controlos de Entidade; - os Controlos de Processo; - os Controlos Aplicacionais; - os Controlos Gerais de SI/TIC[35]. Por outro lado Cascarino (CASCARINO, 2007, pp.xxi-xxiii) divide os controlos dos SI/TIC em Controlos Gerais e Controlos Aplicacionais. Dameri (DAMERI, 2009, p.28) refere mesmo a utilização dos Controlos Aplicacionais e Controlos Gerais de SI/TIC, para a gestão da *Compliance*. Os Controlos Gerais de SI/TIC pretendem gerir o ambiente dos SI/TIC no qual estes são desenvolvidos, mantidos e operados. Estes devem englobar todos os elementos da Organização, ou seja neste caso dos SI/TIC (CASCARINO, 2007) (Secção 2.1.2). Os Controlos Aplicacionais podem ser manuais ou embebidos nas aplicações de forma a assegurar que os dados são processados com efectividade, eficiência, confidencialidade, integridade, disponibilidade e confiabilidade.

2.5 Conclusão do enquadramento da *Compliance*

O aumento de forma continuada das exigências dos Requisitos de Conformidade (Secção 2.1.1) provoca constantes alterações nas necessidades de *Compliance* (Secção 2.1.2) nos SI/TIC. As necessidades de *Compliance* pretendem garantir a efectividade da *Compliance* dos SI/TIC (Secção 2.1.3) e resultam dos novos Requisitos de Conformidade ou alterações aos existentes, e a quaisquer Recomendações de melhorias e remediação oriundas da monitorização à *Compliance* que ocorrem e surgem de forma continuada nos SI/TIC. A garantia da efectividade da *Compliance* dos SI/TIC obriga a um esforço constante para assegurar de forma continuada as exigências dos Requisitos de Conformidade, e a mitigação do Risco de *Compliance* (Secção 2.1.2) através da garantia da efectividade dos Controlos de *Compliance* (Secção 2.1.2).

A figura 1 pretende estruturar o enquadramento da *Compliance* apresentado neste capítulo.

[35] Os Controlos de Entidade são controlos que ajudam a garantir que as directrizes da Gestão são executadas na organização; os Controlos de Processo são controlos que ajudam a garantir que os processos são executados conforme foram concebidos e que os riscos de execução dos mesmos são minimizados.

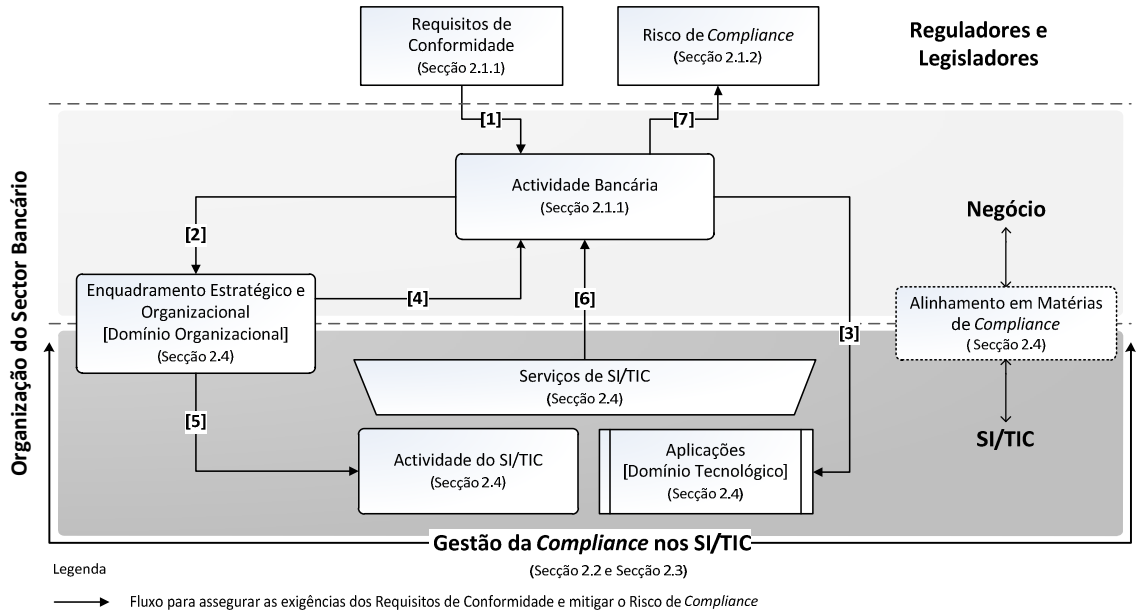

Figura 1 – Diagrama de Contexto com base no enquadramento da *Compliance*

Os Requisitos de Conformidade que são impostos a uma Organização do Sector Bancário pelos reguladores e legisladores devem ser tratados para assegurar as exigências de tais requisitos na Actividade Bancária (Secção 2.1.1) [1].

Para o tratamento destes requisitos é importante o alinhamento em matérias de *Compliance* entre o Negócio e os SI/TIC (Secção 2.2.2) em matérias de *Compliance* (Secção 2.1.3). Para assegurar o tratamento dos Requisitos de Conformidade na actividade Bancária, deverão ser analisados os respectivos impactos no Domínio Organizacional [2] e no Domínio Tecnológico [3].

No Domínio Organizacional (Enquadramento Estratégico e Organizacional) os impactos devem ser analisados em termos das políticas, normas internas, processos e procedimentos, sendo estes que definem a Actividade Bancária [4] e dos SI/TIC [5] (Secção 2.4).

No Domínio Tecnológico devem ser analisados através dos impactos nas Aplicações (Secção 2.4). Para que a Actividade Bancária esteja em *Compliance* (Secção 2.1.2) necessita que o fornecimento dos Serviços SI/TIC (Secção 2.4) assegurem de forma continuada, através dos Controlos de *Compliance* (Secção 2.1.2), que são cumpridas as exigências dos Requisitos de Conformidade nas Actividades dos SI/TIC e nas Aplicações [6].

O Risco de *Compliance* ocorre na Actividade Bancária quando esta não assegura de forma continuada as exigências dos Requisitos de Conformidade [7].

O desenvolvimento da *Framework* para a Gestão da *Compliance* nos SI/TIC teve por base as propostas de Ho (HO, 2009) (Secção 2.2.1), Dameri (DAMERI, 2009) (Secção 2.2.2) e Annaswamy

(ANNASWAMY, 2009) (Secção 2.2.3), Bace e Rozwell (BACE e ROZWELL, 2006) (Secção 2.2.4). Estas propostas encontram-se alinhadas com o proposto pelo ISACA no processo COBIT 4.1-ME3 (ITGI, 2007) (Secção 2.3.1) e pelos componentes do COSO-ERM COSO, 2007) Ambiente de Controlo, Monitorização e Informação e Comunicação (Secção 2.3.2).

Neste contexto propomos no capítulo quatro uma *framework*, denominada - *Framework* para a Gestão da *Compliance* nos SI/TIC, que pretende suportar a identificação e análise dos Requisitos de Conformidade e das Recomendações resultantes da monitorização - Analisar, a implementação das medidas e Controlos necessários para assegurar as exigências dos Requisitos de Conformidade - Implementar, a monitorização da *Compliance*- Monitorizar, bem como a comunicação às partes interessadas do estado da efectividade da *Compliance* dos SI/TIC - Reportar.

3 Metodologia

Neste capítulo pretende-se apresentar o problema, o objectivo e a metodologia adoptada nesta dissertação.

3.1 Problema

Necessidade de uma entidade gestora dos SI/TIC de uma Organização do Sector Bancário determinar o (a) que fazer e (b) como fazer para assegurar a aderência aos Requisitos de Conformidade (Secção 2.1.1) nos SI/TIC, evitando incorrer em risco de não *Compliance* (Secção 2.1.2).

A gestão da *Compliance* nos SI/TIC foi mesmo considerada como a principal questão no estudo "*Regulatory compliance is top concern in 2011*" do ISACA (ISACA, 2011), tendo sido referido por Cox (COX, 2008, p.553) que deve existir uma proactividade no tratamento da *Compliance*, sugerindo deste modo a criação de processos proactivos para o tratamento dos Requisitos de Conformidade (Secção 2.2).

- Problema 1: No que se refere à determinação do que fazer, é devido à complexidade de alguns requisitos, porque são escritos num contexto jurídico e num sentido demasiado generalista para terem uma ampla aplicabilidade, e raramente dizem como as entidades gestora dos SI/TIC devem agir na prática. Este problema também foi identificado por Ho (HO, 2009), Dameri (DAMERI, 2009) (Secção 2.2.2), Breaux e Antón (BREAUX and ANTÓN, 2007) e Hansson (HANSSON, 2008) (Secção 2.2).

- Problema 2: No que se refere à determinação de como fazer, é devido à falta de uma abordagem transversal quanto à gestão dos Requisitos de Conformidade poder limitar uma visão mais ampla do valor efectivo da *Compliance* quanto ao risco associado à não implementação das medidas e Controlos que assegurem as exigências de tais requisitos. Este problema também foi referido por Ho (HO, 2009) (Secção 2.2.1), Dameri (DAMERI, 2009) (Secção 2.2.2), Annawamy (ANNASWAMY, 2009), Bace e Rozwell (BACE e ROZWELL, 2006) (Secção 2.2.3) e Ross (ROSS,2007) (Secção 2.2).

3.2 Objectivos

Esta dissertação pretende alcançar os seguintes objectivos:

- Objectivo 1: Elaborar uma framework baseada nas orientações e boas práticas para operacionalizar o suporte no tratamento dos Requisitos de Conformidade.

- Objectivo 2: Certificar a adequação da Framework para a *Compliance* dos Serviços de SI/TIC à solução de um problema real.

Pretende-se também que a *framework* dê, de forma sucinta e sistematizada, uma resposta científica ao problema (Secção 3.1), ainda pouco explorado a nível académico.

3.3 Metodologia

A metodologia de investigação adoptada tem duas fases principais: (i) pesquisa exploratória e desenvolvimento da *framework;* e (ii) elaboração de um estudo de caso para certificar a sua adequação na garantia da *Compliance* dos SI/TIC com os Requisitos de Conformidade.

A fase (i) iniciou-se com uma pesquisa exploratória para o desenvolvimento da *framework* através da análise das propostas de vários autores (Secção 2.2) citados nesta dissertação e entidades como o ISACA através do processo COBIT 4.1 - ME3 (ITGI, 2007) (Secção 2.3.1) e COSO-ERM COSO, 2007) (Secção 2.3.2) sobre a gestão do tratamento dos Requisitos de Conformidade nos SI/TIC. Complementarmente explorou-se as orientações e boas práticas das *frameworks* e normas com o objectivo de fundamentar o desenvolvimento da *framework*. Com base nesta pesquisa foi desenvolvida a *Framework* para a Gestão da *Compliance* nos SI/TIC.

Na fase (ii) foi realizado um estudo de caso para a avaliação da *framework* desenvolvida. O estudo de caso foi efectuado numa entidade gestora dos SI/TIC do Sector Bancário português, dado o autor ter uma intervenção directa na sua implementação.

Yin (YIN, 2003) recomenda o método, estudo de caso quando os fenómenos em estudo não são dissociáveis do seu contexto. O objectivo deste estudo de caso é relatar os factos como sucederam, descrevendo situações factuais, proporcionar conhecimento acerca do fenómeno estudado através da sua análise e avaliação.
A figura 2 apresenta o diagrama de contexto da metodologia adoptada nesta dissertação.

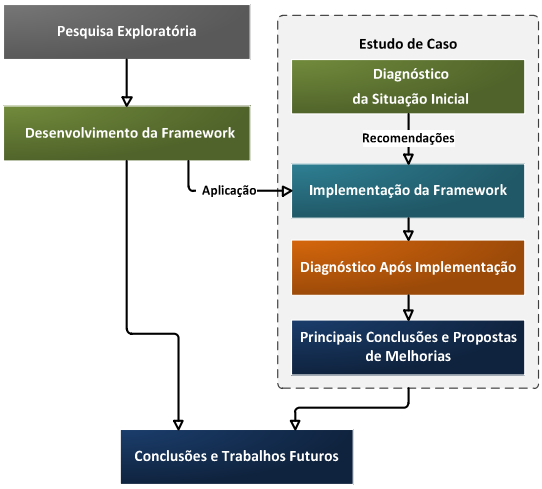

Figura 2 – Diagrama de Contexto da Metodologia Adoptada

4 A *Framework* para a Gestão da *Compliance* dos SI/TIC

Neste capítulo é apresentado o desenvolvimento da *framework* para a *Compliance* dos SI/TIC. Este desenvolvimento encontra-se sustentado pelo apresentado no capítulo 2 desta dissertação.

A *framework* desenvolvida pretende suportar o tratamento dos Requisitos de Conformidade e as Recomendações oriundas da Monitorização da *Compliance* nos SI/TIC, para garantir a efectividade da *Compliance* dos SI/TIC. Para atingir este objectivo são propostos quatro processos para a *Framework* para a Gestão da *Compliance* dos SI/TIC: Analisar; Implementar; Monitorizar; Reportar.

Na figura 3, recorrendo à notação EPC[36], são apresentados os processos da *Framework* para a *Compliance* dos SI/TIC desenvolvida.

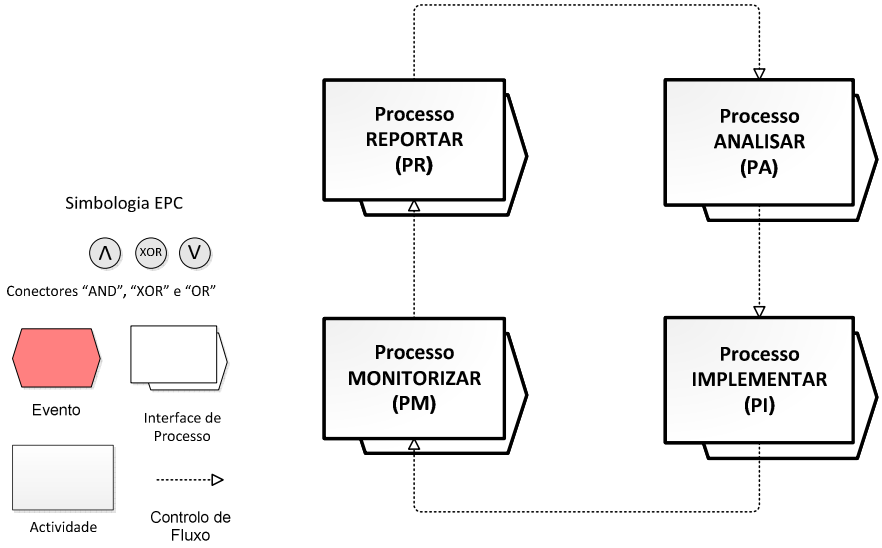

Figura 3 – Modelo dos processos da *Framework* para a Gestão da *Compliance* nos SI/TIC.

[36] A notação EPC (Event-Driven Process Chain), desenvolvida pela IDS-Scheer dentro da arquitectura do ARIS (*Architecture of Integrated Information Systems*) - é uma das ferramentas de maior sucesso mundial na área de modelação de processos e tem sido usada por muitas Organizações para modelar, analisar e redesenhar os seus processos.

4.1 Caracterização do processo: Analisar (PA)

A tabela 1 apresenta a caracterização do processo: Analisar (PA).

<table>
<tr><th colspan="2">Objectivo</th></tr>
<tr><td colspan="2">Este processo tem como objectivos assegurar a identificação das necessidades de Compliance, analisar os seus impactos, e propor os custos de implementação para assegurar as exigências do Requisito de Conformidade nos SI/TIC (Secção 2.2, Secção 2.3).</td></tr>
<tr><th>Entradas (Figura 4)</th><th>Procedência</th></tr>
<tr><td>Novos Requisitos de Conformidade ou alterações aos existentes (PA.E1).</td><td>Reguladores, Legisladores, e as políticas e normas internas à Organização (Secção 2.1.1).</td></tr>
<tr><td>Recomendações da Monitorização da Compliance dos SI/TIC (PR.E2)</td><td>Processo Reportar (PR) (Figura 4)</td></tr>
<tr><th colspan="2">Descrição</th></tr>
<tr><td colspan="2">O processo Analisar (PA) é composto por três actividades:
• Identificar e Catalogar Requisitos de Conformidade (PA.1)
• Determinar Âmbito e Objectivos (PA.2)
• Quantificar os Impactos para a Compliance (PA.3)
Deverá ser usada uma ferramenta de suporte à Gestão da Compliance dos SI/TIC (Secção 2.2.1 e Secção 2.3.1), para o registo e consulta da informação que a Organização entender adequada.</td></tr>
<tr><th colspan="2">Intervenientes</th></tr>
<tr><td colspan="2">O ISACA através do processo COBIT 4.1-ME3(ITGI, 2007) e o BIS (BIS, 2005), propõem os seguintes intervenientes:
• Função Compliance dos SI/TIC e a Função Compliance da Organização.
• Domínio Organizacional pelo Dono do Processo de Negócio.
• Domínio tecnológico através do Responsável pelo Desenvolvimento e áreas de Risco e Segurança, PMO (Project Management Officer) e Responsável pela Administração dos SI/TIC (funções como Qualidade, Recursos Humanos, e Controlo Interno).</td></tr>
<tr><th>Saídas (Figura 4)</th><th>Subsequência (Figura 4)</th></tr>
<tr><td>Proposta de Solução de Compliance Aprovada (PA.E4)</td><td>Processo Implementar (PI).</td></tr>
</table>

Tabela 1 - Caracterização do processo: Analisar (PA).

4.1.1 Modelação do Processo (PA)

A figura 4 apresenta a modelação do processo Analisar (PA), que contempla as suas actividades, eventos de entrada e saída, e as interfaces com outros processos da *Framework* para a Gestão da *Compliance* nos SI/TIC (Figura 3).

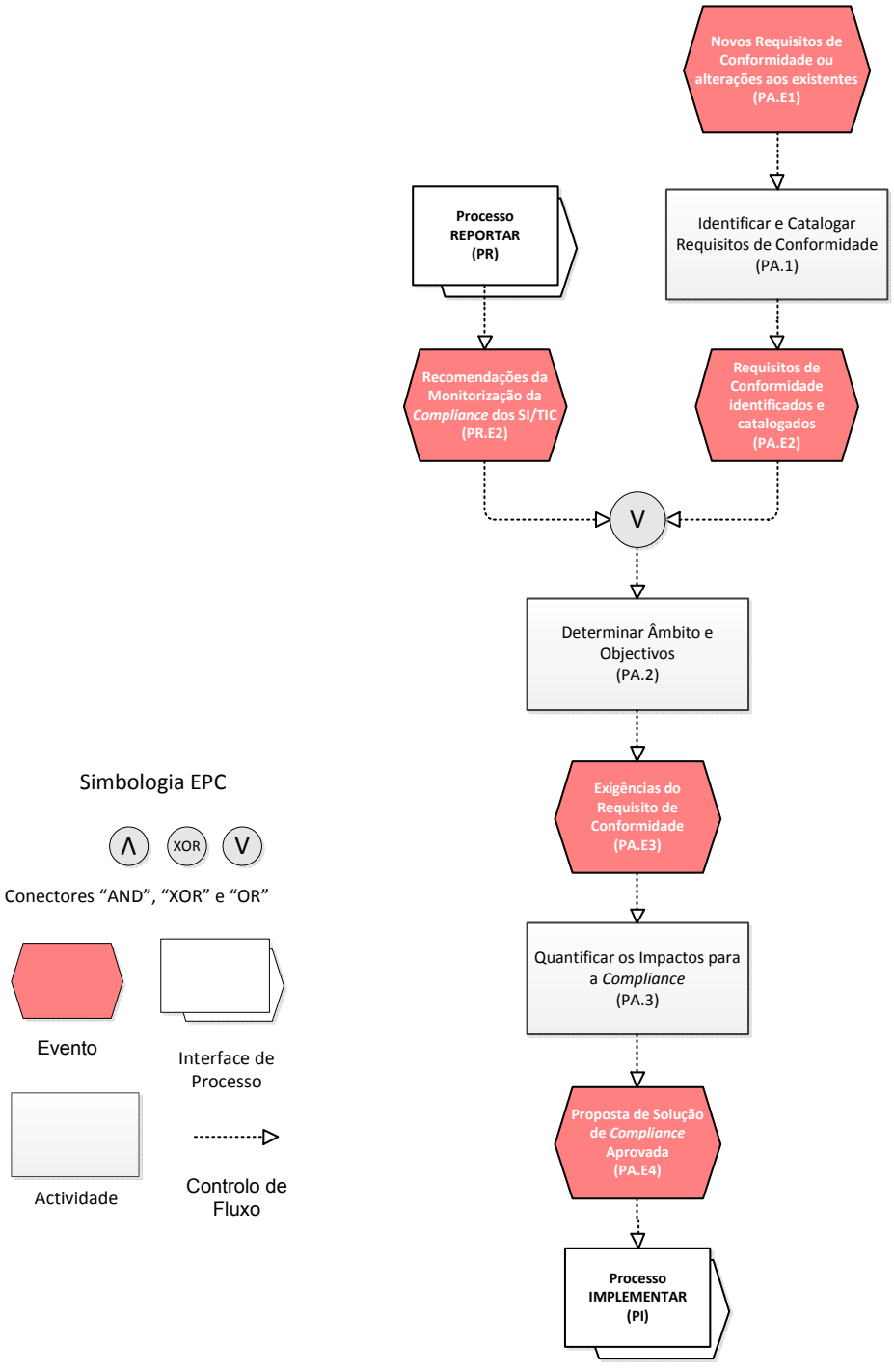

Figura 4 – Modelo EPC do processo Analisar (PA).

4.1.2 Actividade: Identificar e Catalogar Requisitos de Conformidade (PA.1)

A tabela 2 apresenta a caracterização da actividade: Identificar e Catalogar Requisitos de Conformidade (PA.1), do processo Analisar (PA).

Proposta de Solução Alternativa	
Os objectivos desta actividade são a identificação de novos Requisitos de Conformidade ou alterações aos existentes e a sua catalogação[37].	
Entradas (Figura 4)	**Procedência**
Novos Requisitos de Conformidade ou alterações aos existentes (PA.E1).	Reguladores, Legisladores, e as políticas e normas internas à Organização (Secção 2.1.1).
Descrição	
Nesta actividade para a identificação contínua de Novos Requisitos de Conformidade ou alterações aos existentes (PA.E1) deverá ocorrer: • Reuniões de forma continuada com as partes interessadas em matérias de *Compliance* da Organização, ou reuniões com Reguladores, Legisladores. • Análise do ambiente da *Compliance* e sempre que possível antecipar e perceber as exigências dos requisitos.	
Intervenientes e Atribuição de Responsabilidades	
• A execução deverá ser assegurada pela Função *Compliance* dos SI/TIC e pela Função *Compliance* da Organização.	
Saídas (Figura 4)	**Subsequência** (Figura 4)
Requisitos de Conformidade identificados e catalogados (PA.E2).	Actividade Determinar Âmbito e Objectivos (PA.2) do processo Analisar (PA).

Tabela 2 - Identificar e Catalogar Requisitos de Conformidade (PA.1), do processo Analisar (PA).

[37] Como (i) indicado pelo ISACA através do processo COBIT 4.1- ME3 (ITGI, 2007) ((ME3-1) - Secção 2.3.1); (ii) as boas práticas de controlo deste processo (ITGI, 2007b) (Secção 2.4); e (iii) referido pelos seguintes autores citados: Ho (HO, 2009) ((H1) - Secção 2.2.1), e Annaswamy (ANNASWAMY, 2009) ((P) - Secção 2.2.3).

4.1.3 Actividade: Determinar Âmbito e Objectivos (PA.2)

A tabela 3 apresenta a proposta de solução para a actividade: Determinar Âmbito e Objectivos (PA.2), do processo Analisar (PA).

<table>
<tr><th colspan="2">Proposta de Solução Alternativa</th></tr>
<tr><td colspan="2">Os objectivos desta actividade são determinar o âmbito e objectivos dos Requisitos de Conformidade e das Recomendações da Monitorização da Compliance dos SI/TIC[38].</td></tr>
<tr><th>Entradas (Figura 4)</th><th>Procedência (Figura 4)</th></tr>
<tr><td>Requisitos de Conformidade identificados e catalogados (PA.E2)</td><td>Actividade Identificar e Catalogar Requisitos de Conformidade (PA.1) do processo Analisar (PA)</td></tr>
<tr><td>Recomendações da Monitorização da Compliance dos SI/TIC (PR.E2)</td><td>Processo Reportar (PR)</td></tr>
<tr><th colspan="2">Descrição</th></tr>
<tr><td colspan="2">Nesta actividade com base nos Requisitos de Conformidade identificados e catalogados (PA.E2), novos ou alterados, e das Recomendações da Monitorização da Compliance dos SI/TIC (PR.E2), deverá ocorrer para cada requisito:
Determinação/revisão e documentação dos objectivos e âmbito através da:
Indicação das boas práticas (Domínio Organizacional) das frameworks e normas aplicáveis ao descrito nas secções/artigos do Requisito de Conformidade.
Especificação dos Requisitos Aplicacionais (Domínio Tecnológico) com base nas exigências do Requisito de Conformidade.
Caso se aplique deverá ser solicitado aconselhamento independente para desfazer quaisquer dúvidas sobre os objectivos e âmbito do Requisito de Conformidade.
Determinação, documentação e comunicação das Exigências do Requisito de Conformidade (PA.E3), e subsequente aprovação pela Gestão.</td></tr>
<tr><th colspan="2">Intervenientes e Atribuição de Responsabilidades</th></tr>
<tr><td colspan="2">A realização deverá ser assegurada pela Função Compliance dos SI/TIC, do Responsável do Processo de Negócio, do Responsável pelo Desenvolvimento, PMO e Responsável pela Administração dos SI/TIC.
O acompanhamento deverá ser assegurado pela Função Compliance da Organização e das áreas de Risco e Segurança.</td></tr>
</table>

[38] Como (i) indicado pelo ISACA através do processo COBIT 4.1- ME3 (ITGI, 2007) ((ME3-2) - Secção 2.3.1); (ii) as boas práticas de controlo deste processo (ITGI, 2007b) (Secção 2.4);, (iii) pelo COSO (COSO, 1994) e COSO-ERM (COSO, 2007) através do seu componente, Ambiente de Controlo (Secção 2.3.2); e (iv) referido pelos seguintes autores citados: Ho (HO, 2009) ((H2), (H4) e (H6) - Secção 2.2.1) e Dameri (DAMERI, 2009) ((D2) - Secção 2.2.2), Bace e Rozwell (BACE e ROZWELL, 2006) ((B1) e (B2) - Secção 2.2.4).

Saídas (Figura 4)	**Subsequência** (Figura 4)
Exigências do Requisito de Conformidade (PA.E3)	Actividade Quantificar os Impactos para a *Compliance* (PA.3) do processo Analisar (PA)

Tabela 3 - Determinar Âmbito e Objectivos (PA.2), do processo Analisar (PA).

4.1.4 Actividade: Quantificar os Impactos para a *Compliance* (PA.3)

A tabela 4 apresenta a proposta de solução para a actividade: Quantificar os Impactos para a *Compliance* (PA.3), do processo Analisar (PA).

Proposta de Solução Alternativa	
Os objectivos desta actividade são a identificação das lacunas para aferir os impactos e indicar os custos relacionados com as medidas e os Controlos de *Compliance* necessários implementar, para a *Compliance* dos SI/TIC [39].	
Entradas (Figura 4)	**Procedência** (Figura 4)
Exigências do Requisito de Conformidade (PA.E3)	Actividade Determinar Âmbito e Objectivos (PA.2) do processo Analisar (PA)
Descrição	
Nesta actividade, com base nas Exigências do Requisito de Conformidade (PA.E3) deverá ocorrer: • A determinação e documentação: o Das Funcionalidades Aplicacionais com base nos Requisitos Aplicacionais. o Das lacunas entre as exigências do requisito e os Referênciais de Qualidade (Secção 2.4) existentes, as Funcionalidades Aplicacionais e Controlos de *Compliance* existentes, que possam dar resposta total ou parcial às exigências do requisito. o Dos impactos do que será necessário implementar para assegurar as exigências do requisito. o Dos riscos associados à não implementação das exigências do requisito. o Do alinhamento das medidas e Controlos de *Compliance* dos SI/TIC com os objectivos de Negócio. o Dos custos associados de implementação para a *Compliance* dos SI/TIC. • Elaboração, comunicação da Proposta de Solução de *Compliance* (PA.E4) e subsequente aprovação pela Gestão. A proposta deverá contemplar a informação relacionada com a resposta às exigências do Requisito de Conformidade.	

[39] Como (i) indicado pelo ISACA através do processo COBIT 4.1- ME3 (ITGI, 2007) ((ME3-2) - Secção 2.3.1); e (ii) referido pelos seguintes autores citados: Ho (HO, 2009) ((H5) - Secção 2.2.1), Annaswamy (ANNASWAMY, 2009) ((P) - Secção 2.2.3) e Dameri (DAMERI, 2009) ((D3) - Secção 2.2.2).

Intervenientes e Atribuição de Responsabilidades	
• A realização deverá ser assegurada pela Função *Compliance* dos SI/TIC, do Responsável do Processo de Negócio, do Responsável pelo Desenvolvimento, PMO e Responsável pela Administração dos SI/TIC. • O acompanhamento deverá ser assegurado pela Função *Compliance* da Organização e pelas áreas de Risco e Segurança e Responsável pela Administração dos SI/TIC.	
Saídas (Figura 4)	**Subsequência** (Figura 4)
Proposta de Solução de *Compliance* Aprovada (PA.E4)	Processo Implementar (PI)

Tabela 4 - Quantificar os Impactos para a *Compliance* (PA.3), do processo Analisar (PA).

4.1.5 Métricas e Indicadores do Processo (PA)

A tabela 5 apresenta as Métricas e os Indicadores do processo Analisar (PA), tendo como referencia as métricas exemplificativas[40] indicadas pelo ISACA, através do processo COBIT 4.1-ME3 (ITGI, 2007). Os períodos actuais e anteriores[41] apresentados na tabela 5 deverão ser definidos pela Organização.

[40] As métricas exemplificativas indicadas pelo ISACA são: (i) Intervalo médio entre a identificação do Requisito de Conformidade e a sua resolução; (ii) Intervalo médio entre a publicação de um Requisito de Conformidade e o início de um processo de revisão de conformidade**.** Para maior detalhe sobre as métricas do processo COBIT4.1: ME3 consultar o Anexo - Relacionamento entre Objectivos e Métricas do processo COBIT 4.1: ME3.

[41] O Periodo é o intervalo de tempo caracterizado por determinados acontecimentos ou fenómenos que medeia duas datas. Neste contexto o período actual é o tempo que medeia a data na qual foi determinado o indice anterior (periodo anterior) e a data em que esse irá ser novamente determinado (e.g. perído anterior de Janeiro a Fevereiro, perído actual de Fevereiro a Março para se derterminar o indice referente ao periodo de Março).

ID	Objectivos	Indicadores	Métricas
M1	Reduzir o intervalo médio entre a publicação de um Requisito de Conformidade (novo/alteração) e a sua catalogação.	I_{M1} = Índice do número de dias entre a publicação do Requisito de Conformidade (novo/alteração) e a catalogação do pedido, no período. Fórmula $I_{M1} = B_{M1} / A_{M1} \times 100$	A_{M1} = Número de dias entre a publicação do Requisito de Conformidade (novo/alteração) e a catalogação do pedido, no período anterior. B_{M1} = Número de dias entre a publicação do Requisito de Conformidade (novo/alteração) e a catalogação do pedido, no período actual.
M2	Reduzir o número de recomendações de remediação identificadas na Monitorização.	I_{M2} = Índice do número de recomendações de remediação identificadas na Monitorização, no período. Fórmula $I_{M2} = B_{M2} / A_{M2} \times 100$	A_{M2} = Número de recomendações de remediação identificadas na Monitorização, no período anterior. B_{M2} = Número de recomendações de remediação identificadas na Monitorização, no período actual.
M3	Reduzir o custo associado à correcção das recomendações de remediação identificadas na Monitorização. (1)	I_{M3} = Índice do custo associado à correcção das deficiências identificadas na Monitorização, no período. Fórmula $I_{M3} = B_{M3} / A_{M3} \times 100$	A_{M3} = Custos associados à correcção das deficiências identificadas na Monitorização, no período anterior. B_{M3} = Custos associados à correcção das deficiências identificadas na Monitorização, no período actual.

(1) Deverá ser tido em consideração a complexidade das exigências do requisito e da sua implementação, bem como os critérios de interpretação dos mesmos.

Tabela 5 - Métricas e Indicadores do processo Analisar (PA).

4.2 Caracterização do processo: Implementar (PI)

A tabela 6 apresenta a caracterização do processo: Implementar (PI).

<table>
<tr><th colspan="2">Objectivo</th></tr>
<tr><td colspan="2">Este processo tem como objectivo assegurar que o que é implementado corresponde à Proposta de Solução de Compliance para a Compliance dos SI/TIC (Secção 2.2, Secção 2.3 e Secção 2.4).</td></tr>
<tr><th>Entradas (Figura 5)</th><th>Procedência (Figura 5)</th></tr>
<tr><td>Proposta de Solução de Compliance Aprovada (PA.E4)</td><td>Processo Analisar (PA)</td></tr>
<tr><th colspan="2">Descrição</th></tr>
<tr><td colspan="2">O processo Implementar (PI) é composto por quatro actividades:
• Conceber a Solução de Compliance (PI.1)
• Validar a Concepção da Solução de Compliance (PI.2)
• Implementar a Solução de Compliance (PI.3)
• Aferir a Efectividade da Solução de Compliance (PI.4)
Deverá ser usada uma ferramenta de suporte à Gestão da Compliance dos SI/TIC (Secção 2.2.1 e Secção 2.3.1), para o registo e consulta da informação que a Organização entender adequada.</td></tr>
<tr><th colspan="2">Intervenientes</th></tr>
<tr><td colspan="2">O ISACA através do processo COBIT 4.1-ME3(ITGI, 2007) e o BIS (BIS, 2005), propõem os seguintes intervenientes:
• Função Compliance dos SI/TIC e a Função Compliance da Organização.
• Domínio Organizacional pelo Responsável do Processo de Negócio.
• Domínio Tecnológico através do Responsável pelo Desenvolvimento, áreas de Risco e Segurança, PMO, Responsável pelas Operações, Responsável pela Administração dos SI/TIC.</td></tr>
<tr><th>Saídas (Figura 5)</th><th>Subsequência (Figura 5)</th></tr>
<tr><td>Compliance Implementada Aprovada (PI.E5)</td><td>Processo Monitorizar (PM)</td></tr>
</table>

Tabela 6 - Caracterização do processo: Implementar (PI)

4.2.1 Modelação do Processo (PI)

A figura 5 apresenta a modelação do processo Implementar (PI), que contempla as suas actividades, eventos de entrada e saída, e as interfaces com outros processos da *Framework* para a Gestão da *Compliance* nos SI/TIC (Figura 3).

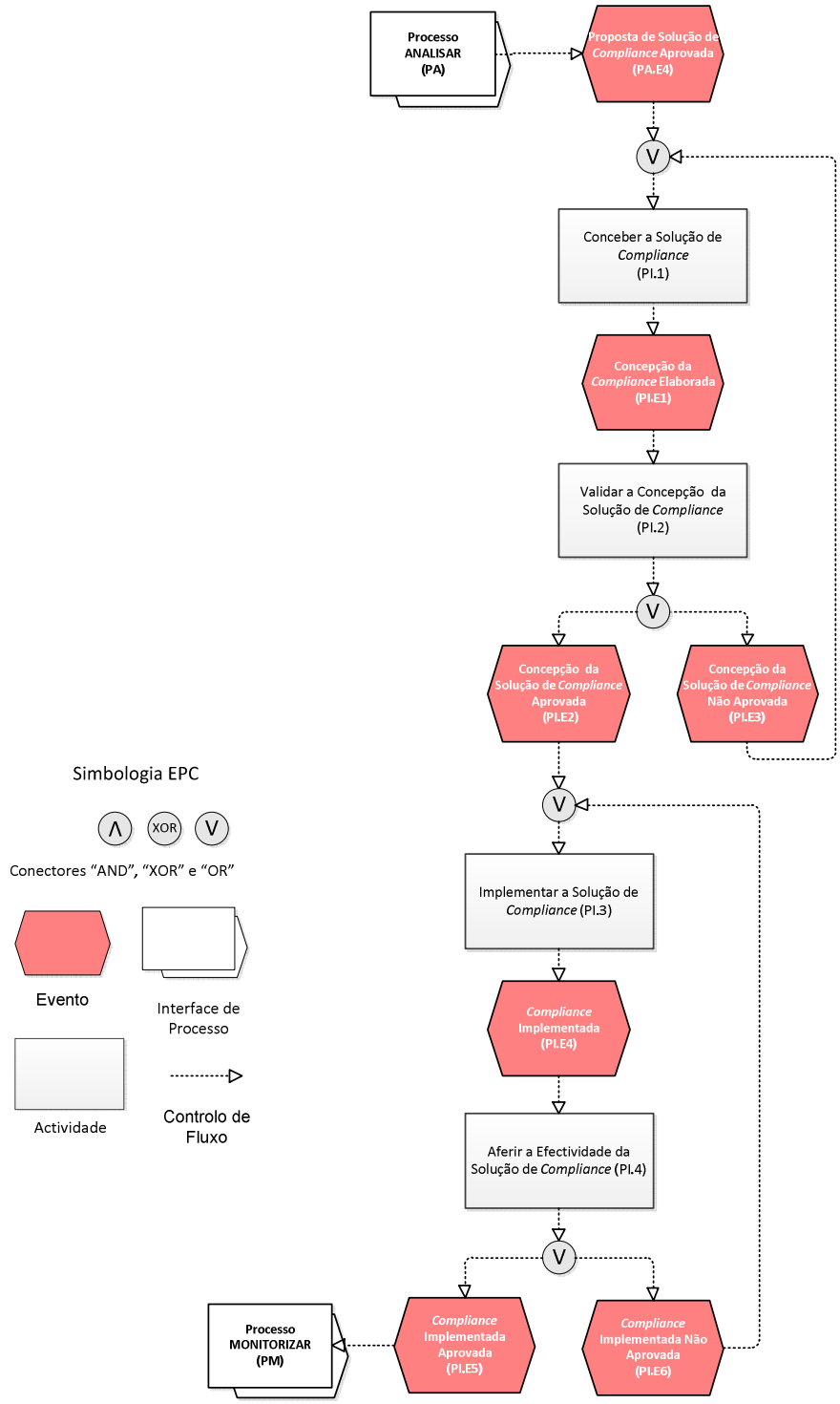

Figura 5 – Modelo EPC do processo Implementar (PI)

4.2.2 Actividade: Conceber a Solução de *Compliance* (PI.1)

A tabela 7 apresenta a proposta de solução para a actividade: Conceber a Solução de *Compliance* (PI.1), do processo Implementar (PI).

Proposta de Solução Alternativa	
O objectivo desta actividade é a concepção da *Compliance*[42].	
Entradas (Figura 5)	**Procedência** (Figura 5)
Proposta de Solução de *Compliance* Aprovada (PA.E4)	Processo Analisar (PI)
Concepção da Solução de *Compliance* Não Aprovada (PI.E3)	Actividade Validar a Concepção da Solução de *Compliance* (PI.2) do processo Implementar (PI)
Descrição	
Nesta actividade, com base na Proposta de Solução de *Compliance* (PA.E4), deverá ocorrer: • O detalhe das medidas e dos Controlos de *Compliance* necessárias para a *Compliance* tecnológica e organizacional. • Indicação das responsabilidades pelos Controlos de *Compliance*. • Determinar os mecanismos, os critérios e a frequência de monitorização dos Controlos de *Compliance*. • No caso de Concepção da Solução de *Compliance* Não Aprovada (PI.E3), deverão ser analisadas e efectuadas as devidas correcções indicadas no Relatório de Constatações da Concepção da *Compliance*.	
Intervenientes e Atribuição de Responsabilidades	
• A realização deverá ser assegurada pelo Responsável pelo Desenvolvimento, PMO e pelo Responsável pela Administração dos SI/TIC. • O acompanhamento deverá ser assegurado pela Função *Compliance* dos SI/TIC, pela Função *Compliance* da Organização e pelas áreas de Risco e Segurança.	
Saídas (Figura 5)	**Subsequência** (Figura 5)
Concepção da Solução de *Compliance* Elaborada (PI.E1)	Actividade Validar a Concepção da Solução de *Compliance* (PI.2) do processo Implementar (PI)

Tabela 7 - Conceber a Solução de *Compliance* (PI.1), do processo Implementar (PI).

[42] Como (i) indicado pelo ISACA através do processo COBIT 4.1- ME3 (ITGI, 2007) ((ME3-2) - Secção 2.3.1); (ii) referido pelos autores citados: Ho (HO, 2009) ((H6) - Secção 2.2.1), Dameri (DAMERI, 2009) ((D3) - Secção 2.2.2) e Bace e Rozwell (BACE e ROZWELL, 2006) (B2) - Secção 2.2.4); e (iii) e no contexto do apresentado na Secção 2.4 sobre a implementação das medidas e controlos.

4.2.3 Actividade: Validar a Concepção da Solução de *Compliance* (PI.2)

A tabela 8 apresenta a proposta de solução para a actividade: Validar a Concepção da Solução de *Compliance* (PI.2), do processo Implementar (PI).

Proposta de Solução Alternativa	
O objectivo desta actividade é o de verificar a adequação da eficiência da concepção das medidas e dos Controlos de *Compliance* indicados na Proposta de Solução de *Compliance*[43].	
Entradas (Figura 5)	**Procedência** (Figura 5)
Concepção da Solução de *Compliance* Elaborada (PI.E1)	Actividade Conceber a Solução de *Compliance* (PI.1) do processo Implementar (PI)
Descrição	
Nesta actividade com base na Concepção da Solução de *Compliance* Elaborada (PI.E1) deverá ocorrer: • Testes à concepção para aferir a existência de deficiências da concepção. • Caso não existam deficiências na concepção (PI.E2) deverá ser remetido para Implementar a Solução de *Compliance* (PI.3), e subsequente aprovação pela Gestão. • Caso existam deficiências deverá ser elaborado o Relatório de Constatações de Concepção da *Compliance,* e remetido para as devidas correcções (PI.E3).	
Intervenientes e Atribuição de Responsabilidades	
• A realização deverá ser assegurada pela Função *Compliance* dos SI/TIC e pelo Responsável do Processo de Negócio, áreas de Risco e Segurança. • O acompanhamento deverá ser assegurado pela Função *Compliance* da Organização, e pelo Responsável pelo Desenvolvimento, PMO e Responsável pela Administração dos SI/TIC.	
Saídas (Figura 5)	**Subsequência** (Figura 5)
Concepção da Solução de *Compliance* Aprovada (PI.E2)	Actividade Implementar a Solução de *Compliance* (PI.3) do processo Implementar (PI)
Concepção da Solução de *Compliance* Não Aprovada (PI.E3)	Actividade Conceber a Solução de *Compliance* (PI.1) do processo Implementar (PI)

Tabela 8 - Validar a Concepção da Solução de *Compliance* (PI.2), do processo Implementar (PI).

[43] Como (i) indicado pelo ISACA através do processo COBIT 4.1- ME3 (ITGI, 2007) ((ME3-2) - Secção 2.3.1); (ii) referido pelos autores citados: Ho (HO, 2009) ((H8) - Secção 2.2.1) e Dameri (DAMERI, 2009) ((D4) - Secção 2.2.2); e (iii) e no contexto do apresentado na Secção 2.4 sobre a implementação das medidas e controlos.

4.2.4 Actividade: Implementar a Solução de *Compliance* (PI.3)

A tabela 9 apresenta a proposta de solução para a actividade: Implementar a Solução de *Compliance* (PI.3), do processo Implementar (PI).

<table>
<tr><th colspan="2">Proposta de Solução Alternativa</th></tr>
<tr><td colspan="2">O objectivo desta actividade é a implementação da Compliance concebida[44].</td></tr>
<tr><th>Entradas (Figura 5)</th><th>Procedência (Figura 5)</th></tr>
<tr><td>Concepção da Solução de Compliance Aprovada (PI.E2)</td><td>Actividade Validar a Concepção da Solução de Compliance (PI.2) do processo Implementar (PI)</td></tr>
<tr><td>Compliance Implementada Não Aprovada (PI.E6)</td><td>Actividade Aferir a Efectividade da Solução de Compliance (PI.4) do processo Implementar (PI)</td></tr>
<tr><th colspan="2">Descrição</th></tr>
<tr><td colspan="2">Nesta actividade, com base na Concepção da Solução de Compliance Aprovada (PI.E2),deverá ocorrer:
• Implementação das medidas e dos Controlos de Compliance necessárias para a Compliance tecnológica e organizacional.
• No caso de Compliance Implementada Não Aprovada (PI.E6), deverão ser analisadas e efectuadas as devidas correcções às deficiências operacionais indicadas no Relatório de Constatações da Implementação da Compliance.</td></tr>
<tr><th colspan="2">Intervenientes e Atribuição de Responsabilidades</th></tr>
<tr><td colspan="2">• A realização deverá ser assegurada pelo Responsável pelo Desenvolvimento, PMO e Responsável pela Administração dos SI/TIC.
• O acompanhamento deverá ser assegurado pela Função Compliance dos SI/TIC e pela Função Compliance da Organização e pelo Responsável do Processo de Negócio, áreas de Risco e Segurança.</td></tr>
<tr><th>Saídas (Figura 5)</th><th>Subsequência (Figura 5)</th></tr>
<tr><td>Compliance Implementada (PI.E4)</td><td>Actividade Aferir a Efectividade da Solução de Compliance (PI.4) do processo Implementar (PI)</td></tr>
</table>

Tabela 9 - Implementar a Solução de *Compliance* (PI.3), do processo Implementar (PI).

[44] Como (i) indicado pelo ISACA através do processo COBIT 4.1- ME3 (ITGI, 2007) ((ME3-2) - Secção 2.3.1); (ii) sugerido de de modo indirecto a implementação da Solução de *Compliance* pelos autores citados na Secção 2.2.2; e (iii) e no contexto do apresentado na Secção 2.4 sobre a implementação das medidas e controlos.

4.2.5 Actividade: Aferir a Efectividade da Solução de *Compliance* (PI.4)

A tabela 10 apresenta a proposta de solução para a actividade: Aferir a Efectividade da Solução de *Compliance* (PI.4), do processo Implementar (PI).

Proposta de Solução Alternativa	
O objectivo desta actividade é o de aferir a eficácia da implementação da *Compliance*[45].	
Entradas (Figura 5)	**Procedência** (Figura 5)
Compliance Implementada (PI.E4)	Actividade Implementar a Solução de *Compliance* (PI.3) do processo Implementar (PI)
Descrição	
Nesta actividade após a Implementação da *Compliance* (PI.E4) deverá ocorrer: • Testes para aferir a existência de deficiências operacionais. • Caso não existam deficiências na implementação (PI.E5) e após aprovação pela Gestão, deverá ser iniciada a monitorização e auditorias da *Compliance* nos SI/TIC. Por outro lado, deverão ocorrer avaliações aos Fornecedores de Serviços Externos de SI/TIC no que se refira a matérias de *Compliance* relacionadas com o Requisito de Conformidade. • Caso existam deficiências deverá ser elaborado o relatório de Constatações de Implementação da *Compliance,* e remetido para as devidas correcções (PI.E6).	
Intervenientes e Atribuição de Responsabilidades	
• A realização deverá ser assegurada pela Função *Compliance* dos SI/TIC e pelo Responsável do Processo de Negócio, áreas de Risco e Segurança. • O acompanhamento deverá ser assegurado pela Função *Compliance* da Organização, e pelo Responsável pelo Desenvolvimento, PMO e Responsável pela Administração dos SI/TIC.	
Saídas (Figura 5)	**Subsequência** (Figura 5)
Compliance Implementada Aprovada (PI.E5)	Processo Monitorizar (PM)
Compliance Implementada Não Aprovada (PI.E6)	Actividade Implementar a Solução de *Compliance* (PI.3) do processo Implementar (PI)

Tabela 10 - Aferir a Efectividade da Solução de *Compliance* (PI.4), do processo Implementar (PI).

[45] Como (i) indicado pelo ISACA através do processo COBIT 4.1- ME3 (ITGI, 2007) ((ME3-2) - Secção 2.3.1); (ii) referido pelos seguintes autores citados: Ho (HO, 2009) ((H8) - Secção 2.2.1) e Dameri (DAMERI, 2009) ((D4) - Secção 2.2.2); e (iii) e no contexto do apresentado na Secção 2.4 sobre a implementação das medidas e controlos.

4.2.6 Métricas e Indicadores do Processo (PI)

A tabela 11 apresenta a Métrica e o Indicador do processo Implementar (PI), tendo como referência as métricas exemplificativas[46] indicadas pelo ISACA, através do processo COBIT 4.1-ME3 (ITGI, 2007). Os períodos actuais e anteriores apresentados na tabela 11 deverão ser definidos pela Organização.

ID	Objectivos	Indicadores	Métricas
M4	Reduzir o número de deficiências detectadas na implementação da Solução de *Compliance*.	I_{M4} = Índice do número de deficiências detectadas na implementação da Solução de *Compliance* no período. Fórmula $I_{M4} = B_{M4} / A_{M4} \times 100$	A_{M4} = Número de deficiências detectadas na implementação da Solução de *Compliance,* no período anterior; B_{M4} = Número de deficiências detectadas na implementação da Solução de *Compliance,* no período atual.

Tabela 11 - Métricas e Indicadores do processo Implementar (PI).

[46] A métrica exemplificativas indicadas pelo ISACA é: (iv) Quantidade de não-conformidades críticas identificadas por ano; (iii) Dias de formação por colaborador dos SI/TIC por ano relacionado a *Compliance*. Para maior detalhe sobre as métricas do processo COBIT4.1: ME3 consultar o Anexo - Relacionamento entre Objectivos e Métricas do processo COBIT 4.1: ME3.

4.3 Caracterização do processo: Monitorizar (PM)

A tabela 12 apresenta a caracterização do processo: Monitorizar (PM).

<table>
<tr><th colspan="2">Objectivo</th></tr>
<tr><td colspan="2">Este processo tem como objectivo assegurar a recolha dos dados e a elaboração de relatórios do estado da efectividade da Compliance dos SI/TIC (Secção 2.2, Secção 2.3).</td></tr>
<tr><th>Entradas (Figura 6)</th><th>Procedência (Figura 6)</th></tr>
<tr><td>Compliance Implementada Aprovada (PI.E5)</td><td>Processo Implementar (PI)</td></tr>
<tr><th colspan="2">Descrição</th></tr>
<tr><td colspan="2">O processo Monitorizar (PM) é composto por três actividades:
• Monitorizar a Compliance (PM.1)
• Acompanhar as Auditorias de Compliance (PM.2)
• Avaliar a Compliance dos Fornecedores (PM.3)
Deverá ser usada uma ferramenta de suporte à Gestão da Compliance dos SI/TIC (Secção 2.2.1 e Secção 2.3.1), para o registo e consulta da informação que a Organização entender adequada.</td></tr>
<tr><th colspan="2">Intervenientes</th></tr>
<tr><td colspan="2">O ISACA através do processo COBIT 4.1-ME3 (ITGI, 2007) e o BIS (BIS, 2005), propõem os seguintes intervenientes:
• Função Compliance dos SI/TIC e a Função Compliance da Organização.
• Domínio Organizacional pelo Responsável do Processo de Negócio.
• Domínio Tecnológico pelo Responsável pelas Operações e Responsável pela Administração dos SI/TIC, áreas de Risco e Segurança.</td></tr>
<tr><th>Saídas (Figura 6)</th><th>Subsequência (Figura 6)</th></tr>
<tr><td>Monitorização da Compliance dos SI/TIC Concluída (PM.E1)</td><td rowspan="3">Processo Reportar (PR)</td></tr>
<tr><td>Auditoria da Compliance dos SI/TIC Concluída (PM.E2)</td></tr>
<tr><td>Avaliação dos Fornecedores de Serviços Externos de SI/TIC Concluída (PM.E3)</td></tr>
</table>

Tabela 12 - Caracterização do processo: Monitorizar (PM)

4.3.1 Modelação do Processo (PM)

A figura 6 apresenta a modelação do processo Monitorizar (PM), que contempla as suas actividades, eventos de entrada e saída, e as interfaces com outros processos da *Framework* para a Gestão da *Compliance* nos SI/TIC (Figura 3).

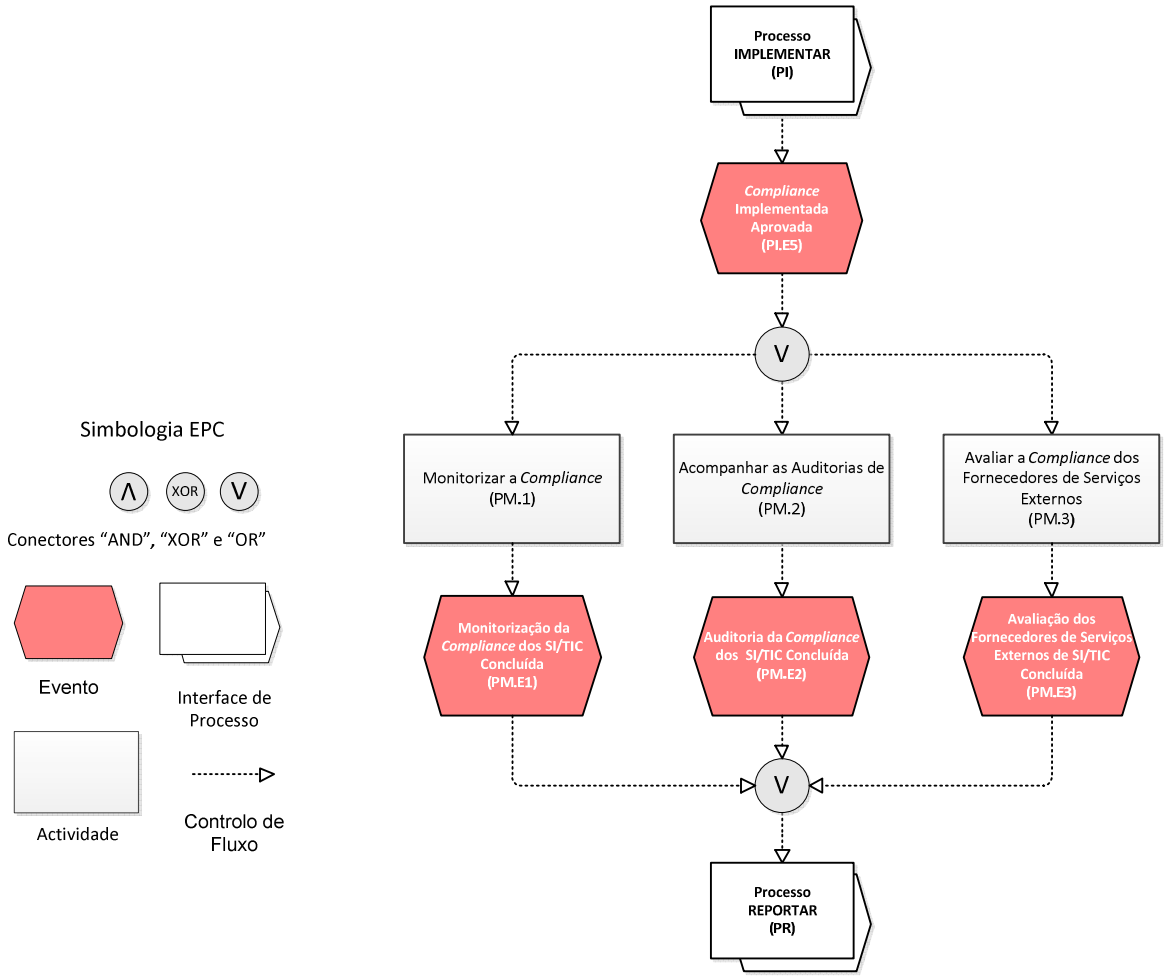

Figura 6 – Modelo EPC do processo Monitorizar (PM).

4.3.2 Actividade: Monitorizar a *Compliance* (PM.1)

A tabela 13 apresenta a proposta de solução para a actividade: Monitorizar a *Compliance* (PM.1), do processo Monitorizar (PM).

Proposta de Solução Alternativa	
O objectivo desta actividade é a monitorização da *Compliance* nos SI/TIC[47].	
Entradas (Figura 6)	**Procedência** (Figura 6)
Compliance Implementada Aprovada (PI.E5)	Processo Implementar (PI)
Descrição	
Nesta actividade com base nos Controlos e nos Mecanismos de Monitorização da *Compliance* nos SI/TIC implementados e aprovados (PI.E5) e após a sua operacionalização deverá ocorrer para cada ciclo de Monitorização: • A identificação dos objectivos e o âmbito para assegurar de forma continuada da efectividade da *Compliance* dos SI/TIC, ou seja que os controlos continuam a operar conforme foram concebidos e implementados. • Recolha de dados da Monitorização. • Elaboração, comunicação do Relatório de Monitorização da *Compliance* dos SI/TIC (PM.E1) e subsequente aprovação pela Gestão.	
Intervenientes e Atribuição de Responsabilidades	
• A realização deverá ser assegurada pelo Responsável pelas Operações e pela Função *Compliance* dos SI/TIC. • O acompanhamento deverá ser assegurado pelo Responsável pela Administração dos SI/TIC, áreas de Risco e Segurança. Sempre que se aplique deverá ser acompanhada pela Função *Compliance* da Organização.	
Saídas (Figura 6)	**Subsequência** (Figura 6)
Monitorização da *Compliance* dos SI/TIC Concluída (PM.E1)	Processo Reportar (PR)

Tabela 13 - Monitorizar a *Compliance* (PM.1), do processo Monitorizar (PM).

[47] Como (i) indicado pelo ISACA através do processo COBIT 4.1- ME3 (ITGI, 2007) ((ME3-3) - Secção 2.3.1); (ii) pelo COSO (COSO, 1994) e COSO-ERM (COSO, 2007) através dos seus componentes, Ambiente de Controlo, Monitorização (Secção 2.3.2); e (iii) referido pelos seguintes autores citados: Ho (HO, 2009) ((H7) - Secção 2.2.1), Dameri (DAMERI, 2009) ((D4) - Secção 2.2.2), e Annaswamy (ANNASWAMY, 2009) ((A) - Secção 2.2.3), Bace e Rozwell (BACE e ROZWELL, 2006) (B3) - Secção 2.2.4).

4.3.3 Actividade: Acompanhar as Auditorias de *Compliance* (PM.2)

A tabela 14 apresenta a proposta de solução para a actividade: Acompanhar as Auditorias de *Compliance* (PM.2), do processo Monitorizar (PM).

Proposta de Solução Alternativa	
O objectivo desta actividade é o acompanhamento das auditorias da *Compliance* nos SI/TIC, quer a auditoria seja parcelar ou global[48].	
Entradas (Figura 6)	**Procedência** (Figura 6)
Compliance Implementada Aprovada (PI.E5)	Processo Implementar (PI)
Descrição	
Nesta actividade com base nos Controlos e nos Mecanismos de Monitorização da *Compliance* nos SI/TIC, na aprovação da Implementação da *Compliance* (PI.E5) e após a sua operacionalização deverá ocorrer para cada auditoria: • A identificação dos objectivos e o âmbito, bem como o plano para aferir de forma independente a efectividade dos controlos e da solidez global da *Compliance* nos SI/TIC. • Acompanhamento dos auditores internos e/ou externos para que seja disponibilizada toda a informação necessária para a realização da auditoria.	
Intervenientes e Atribuição de Responsabilidades	
• A realização deverá ser assegurada pelos Auditores internos ou externos à Organização. • O acompanhamento deverá ser assegurado pela Função *Compliance* dos SI/TIC. Sempre que se aplique deverá ser acompanhada pela Função *Compliance* da Organização, pelo Responsável pelas Operações, áreas de Risco e Segurança.	
Saídas (Figura 6)	**Subsequência** (Figura 6)
Auditoria da *Compliance* dos SI/TIC Concluída (PM.E2)	Processo Reportar (PR)

Tabela 14 - Acompanhar as Auditorias de *Compliance* (PM.2), do processo Monitorizar (PM).

[48] Como (i) indicado pelo ISACA através do processo COBIT 4.1- ME3 (ITGI, 2007) ((ME3-3) - Secção 2.3.1); (ii) pelo COSO (COSO, 1994) e COSO-ERM (COSO, 2007) através dos seus componentes, Ambiente de Controlo, Monitorização (Secção 2.3.2); e (iii) referido pelos seguintes autores citados: Ho (HO, 2009) ((H7) - Secção 2.2.1), Dameri (DAMERI, 2009) ((D4) - Secção 2.2.2), Annaswamy (ANNASWAMY, 2009) ((A) - Secção 2.2.3), e Bace e Rozwell (BACE e ROZWELL, 2006) (B3) - Secção 2.2.4).

4.3.4 Actividade: Avaliar a *Compliance* dos Fornecedores de Serviços Externos (PM.3)

A tabela 15 apresenta a proposta de solução para a actividade: Avaliar a Compliance dos Fornecedores de Serviços Externos (PM.3), do processo Monitorizar (PM).

Proposta de Solução Alternativa	
O objectivo desta actividade é o de avaliar que os serviços prestados pelos Fornecedores de Serviços Externos de SI/TIC da Organização cumprem com os Requisitos de Conformidade que a Organização considere obrigatórios[49].	
Entradas (Figura 6)	**Procedência** (Figura 6)
Compliance Implementada Aprovada (PI.E5)	Processo Implementar (PI)
Descrição	
Nesta actividade, com base nos Controlos e nos Mecanismos de Monitorização da *Compliance* nos SI/TIC da Organização relacionados com os serviços prestados pelos Fornecedores de Serviços Externos de SI/TIC, na aprovação da Implementação da *Compliance* (PI.E5) e após a sua operacionalização deverá ocorrer: • Para cada avaliação, a identificação dos objectivos e do âmbito da avaliação do Fornecedor de Serviços Externos de SI/TIC da Organização em matérias de *Compliance.* A periodicidade deverá ser definida pela Organização. • Realização da Avaliação, através da análise das cláusulas contractuais do Fornecedor de Serviços Externos de SI/TIC com as exigências de *Compliance* da Organização. • Elaboração, comunicação do Relatório de Avaliação dos Fornecedores de Serviços Externos de SI/TIC (PM.E3) e subsequente aprovação pela Gestão.	
Intervenientes e Atribuição de Responsabilidades	
• A realização deverá ser assegurada pela Função *Compliance* dos SI/TIC e pelos Fornecedores de Serviços Externos de SI/TIC da Organização. • Sempre que se aplique deverá ser acompanhada pela Função *Compliance* da Organização, pelo Responsável pelas Operações, áreas de Risco e Segurança, e Responsável pela Administração dos SI/TIC.	

[49] Como (i) indicado pelo ISACA através do processo COBIT 4.1- ME3 (ITGI, 2007) ((ME3-3) - Secção 2.3.1); (ii) pelo COSO (COSO, 1994) e COSO-ERM (COSO, 2007) através dos seus componentes, Ambiente de Controlo, Monitorização (Secção 2.3.2); e (iii) referido pelos seguintes autores citados: Ho (HO, 2009) ((H7) - Secção 2.2.1), Dameri (DAMERI, 2009) ((D4) - Secção 2.2.2), Annaswamy (ANNASWAMY, 2009) ((A) - Secção 2.2.3), e Bace e Rozwell (BACE e ROZWELL, 2006) (B3) - Secção 2.2.4).

Saídas (Figura 6)	**Subsequência** (Figura 6)
Avaliação dos Fornecedores de Serviços Externos de SI/TIC Concluída (PM.E3)	Processo Reportar (PR)

Tabela 15 - Avaliar a *Compliance* dos Fornecedores de Serviços Externos (PM.3), do processo Monitorizar (PM).

4.3.5 Métricas e Indicadores do Processo (PM)

A tabela 16 apresenta as Métricas e os Indicadores do processo Monitorizar (PM), tendo como referência as métricas exemplificativas[50] indicadas pelo ISACA, através do processo COBIT 4.1-ME3 (ITGI, 2007). Os períodos actuais e anteriores apresentados na tabela 16 deverão ser definidos pela Organização.

ID	Objectivos	Indicadores	Métricas
M5	Aumentar o número de Requisitos de Conformidade Monitorizados.	I_{M5} = Índice do número de Requisitos de Conformidade Monitorizados; $I_{M5} = \sum B_{M5} / \sum A_{M5} \times 100$	A_{M5} = Número de Requisitos de Conformidade Monitorizados no período anterior; B_{M5} = Número de Requisitos de Conformidade Monitorizados no período atual.
M6	Aumentar o número de Requisitos de Conformidade Avaliados.	IM6 = Índice do número de Requisitos de Conformidade Avaliados; $IM6 = \sum BM6 / \sum AM6 \times 100$	AM6 = Número de Requisitos de Conformidade Avaliados no período anterior; BM6 = Número de Requisitos de Conformidade Avaliados no período atual.
M7	Aumentar o número de Requisitos de Conformidade Auditados.	I_{M7} = Índice do número de Requisitos de Conformidade Auditados; $I_{M7} = \sum B_{M7} / \sum A_{M7} \times 100$	A_{M7} = Número de Requisitos de Conformidade Auditados no período anterior; B_{M7} = Número de Requisitos de Conformidade Auditados no período atual.

Tabela 16 - Métricas e Indicadores do processo Monitorizar (PM).

[50] As métricas exemplificativas indicadas pelo ISACA são: (i) Frequência de revisões da *Compliance*; (ii) Quantidade de não-conformidades reportadas à Gestão de Topo ou causando exposição ou embaraço público**.** O foco destas métricas é o de aumentar o número de recomendações de melhoria. Para maior detalhe sobre as métricas do processo COBIT4.1: ME3 consultar o Anexo - Relacionamento entre Objectivos e Métricas do processo COBIT 4.1: ME3.

4.4 Caracterização do processo: Reportar (PR)

A tabela 17 apresenta a caracterização do processo: Reportar (PR).

<table>
<tr><th colspan="2">Objectivo</th></tr>
<tr><td colspan="2">Este processo tem como objectivo assegurar a análise dos dados da monitorização, auditorias e avaliações do estado da efectividade da Compliance dos SI/TIC (Secção 2.2, Secção 2.3). O resultado da análise deverá ser disponibilizado às partes interessadas quer sejam internas ou externas à Organização.</td></tr>
<tr><th>Entradas (Figura 7)</th><th>Procedência (Figura 7)</th></tr>
<tr><td>Monitorização da Compliance dos SI/TIC Concluída (PM.E1)</td><td rowspan="3">Processo Monitorizar (PM)</td></tr>
<tr><td>Auditoria da Compliance dos SI/TIC Concluída (PM.E2)</td></tr>
<tr><td>Avaliação dos Fornecedores de Serviços Externos de SI/TIC Concluída (PM.E3)</td></tr>
<tr><th colspan="2">Descrição</th></tr>
<tr><td colspan="2">O processo Reportar (PR) é composto por duas actividades:
• Analisar Estado da Compliance (PR.1)
• Reporte Integrado da Compliance da Organização (PR.2)
Deverá ser usada uma ferramenta de suporte à Gestão da Compliance dos SI/TIC (Secção 2.2.1 e Secção 2.3.1), para o registo e consulta da informação que a Organização entender adequada.</td></tr>
<tr><th colspan="2">Intervenientes</th></tr>
<tr><td colspan="2">O ISACA através do processo COBIT 4.1-ME3 (ITGI, 2007) e o BIS (BIS, 2005), propõem os seguintes intervenientes:
• Função Compliance dos SI/TIC e a Função Compliance da Organização.
• Domínio Organizacional pelo Responsável do Processo de Negócio.
• Domínio Tecnológico através do Responsável pelas Operações e Responsável pela Administração dos SI/TIC, áreas de Risco e Segurança.</td></tr>
<tr><th>Saídas (Figura 7)</th><th>Subsequência (Figura 7)</th></tr>
<tr><td>Estado da Compliance dos SI/TIC integrado nos Relatórios da Organização (PR.E2)</td><td>FIM</td></tr>
<tr><td>Recomendações da Monitorização da Compliance dos SI/TIC (PR.E3)</td><td>Processo Analisar (PA)</td></tr>
</table>

Tabela 17 - Caracterização do processo: Reportar (PR)

4.4.1 Modelação do Processo (PR)

A figura 7 apresenta a modelação do processo Reportar (PR), que contempla as suas actividades, eventos de entrada e saída, e as interfaces com outros processos da *Framework* para a Gestão da *Compliance* nos SI/TIC (Figura 3).

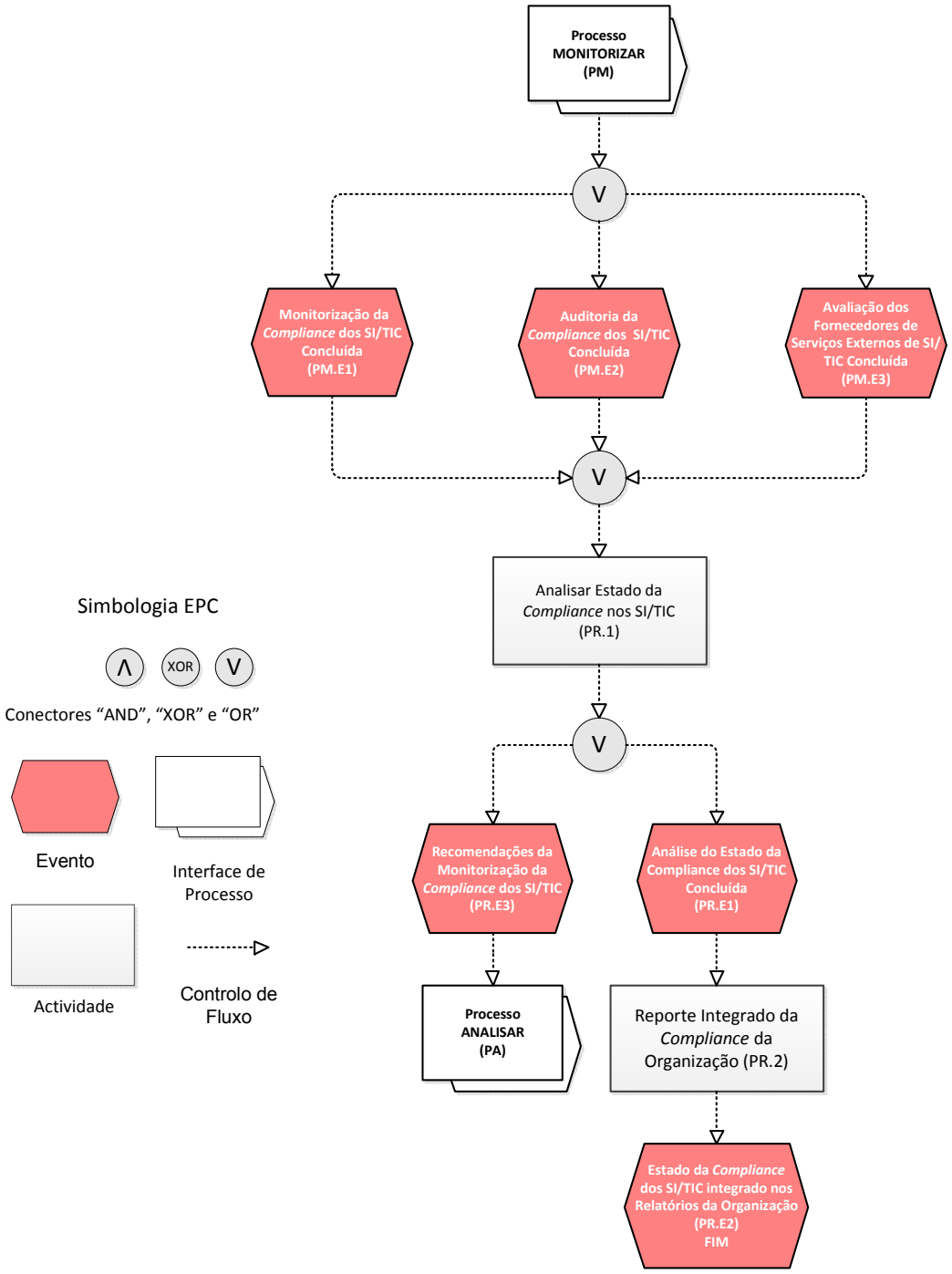

Figura 7 – Modelo EPC do processo Reportar (PR).

4.4.2 Actividade: Analisar Estado da *Compliance* (PR.1)

A tabela 18 apresenta a proposta de solução para a actividade: Analisar Estado da *Compliance* (PR.1), do processo Reportar (PR).

<table>
<tr><th colspan="3">Proposta de Solução Alternativa</th></tr>
<tr><td colspan="3">O objectivo desta actividade é o de analisar o estado da Compliance nos SI/TIC[51].</td></tr>
<tr><td colspan="2">Entradas (Figura 7)</td><td>Procedência (Figura 7)</td></tr>
<tr><td colspan="2">Monitorização da Compliance dos SI/TIC Concluída (PM.E1)</td><td rowspan="3">Processo Monitorizar (PM)</td></tr>
<tr><td colspan="2">Auditoria da Compliance dos SI/TIC Concluída (PM.E2)</td></tr>
<tr><td colspan="2">Avaliação dos Fornecedores de Serviços Externos de SI/TIC Concluída (PM.E3)</td></tr>
<tr><th colspan="3">Descrição</th></tr>
<tr><td colspan="3">Nesta actividade com base no Relatório de Monitorização da Compliance dos SI/TIC (PM.E1), Relatório de Auditoria da Compliance dos SI/TIC (PM.E2) e Relatório de Avaliação dos Fornecedores de Serviços Externos de SI/TIC (PM.E3) deverá ocorrer:
• Analisar e consolidar os dados e informação dos relatórios.
• Caso se aplique, elaboração do relatório de Recomendações da Monitorização da Compliance dos SI/TIC, resultantes das deficiências e melhorias identificadas.
• Aprovação pela Gestão e garantir que as deficiências e melhorias são comunicadas (PR.E3).
• Elaboração, com periodicidade a definir pela Organização, do relatório da Análise do Estado da Compliance dos SI/TIC (PM.E1) que deverá ser constituído pela consolidação da informação sobre o estado da Compliance nos SI/TIC.</td></tr>
<tr><th colspan="3">Intervenientes e Atribuição de Responsabilidades</th></tr>
<tr><td colspan="3">• A realização deverá ser assegurada pela Função Compliance dos SI/TIC.
• O acompanhamento deverá ser assegurado pela Função Compliance da Organização. Sempre que se aplique deverá ser acompanhada pelo Responsável do Processo de Negócio, Responsável pelas Operações e Responsável pela Administração dos SI/TIC, áreas de Risco e Segurança.</td></tr>
<tr><td colspan="2">Saídas (Figura 7)</td><td>Subsequência (Figura 7)</td></tr>
<tr><td colspan="2">Análise do Estado da Compliance dos SI/TIC Concluída (PR.E1)</td><td>Actividade Reporte Integrado da Compliance da Organização (PR.2) do processo Reportar (PR)</td></tr>
<tr><td colspan="2">Recomendações da Monitorização da Compliance dos SI/TIC (PR.E3)</td><td>Processo Analisar (PA)</td></tr>
</table>

Tabela 18 - Analisar Estado da *Compliance* (PR.1), do processo Reportar (PR).

[51] Como (i) indicado pelo ISACA através do processo COBIT 4.1- ME3 (ITGI, 2007) ((ME3-4) - Secção 2.3.1); e (ii) referido pelos seguintes autores citados: Ho (HO, 2009) ((H7) e (H8) - Secção 2.2.1), Dameri (DAMERI, 2009) ((D4) - Secção 2.2.2), Annaswamy (ANNASWAMY, 2009) ((A) - Secção 2.2.3), e Bace e Rozwell (BACE e ROZWELL, 2006) (B3) - Secção 2.2.4).

4.4.3 Actividade: Reporte Integrado da *Compliance* da Organização (PR.2)

A tabela 19 apresenta a proposta de solução para a actividade: Reporte Integrado da *Compliance* da Organização (PR.2), do processo Reportar (PR).

Proposta de Solução Alternativa	
O objectivo desta actividade é o de integrar nos relatórios semelhantes de outras funções da Organização o estado da *Compliance* dos SI/TIC[52].	
Entradas (Figura 7)	**Procedência** (Figura 7)
Análise do Estado da *Compliance* dos SI/TIC Concluída (PR.E1)	Actividade Analisar Estado da *Compliance* (PR.1) do processo Reportar (PR)
Descrição	
Nesta actividade com base no(s) relatório(s) da Análise do Estado da *Compliance* dos SI/TIC (PR.E1) deverá ocorrer: • Compilação de toda a informação sobre o estado da *Compliance* dos SI/TIC com base no(s) relatório(s) da Análise do Estado da *Compliance* dos SI/TIC (PR.E1), e subsequente aprovação pela Gestão. • Comunicação às partes interessadas de acordo com a periodicidade definida pela Organização. • Integração do estado da *Compliance* dos SI/TIC nos relatórios semelhantes da Organização.	
Intervenientes e Atribuição de Responsabilidades	
• A realização deverá ser assegurada pela Função *Compliance* dos SI/TIC. • O acompanhamento deverá ser assegurado pela Função *Compliance* da Organização. Sempre que se aplique deverá ser acompanhada pelo Responsável do Processo de Negócio, Responsável pelas Operações e Responsável pela Administração dos SI/TIC, áreas de Risco e Segurança.	
Saídas (Figura 7)	**Subsequência** (Figura 7)
Estado da *Compliance* dos SI/TIC integrado nos Relatórios da Organização (PR.E2)	FIM

Tabela 19 - Reporte Integrado da *Compliance* da Organização (PR.2), do processo Reportar (PR).

[52] Como (i) indicado pelo ISACA através do processo COBIT 4.1- ME3 (ITGI, 2007) ((ME3-4) - Secção 2.3.1); (ii) pelo COSO (COSO, 1994) e COSO-ERM (COSO, 2007) através do seu componente Informação e Comunicação (Secção 2.3.2); e (iii) referido pelos seguintes autores citados: Ho (HO, 2009) ((H7) - Secção 2.2.1), Dameri (DAMERI, 2009) ((D5) - Secção 2.2.2), Bace e Rozwell (BACE e ROZWELL, 2006) (B4) - Secção 2.2.4).

4.4.4 Métricas e Indicadores do Processo (PR)

A tabela 20 apresenta as Métricas e os Indicadores do processo Reportar (PM), tendo como referencia as métricas exemplificativas indicadas pelo ISACA, através do processo COBIT 4.1-ME3 (ITGI, 2007).

ID	Objectivos	Indicadores	Métricas
M8	Diminuir os custos anuais associados a multas e penalidades.	I_{M8} = Índice dos custos associados a multas e penalidades no periodo. Fórmula $I_{M8} = B_{M8} / A_{M8} \times 100$	A_{M8} = Custos associados a multas e penalidades, no ano anterior; B_{M8} = Custos associados a multas e penalidades no ano atual.
M9	Aumentar o número de Controlos de Compliance dos SI/TIC analisados e reportados.	IM9 = Índice do número de Controlos de Compliance dos SI/TIC analisados e reportados no período. Fórmula IM9 = B M9 / A M9 x 100	AM9 = Número de Controlos de Compliance dos SI/TIC analisados e reportados no período anterior; AM9 = Número de Controlos de Compliance dos SI/TIC analisados e reportados no período atual.

Tabela 20 - Métricas e Indicadores do processo Reportar (PR).

4.5 Conclusão do desenvolvimento da *Framework*

A sistematização e normalização das várias actividades para a gestão da *Compliance* nos SI/TIC numa *framework* têm como pretensão obter os seguintes benefícios:

- (B1) Agilizar o alinhamento estratégico[53] entre SI/TIC e o negócio em matérias de *Compliance*.
- (B2) Aumentar a eficiência e eficácia através da formalização e sistematização dos processos de suporte à Gestão da *Compliance*.
- (B3) Reduzir a complexidade na Gestão da *Compliance* nos SI/TIC.
- (B4) Aumentar a eficácia na tomada de decisão através da integração, na Proposta de Solução *Compliance*, da análise qualitativa e quantitativa das necessidades para assegurar as exigências dos Requisitos de Conformidade.
- (B5) Acompanhar de forma mais eficaz e eficiente o ciclo de vida das adequações (medidas e Controlos de *Compliance*) tecnológicas e organizacionais necessárias para assegurar a *Compliance* dos Serviços de SI/TIC.
- (B6) Melhorar a qualidade dos Serviços de SI/TIC prestados, pela inclusão de procedimentos orientados à *Compliance*.
- (B7) Efectivar a monitorização e reporte integrado sobre a *Compliance* dos Serviços de SI/TIC.

[53] Alinhamento Estratégico – tem a pretensão de assegurar o inter-relacionamento entre o negócio os SI/TIC, sendo necessário alinhar os planos estratégicos dos SI/TIC com os planos estratégicos do negócio (ITGI, 2007).

5 O Estudo de Caso

Neste capítulo apresenta-se o estudo de caso realizado numa Entidade Gestora dos SI/TIC do BANCO (daqui por diante identificada como ENTIDADE), que presta serviços a um dos maiores grupos do Sector Financeiro Português (daqui por diante identificado como BANCO).

O estudo de caso foi iniciado com uma auditoria à gestão dos Requisitos de Conformidade tendo como finalidade a produção de um relatório de diagnóstico da situação inicial e recomendações. Após a implementação da *Framework para a Gestão da Compliance nos SI/TIC* foi realizada outra auditoria com a finalidade de aferir qual a contribuição da *framework* desenvolvida para a melhoria esperada. O resultado desta auditoria traduziu-se em novo relatório de diagnóstico e recomendações da situação após implementação da framework.

5.1 Apresentação da Entidade

A ENTIDADE presta serviços de SI/TIC ao BANCO desenvolvendo a sua actividade em serviços de concepção, desenvolvimento e exploração dos SI/TIC. A estrutura organizacional desta entidade encontra-se dividida em direcções tecnológicas e não tecnológicas. As direcções tecnológicas focam a sua actividade na gestão da procura, nos projectos, na manutenção e operação das aplicações. As direcções não tecnológicas focam a sua actividade na gestão de serviço, nos processos, risco, segurança, qualidade, no planeamento e gestão de recursos humanos.

5.1.1 A Função *Compliance* dos SI/TIC

A Função *Compliance* dos SI/TIC (Secção 2.1.3) encontra-se integrada nas direcções não tecnológicas, tendo como função assegurar a *Compliance* nos SI/TIC. Esta função encontra-se dependente não hierarquicamente da Função *Compliance* do BANCO, sendo esta a responsável por desenvolver e implementar a estratégia, princípios e políticas de gestão de Risco de *Compliance*, reportando, no âmbito deste risco, ao respectivo Administrador do BANCO. A Função *Compliance* do Grupo criou mesmo um regulamento no qual definiu através de uma norma interna o Risco de *Compliance*[54] no BANCO.

A Função de *Compliance* dos SI/TIC tem como objectivos: (1) identificar os Requisitos de Conformidade que condicionam potencialmente as suas actividades e as aplicações; (2) colaborar com a Função *Compliance* do Grupo, na gestão da *Compliance* dos Serviços de SI/TIC; (3) avaliar e reportar periodicamente o cumprimento dos Requisitos de Conformidade nos Serviços de SI/TIC.

[54] Segundo a Função *Compliance* do BANCO o Risco de *Compliance* consiste na probabilidade BANCO incorrer em sanções, em resultado do não cumprimento dos Requisitos de Conformidade. A gestão do Risco de *Compliance* é uma responsabilidade de todos os órgãos de estrutura do BANCO e das Entidades do Grupo do BANCO, devendo em todos os momentos e todas as circunstâncias serem observadas as exigências dos Requisitos de Conformidade. A gestão inadequada do Risco de *Compliance* e o consequente impacto de acções tomadas pelos colaboradores, fornecedores e outras entidades pode resultar em prejuízos financeiros ou de ordem reputacional para o BANCO.

A gestão da *Compliance* na ENTIDADE efectua-se através de três pilares independentes mas relacionados – as funções de *Compliance*, o Sistema da Qualidade e o Portfólio de SI/TIC.

5.1.2 O Sistema da Qualidade

As actividades da ENTIDADE estão especificadas no Catálogo de Processos de Trabalho[55] e Referenciais da Qualidade, dando corpo ao Sistema de Gestão da Qualidade. Como Referenciais de Qualidade são considerados as Políticas, Normas, Guias, Procedimentos, Controlos e Metodologias.
Na ENTIDADE, a função Coordenador é atribuída à pessoa responsável por um ou mais Processos de Trabalho e dos Referenciais da Qualidade associados. O objectivo dos Processos de Trabalho é a especificação das actividades, dos seus intervenientes, bem como a identificação dos seus riscos e dos controlos (Secção 2.4.). Os Processos de Trabalho encontram-se mapeados com os processos do COBIT 4.1 (ITGI, 2007). Este mapeamento tem dois objectivos distintos mas relacionados. O primeiro objectivo é o de facilitar a identificação das boas práticas dos processos do COBIT 4.1 (ITGI, 2007) que possam orientar na estratégia de melhoria contínua dos Processos de Trabalho. As acções de melhoria identificadas são registadas no Catálogo de Melhorias. O segundo objectivo é facilitar a avaliação do nível de maturidade dos processos na ENTIDADE com o objectivo de identificar as melhorias necessárias para incrementar a sua maturidade.

5.1.3 O Portfólio de SI/TIC

No contexto do estudo de caso o Portfólio de SI/TIC é composto pelo Catálogo de Pedidos e o Catálogo Aplicacional. No Catálogo de Pedidos encontram-se identificados todos os pedidos passiveis de serem efectuados pelas direcções do BANCO à ENTIDADE. Este catálogo é gerido pelos Gestores da Procura, função que faz a ligação dos SI/TIC com as Direcções do BANCO. No Catálogo Aplicacional, as aplicações são caracterizadas quanto aos custos de implementação, manutenção e operação, à sua capacidade de evolução, à adequação tecnológica, e ao seu grau de criticidade para o Negócio. As aplicações encontram-se mapeadas com os Processos de Negócio do BANCO e com os Processos de Trabalho da ENTIDADE. Este catálogo é gerido pelos Gestores de Aplicação quando se trata de aplicações em manutenção/operação, ou Gestores de Projecto quando se trata de aplicações novas.

5.2 Auditoria à Situação Inicial

A auditoria à situação inicial da gestão dos Requisitos de Conformidade na ENTIDADE ocorreu antes da implementação da Framework para a Gestão da *Compliance* dos SI/TIC. A auditoria foi realizada através de entrevistas aos responsáveis pela Função *Compliance* dos SI/TIC, de forma a preencher um questionário baseado no documento do ITIG[56] o "*COBIT 4.1 Control Objectives for Information and related Technology*" (ITIG, 2007), e tendo como referência o modelo de maturidade proposto pelo ISACA no processo COBIT 4.1 - ME3 (ITGI, 2007) (Secção 2.3.1). Esta auditoria teve como objectivo

[55] Os Processos de Trabalho destinam-se a uniformizar, determinando como o trabalho é realizado na ENTIDADE sendo um pré-requisito essencial para analisar a eficiência operacional na ENTIDADE e auxiliar na identificação de funções redundantes.
[56] O ITIG (IT Governance Institute) disponibiliza mesmo um ficheiro de excel para o devido efeito em www.isaca.org.

sensibilizar e influenciar a Gestão da ENTIDADE para que esta promovesse um conjunto de iniciativas que mitigassem as lacunas identificadas e como consequência incrementasse o nível de maturidade da organização quanto à *Compliance* dos SI/TIC. O resultado da auditoria, após análise das respostas ao questionário, materializou-se num relatório, constituído por um conjunto de constatações e recomendações, apresentadas estas na tabela 21, e pelo cálculo do nível de maturidade[57] do processo COBIT 4.1 - ME3 (ITGI, 2007) (Secção 2.3.1) cujo resultado indicou o valor de "2,21"[58].

Neste contexto a Gestão da ENTIDADE promoveu reuniões de trabalho com os vários interlocutores das direcções tecnológicas e não tecnológicas, com o objectivo de aplicar a *Framework* para a Gestão da *Compliance* dos SI/TIC desenvolvida e para identificar um Requisito de Conformidade para a implementação do estudo de caso.

Recomendação
(Rai.1) Avaliar regularmente se os Requisitos de Conformidade estão a ser seguidos e se ainda dão resposta às causas que os originaram.
(Rai.2) Desenvolver e comunicar processos, procedimentos e metodologias que ajudem a determinar os impactos dos Requisitos de Conformidade e estabelecer/implementar os controlos adequados.
(Rai.3) Avaliar e monitorizar regularmente o ambiente interno de *Compliance* na ENTIDADE e nos Fornecedores de Serviços Externos de SI/TIC.
(Rai.4) Assegurar que as falhas de *Compliance* são tratadas e que são avaliados regularmente os padrões recorrentes dessas falhas.
(Rai.5) Promover o alinhamento entre os relatórios do estado de *Compliance* da ENTIDADE com os relatórios do BANCO.
(Rai.6) Promover a realização de acções de comunicação sobre Requisitos de Conformidade que garantam que todos os colaboradores da ENTIDADE a todos os níveis estão cientes das suas obrigações de *Compliance*.
(Rai.7) Implementar um processo sistemático para avaliação dos objectivos e métricas relativas ao processo de Gestão dos Requisitos de Conformidade.

Rai.x ("Rai" de recomendação antes da implementação, e "x" número da recomendação).

Tabela 21 - Recomendações resultantes da auditoria à situação inicial.

[57] Para maior detalhe sobre o modelo de maturidade do ME3 consultar o Anexo - Modelo de Maturidade do processo COBIT 4.1: ME3.

[58] Para maior detalhe sobre a Auditoria à Situação Inicial consultar o Anexo – Estudo de Caso: Auditoria à Situação Inicial.

5.3 Implementação da *Framework* para a Gestão da *Compliance* dos SI/TIC

5.3.1 Requisito de Conformidade do Estudo de Caso

Para o estudo de caso foi considerado o Requisito de Conformidade - Lei nº 36/2010[59] de 2 de Setembro 2010 (nas secções seguintes será identificado como Requisito de Conformidade - Lei nº 36/2010) que entrou em vigor no dia 1 de Março de 2011. Esta lei determinou a criação pelo Banco de Portugal de uma "*base de contas bancárias existentes no Sistema Bancário*" para prestação de informação às autoridades judiciárias, no âmbito de um processo penal.

5.3.2 Criação do Grupo de Trabalho

Para o estudo de caso foi constituído um grupo de trabalho na ENTIDADE e no BANCO.

Na tabela 22 apresenta-se o grupo de trabalho de acordo com o definido na *Framework* para a Gestão da *Compliance* dos SI/TIC.

Função	BANCO	ENTIDADE
Responsável pela Administração	Direcção de Processos e Qualidade	Gestor do Processo de Trabalho e Área de Qualidade
Responsável do Processo de Negócio	Unidade de Negócio (*)	-
Função *Compliance*	Função *Compliance* do BANCO	Função *Compliance* dos SI/TIC
Responsável pelo Desenvolvimento	-	Gestor da Procura e Gestor de Aplicação
Responsável pelas Operações	Unidade de Negócio (*)	Gestor de Aplicação
Risco e Segurança	Direcção de Risco e Segurança	Área de Risco e Segurança

(*) Responsável pela Aplicação de Clientes e pela operacionalização das exigências do requisito.

Tabela 22 - Constituição do Grupo de Trabalho.

A Função *Compliance* dos SI/TIC foi representada pelo autor desta dissertação e especialistas em matérias de *Compliance* de SI/TIC duma consultora nacional.

5.3.3 Preparação do Estudo de Caso

A preparação inicial foi composta por três acções distintas mas relacionadas: (1) a criação dos processos para a gestão da *Compliance*, (2) a criação dos meios de comunicação institucional da *Compliance* dos SI/TIC e (3) a criação do Catálogo da *Compliance* dos SI/TIC. Na execução destas acções estiveram envolvidas a Função *Compliance* dos SI/TIC e especialistas em matérias de *Compliance* de SI/TIC duma consultora nacional, tendo sido envolvidos os vários Gestores de Aplicação relacionados com a preparação do estudo de caso.

[59] Para maior detalhe sobre o Requisito de Confrmidade do estudo de caso consultar o Anexo – Requisito de Conformidade - Lei nº 36/2010.

(1) A primeira acção realizada pela ENTIDADE foi a definição dos processos para a gestão da *Compliance* nos SI/TIC de acordo com o especificado na *Framework* para a Gestão da *Compliance* dos SI/TIC desenvolvida (Secção 4). Após a definição, estes foram integrados no Catálogo de Processos do Sistema da Qualidade da ENTIDADE. Esta acção foi realizada pelo Gestor de Processo de Trabalho - Gestão da *Compliance* nos SI/TIC (responsável pela Função *Compliance* dos SI/TIC), pela área de Qualidade e acompanhada pela Função *Compliance* do BANCO, pela Direcção de Processos e Qualidade e pela Direcção de Risco e Segurança. A definição e implementação dos processos possibilitou a sistematização e normalização das várias actividades, permitindo aos colaboradores e à Gestão, ter uma visão clara dos processos, compreender como o trabalho é realizado e conhecer como é que esses processos são geridos e se encontram integrados com os outros processos da ENTIDADE.

Esta implementação veio dar resposta à recomendação: (Rai.2) (Secção 5.2), porque não existiam processos, procedimentos, e metodologias que permitissem determinar os impactos dos Requisitos de Conformidade e como deviam ser revistos ou implementados os controlos de *Compliance* necessários para lhe dar resposta; (Rai.7) (Secção 5.2) porque não estavam definidos e implementados procedimentos para a verificação e/ou monitorização da aderência aos Requisitos de Conformidade, no contexto dos processos de governo do Negócio e dos SI/TIC e Controlo Interno. Por outro lado alinha-se com os benefícios esperados com a implementação da *framework* – (B2) e (B3) (Secção 4.5), porque permite maior eficiência e redução da complexidade na Gestão da *Compliance* nos SI/TIC.

(2) A segunda acção foi a criação e implementação de meios de comunicação institucional da *Compliance* dos SI/TIC entre o BANCO e a ENTIDADE. Foi criado o Fórum *Compliance* dos SI/TIC com o objectivo de trocar informação sobre matérias de *Compliance* entre a Função *Compliance* dos SI/TIC e a Função *Compliance* do BANCO. Este forúm reune trimestralmente. Complementarmente foi criada na intranet/portal da ENTIDADE uma área especifica para a disponibilização de informação relacionada com matérias de *Compliance*. Esta acção foi realizada pela Função *Compliance* dos SI/TIC e pela Função *Compliance* do BANCO. A criação e implementação destes meios de comunicação institucional permitiram reunir as condições necessárias para a comunicação de matérias de *Compliance* aos colaboradores da ENTIDADE, bem como providenciou um canal de comunicação efectivo e institucional entre a ENTIDADE e o BANCO, mitigando possíveis falhas de informação entre a área responsável do grupo em matérias de *Compliance* e os SI/TIC.

Esta implementação veio dar resposta às recomendações: (Rai.1) (Secção 5.2), porque independentemente de terem sido desenvolvidos, documentados e comunicados os Controlos de *Compliance* para assegurar a aderência aos Requisitos de Conformidade, alguns destes procedimentos não eram seguidos de forma continuada; (Rai.6) (Secção 5.2), porque permite a todos os colaboradores da ENTIDADE a todos os níveis estarem cientes das suas obrigações de *Compliance*. Por outro lado, alinha-se com os benefícios esperados com a implementação da

framework – (B5) e (B7) (Secção 4.5), porque permite por um lado um acompanhamento mais eficaz e eficiente do ciclo de vida das adequações (Medidas e Controlos *Compliance*) e por outro lado agregar a informação necessária para o reporte integrado sobre a *Compliance* dos Serviços de SI/TIC.

(3) A terceira acção foi a criação da estrutura do Catálogo da *Compliance* dos SI/TIC com o objectivo de registar toda a informação resultante das actividades numa ferramenta de suporte à Gestão da *Compliance* dos SI/TIC de acordo com especificado (Secção 4). O catálogo é um ficheiro Excel e agrega a seguinte informação: Identificação do Requisito de Conformidade; Origem; Data de Efectivação; Tópicos Abordados; Medidas; Aplicações Relacionadas; Referênciais de Qualidade Relacionados; Controlos de *Compliance* associados; Estado das Medidas e Controlos associados (Análise/ Aprovação/ Concepção/ Implementação/ Monitorização). Para a recolha de informação complementar foram realizadas alterações ao Catálogo de Pedidos e Catálogo Aplicacional. No Catálogo de Pedidos foi criado um campo no registo dos pedidos, para ser obrigatória a identificação do Requisito de Conformidade associado ao pedido. No Catálogo Aplicacional foram criados os seguintes conceitos de informação agregados a cada aplicação: Caracterização dos Requisitos de Conformidade[60]; Controlos Aplicacionais (onde se incluem os Controlos de *Compliance*). Este catálogo foi sendo actualizado ao longo do estudo de caso, tendo sido comunicado à Gestão da ENTIDADE o estado do tratamento do Requisito de Conformidade - Lei nº 36/2010, no Catálogo da *Compliance* dos SI/TIC. A criação e implementação destes repositórios de informação possibilitam uma visão holística com foco na *Compliance* dos SI/TIC, nomeadamente no tratamento dos Requisitos de Conformidade, alinhando-se deste modo com o benefício esperado com a implementação da *framework* – (B5) (Secção 4.5).

5.3.4 Processo: Analisar (PA)

Identificar e Catalogar Requisitos de Conformidade (PA.1)

A Função *Compliance* do BANCO, após ter conhecimento do Requisito de Conformidade - Lei nº 36/2010 registou um pedido no Catálogo de Pedido, porque este implicava a disponibilização de informação residente nas Aplicações geridas pela ENTIDADE. A Gestão da Procura após identificar um pedido relacionado com um Requisito de Conformidade comunicou-o à Função *Compliance* dos SI/TIC tendo efectuado o seu registo no Catálogo da *Compliance* dos SI/TIC.

Na execução desta actividade foram envolvidas pelo BANCO, a Função *Compliance* do BANCO, e pela ENTIDADE, a Gestão da Procura e a Função *Compliance* dos SI/TIC.

[60] Caracterização: BdP; CMVM; DR (Diário da República); Normativo Interno (onde se inclui requisitos vinculados através de ordens de serviço ou cláusulas contratuais obrigatórias, decididas internamente); Outros (onde poderão ser incluídos requisitos futuros especiais como sustentabilidade; ambiente, entre outros).

A realização desta actividade veio dar resposta à recomendação (Rai.1) (Secção 5.2), e o benefício esperado com a implementação da *framework* – (B2) (Secção 4.5), porque permite aumentar a eficiência na identificação dos Requisitos de Conformidade pela ENTIDADE.

Determinar Âmbito e Objectivos (PA.2)

Ao analisar-se o Requisito de Conformidade - Lei nº 36/2010 surgiram dúvidas quanto aos tipos de contas que deveriam ser consideradas. De modo a colmatar estas dúvidas foram envolvidas a Direcção Jurídica do BANCO e o Banco de Portugal. Após colmatadas as dúvidas, conclui-se a determinação dos objectivos e âmbito do requisito, tendo de seguida sido especificados os Requisitos Aplicacionais (Domínio Tecnológico) que assegurassem as suas exigências. Como a informação a enviar é de acesso restrito e confidencial do BANCO, identificou-se o Processo de Trabalho da ENTIDADE que estivesse relacionado com a segurança da informação. O processo identificado foi o da Gestão da Segurança da Informação[61]. Verificou-se que este processo se encontrava mapeado com o processo COBIT 4.1 - ES5: Garantia de Segurança nos Sistemas[62] (ITGI, 2007). De seguida investigou-se nos Referenciais de Qualidade a existência de uma norma relacionada com a segurança da informação. A norma identificada foi a ISO/IEC 27002 (ISO/IEC 27002, 2005). Neste contexto foram identificadas as boas práticas dos objectivos de controlo e actividades de controlo deste processo COBIT 4.1 - ES5 (ITGI, 2007a), e as boas práticas da ISO/IEC 27002 (Código de Prática para a Segurança da Informação). Estas boas práticas foram transformadas em recomendações para assegurar, no Domínio Organizacional, as exigências do Requisito de Conformidade - Lei nº 36/2010. Na tabela 23 são apresentados os tópicos das recomendações das boas práticas identificadas.

ISO/IEC 27002 (Código de Prática para a Segurança da Informação) (ISO/IEC 27002, 2005)	ISACA: processo COBIT 4.1 - ES5: Garantia de Segurança nos Sistemas (ITGI, 2007b)	Processo de Trabalho
Boas práticas da secção - Gestão de Operações e Comunicações.	Boas práticas dos objectivos de controlo e actividades de controlo.	Gestão da Segurança da Informação.

Tabela 23 - Tópicos das Recomendações das boas práticas (Domínio Organizacional).

Após a determinação dos Requisitos Aplicacionais verificou-se que era necessário implementar um mecanismo de extracção de informação de acordo com as exigências do requisito. Foram determinados os riscos associados à não implementação das exigências do requisito como apresentado na tabela 24.

[61] O Processo de Trabalho: Gestão da Segurança da Informação, visa promover a preservação de qualidade, integridade, confidencialidade, privacidade e acessibilidade da informação do Grupo do BANCO, de acordo com requisitos de negócio, técnicos e de *Compliance*, englobando as actividades de gestão de segurança de informação ao nível de toda a organização.

[62] ES5 - Garantia de Segurança nos Sistemas: Garantir a segurança dos sistemas, mantendo a integridade da informação e da infra-estrutura de processamento, minimizando o impacto das vulnerabilidades e dos incidentes de segurança.

Riscos da não implementação		
Ameaça	**Vulnerabilidade**	**Impacto**
Quebra de Segurança física, lógica.	Falta de protecção nas linhas de comunicação.	Acesso indevido a informação confidencial.
Não implementação do Requisito de Conformidade.	Gestão inadequada de Requisitos de Conformidade.	Penalizações e degradação da imagem pelo incumprimento de Requisito de Conformidade.

Tabela 24 - Riscos da não implementação do Requisito de Conformidade - Lei nº 36/2010.

De seguida foi elaborado um relatório com as exigências do Requisito de Conformidade - Lei nº 36/2010 contendo as recomendações resultantes da análise efectuada aos dois referenciais identificados, bem como a especificação dos Requisitos Aplicacionais.

Na execução desta actividade foram envolvidas pelo BANCO, a Função *Compliance* do BANCO, a Unidade de Negócio, e pela ENTIDADE, a Gestão da Procura e a Função *Compliance* dos SI/TIC, tendo sido acompanhada pela Área de Risco e Segurança.

A realização desta actividade veio dar resposta à recomendação (Rai.2) (Secção 5.2), e dos benefícios esperados com a implementação da *framework* – (B1), (B4) (Secção 4.5), através da análise qualitativa e do alinhamento estratégico entre SI/TIC e o negócio quanto às exigências do Requisito de Conformidade.

Quantificar os Impactos para a *Compliance* (PA.3)

Com base no relatório com as exigências do Requisito de Conformidade - Lei nº 36/2010, foram identificados os impactos nos Domínios Organizacional e Tecnológico. No Domínio Tecnológico foram detalhadas os Requisitos Aplicacionais e os objectivos de Controlo que garantissem a *Compliance.* De seguida foram identificadas as aplicações - Datawarehouse de Clientes (aplicação do BANCO) aplicação para extracção dos dados e o BPNet (Sistema de comunicação electrónica que interliga o Banco de Portugal e a ENTIDADE) como aplicação receptora dos dados. No Domínio Organizacional verificou-se que o Processo de Trabalho: Gestão da Segurança da Informação ainda se encontrava em especificação, existindo no entanto processos informais assente na política[63] de Segurança de Informação do BANCO[64]. Neste contexto as recomendações foram registadas no Catálogo de Melhorias para que em sede de especificação do Processo de Trabalho pudessem ser analisadas e incorporadas, no processo, nos Referenciais de Qualidade relacionados, e nos Controlos de *Compliance.* Após a indicação das medidas e dos Controlos de *Compliance* necessários

[63] Política – declarações de intenção de alto nível da Gestão de uma Organização (ISACA, 2010).

[64] A política de Segurança de Informação do BANCO refere que a segurança de informação visa proteger e salvaguardar a informação e os sistemas de informação de eventos adversos que possam causar impacto significativo para o BANCO, contribuindo para um maior controlo interno e para a redução do risco operacional, reputacional e de *compliance*, enquadrada no domínio de Política de Segurança definido no referencial internacional ISO/IEC 27002 (Código de Prática para a Segurança da Informação) (ISO/IEC 27002, 2005).

para responder às exigências do Requisito de Conformidade - Lei nº 36/2010, foram determinados os custos associados, tendo sido elaborada a Proposta de *Compliance***.** A componente do Domínio Organizacional foi enviada para aprovação pela Gestão da ENTIDADE, tendo esta decidido a incorporação das recomendações na especificação do Processo de Trabalho: Gestão da Segurança da Informação**.** A componente do Domínio Tecnológico foi enviada para aprovação do responsável do BANCO pelo pedido. Esta componente depois de aprovada foi remetida para o Comité de Priorização de pedidos relacionados com os SI/TIC. O pedido foi priorizado para o ciclo seguinte de desenvolvimento, porque os pedidos relacionados com os Requisitos de Conformidade são prioritários em relação aos restantes pedidos. Neste comité estão representadas todas as direcções e administração do BANCO e das direcções e administração da ENTIDADE.

Na execução desta actividade além de estarem envolvidas por parte do BANCO a Função *Compliance* do BANCO, a Unidade de Negócio, e pela ENTIDADE a Gestão da Procura e a Função *Compliance* dos SI/TIC, também foi envolvido o Gestor de Aplicação do Datawarehouse de Clientes. Esta actividade foi acompanhada pela Área de Risco e Segurança e Área de Qualidade da ENTIDADE.

A realização desta actividade veio dar resposta à recomendação (Rai.1) (Secção 5.2), e ao benefício esperado com a implementação da *framework* – (B4) (Secção 4.5), através da quantificação dos impactos na ENTIDADE pretendendo-se deste modo aumentar a eficácia na tomada de decisão sobre o que será necessário implementar para responder às exigências do Requisito de Conformidade.

5.3.5 Processo: Implementar (PI)

Conceber a Solução de *Compliance* (PI.1)

No Domínio Tecnológico os Requisitos Aplicacionais foram detalhados, em Funcionalidades Aplicacionais, e os objectivos de controlo em Controlos de *Compliance* aplicáveis, e mecanismos de monitorização e critérios e necessidades de monitorização dos controlos. Os controlos concebidos pretenderam assegurar que a integridade e a veracidade dos dados ao longo de todo o ciclo de extracção e entrega fossem efectuadas por pessoas qualificadas e autorizadas. A pretensão foi garantir que desde a recolha dos dados e que após verificação, detecção e correcção, fosse entregue ao Banco de Portugal, assegurando por outro lado a protecção e autenticidade da mesma durante a sua transmissão. Os mecanismos de monitorização concebidos estavam relacionados com a prevenção de falha na extracção, detecção e correcção de erros nos dados quer da ENTIDADE quer do Banco de Portugal. A periodicidade da monitorização é mensal, ou seja a cada ocorrência de processamento dos dados. No Domínio Organizacional constatou-se que as recomendações para assegurar as exigências do Requisito de Conformidade - Lei nº 36/2010 estavam a ser incorporadas na especificação do Processo de Trabalho: Gestão da Segurança da Informação.

Na execução desta actividade foram envolvidas pela ENTIDADE, a Gestão da Procura e a Função *Compliance* dos SI/TIC, também foi envolvido o Gestor de Aplicação do Datawarehouse de Clientes. Esta actividade foi acompanhada pela Área de Risco e Segurança e Área de Qualidade da ENTIDADE e por parte do BANCO, pela Função *Compliance* do BANCO e pela Unidade de Negócio.

A realização desta actividade veio dar resposta à recomendação: (Rai.2) (Secção 5.2), e o alinhamento com o benefício esperado com a implementação da *framework* – (B6) (Secção 4.5), porque se pretendem conceber as medidas e os Controlos necessários para responder às exigências dos Requisitos de Conformidade, com o objectivo de melhorar a qualidade dos Serviços de SI/TIC prestados em matérias de *Compliance*.

Validar a Concepção da Solução de *Compliance* (PI.2)

Após a concepção, para mitigar situações relacionadas com possíveis deficiências de concepção e especificação, foram executados testes e realizadas reuniões de forma a assegurar que existe uma ligação entre o controlo e o objectivo de controlo, bem como se encontram assegurados os Requisitos Aplicacionais determinados. O grupo de trabalho foi composto pela Direcção de Processo de Qualidade do Banco, a Função *Compliance* do BANCO, a Função *Compliance* dos SI/TIC e um Gestor da Aplicação. Verificou-se que o mecanismo concebido para a extracção dos dados não era o mais adequado por não devolver toda a informação necessária para remeter ao Banco de Portugal.

Na execução desta actividade estiveram envolvidas por parte da ENTIDADE, a Função *Compliance* dos SI/TIC, a Área de Risco e de Segurança, por parte do BANCO, a Unidade de Negócio. Esta actividade foi acompanhada por parte do BANCO, pela Função *Compliance* do BANCO, e pela ENTIDADE, pelo Gestor de Aplicação do Datawarehouse de Clientes.

A realização desta actividade veio dar resposta à recomendação: (Rai.3) (Secção 5.2), porque permite identificar, e comunicar eventuais desvios quanto às medidas e Controlos a implementar para responder às exigências dos Requisitos de Conformidade. Por outro lado alinha-se com o benefício esperado com a implementação da *framework* – (B7) (Secção 4.5), porque o que é pretendido é que a monitorização seja efectiva.

Implementar a Solução de *Compliance* (PI.3)

Após as devidas correcções deu-se início à implementação das Funcionalidades Aplicacionais concebidas. Por outro lado, verificou-se que a especificação do Processo de Trabalho: Gestão da Segurança da Informação ainda se encontrava em curso. No entanto, as recomendações estavam a ser incorporadas, dando garantias de que o que tinha sido determinado para assegurar as exigências do Requisito de Conformidade - Lei nº 36/2010, ao nível do Domínio Organizacional iria ser alcançado.

Na execução desta actividade estiveram envolvidas por parte da ENTIDADE o Gestor de Aplicação do Datawarehouse de Clientes e o Gestor de Processo de Trabalho e Área de Qualidade. Esta

actividade foi acompanhada por parte da ENTIDADE, pela Função *Compliance* dos SI/TIC e pela Área de Risco e Segurança, por parte do BANCO, pela Unidade de Negócio e pela Função *Compliance* do BANCO.

A realização desta actividade veio dar resposta à recomendação: (Rai.2) (Secção 5.2), e o alinhamento com o benefício esperado com a implementação da *framework* – (B6) (Secção 4.5), porque se pretendem implementar as medidas e os Controlos concebidos e avaliados para responder às exigências dos Requisitos de Conformidade, com o objectivo de melhorar a qualidade dos Serviços de SI/TIC prestados em matérias de *Compliance*.

Aferir a Efectividade da Solução de *Compliance* (PI.4)

Terminada a implementação foram executados os testes pelo grupo de trabalho para aferir se o que foi implementado opera conforme foi concebido e cumpre o objectivo de assegurar as exigências do Requisito de Conformidade - Lei nº 36/2010. No Catálogo Aplicacional foi associado o requisito à Aplicação Datawarehouse de Clientes, bem como os controlos concebidos e relacionados com a *Compliance*. Verificou-se que esta informação é bastante relevante para o futuro, porque em caso de alteração ao requisito, facilmente se identificam as aplicações relacionadas bem como os Controlos de *Compliance*, que asseguravam as anteriores exigências do requisito. Deste modo será mais fácil a identificação das possíveis lacunas. Após a aprovação da implementação, ou seja a verificação da efectividade das Funcionalidades Aplicacionais e dos Controlos de *Compliance* foi actualizado o Catálogo de *Compliance* dos SI/TIC. De seguida, as Funcionalidades Aplicacionais e dos Controlos de *Compliance* ficaram disponíveis para assegurar as exigências do Requisito de Conformidade - Lei nº 36/2010.

Na execução desta actividade estiveram envolvidas por parte da ENTIDADE, a Função *Compliance* dos SI/TIC, a Área de Risco e Segurança, por parte do BANCO, a Unidade de Negócio. Esta actividade foi acompanhada por parte da ENTIDADE, pelo Gestor de Aplicação do Datawarehouse de Clientes e por parte do BANCO, pela Função *Compliance* do BANCO.

A realização desta actividade veio dar resposta à recomendação: (Rai.3) (Secção 5.2), porque permite identificar, e comunicar eventuais desvios quanto às medidas e Controlos implementados para responder às exigências dos Requisitos de Conformidade. Por outro lado, alinha-se com o benefício esperado com a implementação da *framework* – (B7) (Secção 4.5), porque o que é pretendido é que a monitorização seja efectiva.

5.3.6 Processo: Monitorizar (PM)

Monitorizar a *Compliance* (PM.1)

A monitorização é efectuada mensalmente aos Controlos de *Compliance* relacionados com o Requisito de Conformidade - Lei nº 36/2010. O resultado desta monitorização é enviado à Função *Compliance* dos SI/TIC, registando-a de seguida no Catálogo da *Compliance* dos SI/TIC. Verificou-se

que os Controlos de *Compliance* operavam conforme foram concebidos e implementados para assegurar as exigências do requisito. A informação resultante da monitorização foi registada no Catálogo de *Compliance* dos SI/TIC.

Na execução desta actividade estiveram envolvidas por parte da ENTIDADE, o Gestor de Aplicação do Datawarehouse de Clientes e a Função *Compliance* dos SI/TIC. Esta actividade foi acompanhada por parte da ENTIDADE, pela Área de Qualidade e Área de Risco e Segurança, por parte do BANCO, pela Função *Compliance* do BANCO.

A realização desta actividade veio dar resposta à recomendação: (Rai.3) (Secção 5.2), porque não era feita uma avaliação regular à ENTIDADE para assegurar a sua aderência aos Requisitos de Conformidade, não era obtida regularmente, dos colaboradores, a confirmação da *Compliance*, nem existia um processo para monitorizar. Por outro lado alinha-se com o benefício esperado com a implementação da *framework* – (B7) (Secção 4.5), porque o que é pretendido é a efectivação da monitorização.

Acompanhar as Auditorias de *Compliance* (PM.2)

No período que decorreu o estudo de caso não existiu nenhuma auditoria à *Compliance* dos SI/TIC unicamente focada no Requisito de Conformidade - Lei nº 36/2010. No entanto, foi tido em consideração o proposto pela *Framework* para o diagnóstico após a implementação do estudo de caso.

Avaliar a *Compliance* dos Fornecedores de Serviços Externos (PM.3)

Verificou-se que a execução das Funcionalidades Aplicacionais poderia ser efectuada por pessoas dos Fornecedores de Serviços Externos de SI/TIC nas instalações da ENTIDADE. Neste contexto foi determinado pela ENTIDADE a realização de uma avaliação ao contrato do prestador de modo a salvaguardar qualquer tipo de risco relacionado com os dados.
Esta avaliação pretendeu verificar a existência de Controlos Compensatórios e se existia Acordo de Confidencialidade assinado. Verificou-se que constava no contrato a existência de um Controlo Compensatório, ou seja uma indemnização referente a penalizações em que o BANCO possa incorrer, por motivos de *Compliance*, que sejam atribuídas a incumprimentos por parte do Fornecedor de Serviços Externos de SI/TIC. Também se verificou que este prestador também tinha assinado o acordo de confidencialidade, que se aplicava a todos os seus recursos. Como resultado desta avaliação foi elaborado o Relatório de Avaliação dos Fornecedores de Serviços Externos de SI/TIC. A informação resultante da avaliação foi registada no Catálogo de *Compliance* dos SI/TIC.

Na execução desta actividade estiveram envolvidas por parte da ENTIDADE a Função *Compliance* dos SI/TIC, tendo sido envolvida o Fornecedor de Serviços Externos de SI/TIC relacionado com a operação. Esta actividade foi acompanhada por parte da ENTIDADE pelo Gestor de Aplicação do Datawarehouse de Clientes.

A realização desta actividade veio dar resposta à recomendação: (Rai.3) (Secção 5.2), porque não era feita uma avaliação regular aos Fornecedores de Serviços de SI/TIC para assegurar a sua aderência aos Requisitos de Conformidade, que a ENTIDADE entenda assegurar. Por outro lado alinha-se com o benefício esperado com a implementação da *framework* – (B7) (Secção 4.5), porque o que é pretendido é a efectivação da monitorização mesmo que estejam envolvidos colaboradores de entidades externas.

5.3.7 Processo: Reportar (PR)

Analisar Estado da *Compliance* (PR.1)

Foram analisados os dados registados no Catálogo da *Compliance* dos SI/TIC oriundos da monitorização, e o Relatório de Avaliação dos Fornecedores de Serviços Externos de SI/TIC. Durante o estudo de caso não surgiu a necessidade de elaborar qualquer tipo de recomendações.

Na execução desta actividade estiveram envolvidas por parte da ENTIDADE, a Função *Compliance* dos SI/TIC. Esta actividade foi acompanhada por parte da ENTIDADE, pelo Gestor de Aplicação do Datawarehouse de Clientes, pela Área de Risco e Segurança e Área de Qualidade, por parte do BANCO, pela Função *Compliance* do BANCO e Unidade de Negócio.

A realização desta actividade veio dar resposta à recomendação: (Rai.4) (Secção 5.2), porque era necessário assegurar uma análise aos padrões recorrentes de falhas de *Compliance* bem como ao seu encaminhamento para investigação adicional e onde necessário, determinar as causas, e como colmatar essas falhas. Por outro lado alinha-se com o benefício esperado com a implementação da *framework* – (B1) (Secção 4.5), porque permite documentar o alinhamento estratégico entre SI/TIC e o negócio em matérias de *Compliance.*

Reporte Integrado da *Compliance* da Organização (PR.2)

Foi disponibilizada a informação sobre o estado da *Compliance* dos SI/TIC referente ao Requisito de Conformidade - Lei nº 36/2010 para ser integrado em relatórios equivalentes do BANCO. A produção deste tipo de relatório é anual de acordo com as exigências do Banco de Portugal.

Na execução desta actividade estiveram envolvidas por parte da ENTIDADE, a Função *Compliance* dos SI/TIC. Esta actividade foi acompanhada por parte da ENTIDADE, pelo Gestor de Aplicação do Datawarehouse de Clientes, pela Área de Risco e Segurança e Área de Qualidade, por parte do BANCO, pela Função *Compliance* do BANCO e Unidade de Negócio.

A realização desta actividade veio dar resposta à recomendação: (Rai.5) (Secção 5.2) porque não existia um alinhamento regular entre os relatórios de *Compliance* da ENTIDADE e os relatórios do BANCO, nem existia retenção do histórico integrado de informação. Por outro lado, alinha-se com o benefício esperado com a implementação da *framework* – (B1) e (B7) (Secção 4.5), porque permite evidenciar o nível de alinhamento estratégico entre SI/TIC e o Negócio em matérias de *Compliance.*

5.4 Auditoria da Situação Pós Implementação

A metodologia da auditoria da situação pós implementação da *Framework* para a Gestão da *Compliance* dos SI/TIC foi idêntica à da auditoria inicial. Esta auditoria teve como objectivo validar o resultado da utilização desta *framework* na ENTIDADE. Após a análise das respostas ao questionário verificou-se que o nível de maturidade do processo COBIT 4.1 - ME3 (ITGI, 2007) (Secção 2.3.1), foi incrementado para "3,33"[65] posicionando-se agora em processo definido. Este nível de maturidade aproxima-se do valor objectivo de maturidade "4" (processos geridos e medidos) como proposto pelo ISACA como resposta às exigências de Basileia II (Secção 2.3.1). Este valor é muito relevante para a ENTIDADE e o BANCO, pois existe uma relação directa entre a maturidade dos SI/TIC e o nível de reservas financeiras exigido pelo Banco de Portugal (BANCO DE PORTUGAL, 2007) estando este alinhado com o acordo de Basileia II[66] (BIS, 2006). Outro resultado da auditoria, numa perspectiva de melhoria contínua da gestão da *Compliance* na ENTIDADE foram as recomendações apresentadas na tabela 25.

Recomendação
(Rpi.1) Potenciar a antecipação de novas exigências dos Requisitos de Conformidade que devem ser asseguradas pelos SI/TIC.
(Rpi.2) Implementar processos que possam consolidar e expandir a cultura de *Compliance*.
(Rpi.3) Aplicar e consolidar os processos de gestão da *Compliance* por toda a ENTIDADE.

Rpi.x ("Rpi" de recomendação pós implementação, e "x" número da recomendação).

Tabela 25 - Recomendações resultantes da auditoria pós implementação da *Framework*

5.1 Principais Conclusões

A utilização da *framework* contribuiu para a incrementação do nível de maturidade do processo COBIT 4.1 - ME3 (ITGI, 2007) (Secção 2.3.1), e pela sistematização e normalização da gestão da *Compliance* nos SI/TIC, estabelecendo uma estrutura comum para os processos, as actividades e procedimentos.

O estudo de caso demonstrou, também, que a análise qualitativa e quantitativa das medidas e Controlos para assegurar as exigências dos Requisitos de Conformidade, providenciou uma visão holística quanto aos impactos destes nos domínios Tecnológicos e Organizacional, facilitando desta forma a tomada de decisões, bem como a possibilidade de um alinhamento entre o BANCO (Negócio) e a ENTIDADE (SI/TIC) em matérias de *Compliance*. Por outro lado, mostrou-se eficiente e eficaz no acompanhamento das necessárias adequações aos SI/TIC, desde a identificação do

[65] Para maior detalhe sobre a Auditoria à Situação Inicial consultar o Anexo – Estudo de Caso: Auditoria à Situação Após Implementação.
[66] Para maior detalhe sobre o acordo de Basileia II consultar o Anexo –Basileia II.

Requisito de Conformidade até à monitorização e posterior reporte das medidas e Controlos que asseguraram as exigências do requisito. Não foi possível aferir os resultados da *Compliance* no domínio Organizacional porque o "Processo de Trabalho: Gestão da Segurança da Informação" ainda se encontrava em especificação. Constatou-se, no entanto, que as recomendações para assegurar as exigências do Requisito de Conformidade - Lei nº 36/2010 estavam a ser incorporadas nessa especificação (Secção 5.3.5). Também não foi possível realizar qualquer tipo de auditoria à *Compliance* dos SI/TIC no período que decorreu o estudo de caso (Secção 5.3.5). Durante o estudo de caso, não foi possível recolher indicadores, no entanto, foi entendimento dos colaboradores da ENTIDADE que a sistematização e normalização das várias actividades permitiram uma melhoria para já qualitativa da Gestão da *Compliance* nos SI/TIC.

O administrador da ENTIDADE responsável pela *Compliance* referiu que a pressão resultante das exigências decorrentes do cumprimento dos Requisitos de Conformidade deve, à semelhança de outras exigências de Negócio, ser encarada como uma oportunidade para tornar as Organizações e os processos de Negócio mais ágeis, mais eficientes e mais seguros num contexto de melhoria continua e participada. Neste contexto, afirmou que o estudo de caso sobre a implementação da *framework* é uma base de trabalho testada cuja utilização continuada se constituirá numa ferramenta para alcançar tais objectivos.

5.2 Propostas de Melhoria

A *framework* poderá ser melhorada através da inclusão de processos para antecipar as novas exigências dos Requisitos de Conformidade quer estes sejam novos ou alterações aos existentes (Rpi.1) (Secção 5.4).

Uma das questões identificadas durante a implementação do estudo de caso, e não explorada, foi a situação de se constatar que não existam condições para implementar as exigências dos Requisitos de Conformidade. Esta situação poderá ser analisada pela continuação da utilização da *framework* na ENTIDADE ou em futuras implementações noutras Organizações. A sua utilização identificará outras questões ainda não identificadas mas que deverão ser alvo de análise e melhoramento da *framework*.

No que se refere à ENTIDADE, a melhoria poderá passar pela (Rpi.2) (Secção 5.4) massificação de uma cultura de *Compliance*, bem como (Rpi.3) (Secção 5.4) pela consolidação dos processos de gestão da *Compliance* e aplicar estes processos a todos os Requisitos de Conformidade dos quais a ENTIDADE entenda que devam ser asseguradas as suas exigências.

6 Conclusões e Trabalhos Futuros

Neste capítulo apresentam-se as conclusões desta dissertação e trabalhos futuros.

6.1 Conclusões

Considera-se que os objectivos propostos nesta dissertação, tal como inicialmente formulados (Secção 3.2), foram atingidos. Através do estudo de caso ficou demonstrado que a utilização da *framework* desenvolvida deu resposta aos problemas identificados (Secção 3.1) e que esta dissertação pretendia resolver. Não foi possível a recolha de indicadores que pudessem servir de base comparativa para a medição da eficiência da implementação da *framework*, no entanto, foi de entendimento geral na ENTIDADE que a sua utilização melhorou a Gestão da *Compliance* nos SI/TIC (Secção 5.1).

O objectivo 1 (Secção 3.2) consubstanciou-se no desenvolvimento da *framework* (Secção 4), com base na integração e consolidação das orientações e boas práticas propostas pelos modelos dos vários autores (Secção 2.2) e do ISACA (Secção 2.3.1), que pretendeu responder ao problema (Problema 2, Secção 3.1) da falta de uma abordagem transversal quanto à gestão dos Requisitos de Conformidade, providenciando a *framework* uma visão mais ampla do valor efectivo da *Compliance* quanto ao risco associado à não implementação das medidas e Controlos que assegurem as exigências de tais requisitos.

O objectivo 2 (Secção 3.2) foi alcançado como demonstrado pelos resultados da sua implementação (Secção 5) tendo sido consolidados nas suas conclusões (Secção 5.1), incrementando mesmo o nível de maturidade (Secção 5.4) na gestão da *Compliance* na ENTIDADE. Deste modo, pretendeu-se responder ao problema (Problema 1, Secção 3.1) porque, através da sua implementação reduziu-se a complexidade da sua interpretação e da identificação do que seria necessário para assegurar as exigências (Secção 5.3.4) do Requisito de Conformidade tratado.

6.2 Trabalhos Futuros

Embora a metodologia apresentada tenha sido baseada na implementação da *framework* a um Requisito de Conformidade específico, seria interessante que esta fosse testada noutras organizações, em particular face a factores não contemplados que poderão condicionar a implementação, de modo a ajustá-la e melhorá-la. Os factores poderão passar pela dimensão da organização, a sua estrutura organizacional, a complexidade e diversidade das suas operações, e os requisitos de conformidade aplicáveis à Entidade prestadora de serviços de SI/TIC. Estas novas implementações deverão incluir uma fase inicial de recolha de indicadores que possam servir de base comparativa para a medição da eficiência da implementação em estudo.
A integração da metodologia "*Frame-Based Requirements Analysis Method (FBRAM)*" proposta Breaux e Antón (BREAUX e ANTÓN, 2007, p.1) (Secção 2.2), nesta *framework* desenvolvida.

7 Glossário

Auditoria - Inspecção formal e verificação para aferir se uma norma ou conjunto de directrizes estão a ser seguidas, os dados são exactos, ou as metas de eficiência e eficácia estão a ser alcançadas. Uma auditoria pode ser realizada por recursos internos ou externos à Organização (ISACA, 2010).

Aplicação - é um sistema para recolher, processar, armazenar e apresentar dados por meio de um computador (ISO/IEC/IEEE 24765, 2010), ou Software de suporte a um ou vários processos de negócio, com um conjunto de funcionalidades. De um modo geral, abrange procedimentos de recolha, processamento, armazenamento e disponibilização de informação (ITGI, 2007).

Boas práticas – Processo ou actividade comprovada que tem sido utilizado com sucesso por várias Organizações (ISACA, 2010).

Controlo – É uma forma de gerir um risco, garantindo que um objectivo de Negócio é atingido, ou que um processo seja seguido. É a medida posta em prática para regular, orientar e monitorizar um risco (ITGI, 2007b).

Efectividade – é a preocupação com a garantia relativa à relevância e utilidade da informação fornecida a entidades ou processos (ITGI, 2007).

Métrica – Medida quantitativa usada para avaliar e comunicar os indicadores entre os resultados obtidos e os objectivos determinados (ISACA, 2010).

Objectivos de Controlo – são declarações genéricas de um resultado desejado ou proposto para ser atingido, através da implementação de procedimentos de controlo num determinado processo (ITGI, 2007).

8 Bibliografia

(ANNASWAMY, 2009) Annaswamy, Subramanian, "*A Road Map for Regulatory Compliance*", ISACA JOURNAL VOLUME 4 de 2009. Publicado em 2009 pelo ISACA, nos Estados Unidos da América.

(BACE e ROZWELL, 2006) John Bace, Carol Rozwell, 2006 "*Compliance Key Initiative Overview for CIOs*" publicado em 7 Julho de 2006, pela Gartner.

(BCE) The European Central Bank, "*Estabilidade financeira*", consultado em 2010-10-23, em http://www.ecb.int/ecb/orga/tasks/html/financial-stability.pt.html.

(BANCO DE PORTUGAL, 2007) "MAR – Modelo de Avaliação de Riscos". Publicado em 2007 pelo Departamento de Supervisão Bancária do Banco de Portugal, Lisboa, Portugal.

(BANCO DE PORTUGAL, 2008), Aviso do Banco de Portugal nº 5/2008. Publicado em 2008 pelo Banco de Portugal, Lisboa, Portugal.

(BANCO DE PORTUGAL, 2005) Instrução do Banco de Portugal nº 20/2005 - Controlo Interno. Publicado em 2005 pelo Banco de Portugal, Lisboa, Portugal.

(BANCO DE PORTUGAL, 2010) Banco de Portugal; "Riscos de Corrupção e Infracções Conexas": publicado em Maio de 2010, pela Comissão de Coordenação de Segurança (CCS) do Banco de Portugal, Lisboa, Portugal.

(BIS, 2002) Bank for International Settlements, "*Sound Practices for the Management and Supervision of Operational Risk*". Publicado em Junho de 2002 pelo Basel Committee on Banking Supervision. Basileia, Suiça.

(BIS, 2005) Bank for International Settlements,"*Compliance and the Compliance Function in Banks*". Publicado em Abril de 2005 pelo Basel Committee on Banking Supervision. Basileia, Suiça.

(BIS, 2006) Bank for International Settlements "*International Convergence of Capital Measurement and Capital Standards*", publicado em 2006 pelo Basel Committee on Banking Supervision. Basileia, Suiça.

(BREAUX and ANTÓN, 2007), Travis D. Breaux and Annie I. Antón, "*A Systematic Method for Acquiring Regulatory Requirements: A Frame-Based Approach*", publicado em Outubro de 2007 na "6th International Workshop on Requirements for High Assurance Systems (RHAS-6), Delhi, India.

(CALDER, 2008) Calder, Alan, "*Governance, risk, and compliance handbook, technology, finance, environmental, and international guidance and best practices*" capítulo "*IT Governance Overview*". Publicado em 2008 pela JOHN WILEY & SONS, INC., New Jersey, Estados Unidos da América.

(CASCARINO, 2007) Cascarino, Richard E., "Auditor's Guide to Information Systems Auditing", publicado em 2007, pela JOHN WILEY & SONS, INC, New Jersey, Estados Unidos da América.

(COSO, 1994) COSO - "*Internal Control – Integrated Framework*". Publicado em 1994, pela Committee of Sponsoring Organizations of the Treadway Commission (Comissão Nacional sobre Fraudes em Relatórios Financeiros), Jersey City, Estados Unidos da America.

(COSO, 2007) COSO "Gerenciamento de Riscos Corporativos - Estrutura Integrada, Sumário Executivo", publicado em 2007 pela Committee of Sponsoring Organizations of the Treadway Commission (Comissão Nacional sobre Fraudes em Relatórios Financeiros), Jersey City, Estados Unidos da América.

(COSTA, 2010) Costa, Carlos da Silva, "*Discurso de tomada de posse do Governador do Banco de Portugal*", 7 de Junho de 2010, consultado em 2010-10-16, em http://www.bportugal.pt/pt-PT/OBancoeoEurosistema/IntervencoesPublicas/Paginas/intervpub20100607.aspx

(COX, 2008) Cox, Dennis; "*Governance, Risk and Compliance Handbook, Technology, Finance, Environment, and International Guidance and Best Practices*" capítulo "Financial services regulation and corporate governance". publicado em 2008 pela JOHN WILEY & SONS, INC, New Jersey, Estados Unidos da América.

(DAMERI, 2009) Dameri, Renata P., "*Improving the Benefits of IT Compliance Using Enterprise Management Information Systems*." The Electronic Journal Information Systems Evaluation Volume 12 Issue 1 de 2009 (27-38). Publicado em 2009 pela Academic Conferences Ltd, Kidmore End, Reino Unido.

(HANSSON, 2008) Hansson, Lars, "*IT System Regulatory Compliance*" Tese de dissertação do Royal Institute of Technology, Stockholm. Publicado em 2008 pelo Royal Institute of Technology, Stockholm, Sweden.

(HO, 2009) Ho, Amelia, "*Compliance Management: A Holistic Approach*" ISACA JOURNAL VOLUME 5. Publicado em 2009 pelo ISACA, Illinois, Estados Unidos da América.

(ISACA, 2010) Information Systems Audit and Control Association, "*Glossary of Terms*" publicado em 2010 pelo ISACA, Illinois, Estados Unidos da América.

(ISACA, 2011) Information Systems Audit and Control Association, "*Regulatory compliance is top concern in 2011*" publicado em 19 Abril de 2011 pelo ISACA em http://www.isaca.org/About-ISACA/Press-room/News-Releases/2011/Pages/ISACA-survey-regulatory-compliance-is-top-concern-in-2011.aspx e consultado em Maio de 2011, Illinois, Estados Unidos da América.

(ISO/IEC/IEEE 24765, 2010) International Organization for Normalization, "ISO/IEC/IEEE 24765 Systems and software engineering – Vocabulary", publicado em 2010 pela ISO e consultado em http://www.iso.org.

(ISO/IEC 27001, 2005) International Organization for Normalization, "ISO/IEC 27001 Requisitos do Sistemas de Gestão de Segurança da Informação", publicado em 2005 pela ISO e consultado em http://www.iso.org.

(ISO/IEC 27002, 2005) International Organization for Normalization, "ISO/IEC 27002 Código de Prática para a Segurança da Informação", publicado em 2005 pela ISO e consultado em http://www.iso.org.

(ITIL V3, 2007) Information Technology Infrastructure Library, "Glossário de Termos, Definições e Acrónimos", Versão v3.1.24. Publicado em Maio de 2007, pela OGC (Office for Government Commerce) , Reino Unido.

(ITGI, 2007) IT Governance Institute, "*COBIT 4.1 Control Objectives for Information and related Technology*", publicado em 2007 pelo IT Governance Institute, Illinois, Estados Unidos da América.

(ITGI, 2007a) IT Governance Institute, "*COBIT Control Practices, 2ª Edition*". Publicado em 2007 pelo IT Governance Institute, Illinois, Estados Unidos da América.

(ITGI, 2007b) IT Governance Institute, "*IT Control Objectives for Basel II: The Importance of Governance and Risk Management for Compliance*". Publicado em 2007 pelo IT Governance Institute, Illinois, Estados Unidos da América.

(PMI, 2004) Project Management Institute; "*A Guide to the Project Management Body of Knowledge-Fourthe Edition*"; publicado em 2008 pelo PMI.

(ROSS , 2007) Ross, Steven J., "*Compliance and Beyond*" Information Systems Control Journal, Volume 4. Publicado em 2007 pelo ISACA, Illinois, Estados Unidos da América.

(SANTS, 2007) Sants, Hector "*Managing Compliance Risk in Major Investment Banks - Good Practices*", estudo publicado pela Financial Services Authority, em Julho de 2007, Londres, Reino Unido.

(SANTOS, 2002) Santos, Teixeira," O Sistema Financeiro e a Globalização - A Regulação do Sistema Financeiro", Conferência organizada pelo IDEF-ISEG 17 de Junho de 2002, Lisboa, Portugal.

(TARANTINO, 2008) Tarantino, Anthony, "*Governance, Risk and Compliance Handbook, Technology, Finance, Environment, and International Guidance and Best Practices*", capítulo "*Introduction*" publicado em 2008 pela JOHN WILEY & SONS, INC., New Jersey, Estados Unidos da América.

(SOX, 2008) "*SARBANES-OXLEY SECTION 404: A Guide for Management by Internal Controls Practitioners*" 2nd Edition, publicado pelo The Institute of Internal Auditors em Janeiro de 2008.

(YIN, 2003) Yin, Robert; "*Applications of Case Study Research*"; 2ª Edição. Publicado em 2003 pela Sage.

9 ANEXOS

Anexo A - Caracterização e Funções do Sistema Financeiro

O Banco Central Europeu (BCE) caracteriza o Sistema Financeiro, em: (i) Mercados Financeiros[67]; (ii) Intermediários Financeiros[68]; e (iii) Infra-estrutura Financeira[69]. A figura 8 apresenta o diagrama adaptado das funções do Sistema Financeiro, como ele é visto pelo Banco Central Europeu.

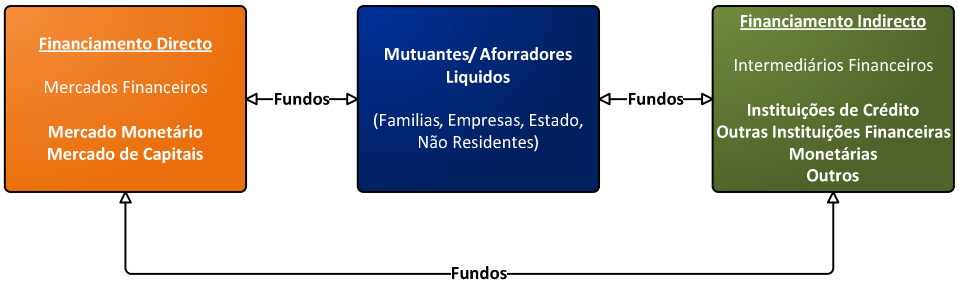

Figura 8 – Diagrama das Funções do Sistema Financeiro

Em Portugal o Sistema Financeiro integra três sectores: (i) o Sector Bancário[70]; (ii) o Sector dos Valores Mobiliários[71], e (iii) o Sector Segurador[72]. A fronteira entre os três sectores tem vindo a esbater-se, devido essencialmente a um processo de integração tecnológico, geográfico e funcional como refere Santos (SANTOS, 2002).

O Decreto-Lei n° 298/92, de 31 de Dezembro, do Regime Geral das Instituições de Crédito e Sociedades Financeiras (conhecido pela abreviatura RGICSF), regulamenta o processo de estabelecimento e exercício da actividade das instituições de crédito e das sociedades financeiras em Portugal, devendo-se estas reger pelo descrito no preâmbulo do Decreto-Lei n° 298/92 onde são referidos os cinco pilares em que assenta a integração financeira na Comunidade Europeia: (i) Liberdade de estabelecimento das empresas financeiras; (ii) Liberdade de prestação de serviços por estas empresas; (iii) Harmonização e reconhecimento mútuo das regulamentações nacionais; (iv) Liberdade de circulação de capitais; (v) União económica e monetária. O artigo n° 3 do Decreto-Lei n°

[67] Tais como os mercados monetários e de capitais, os quais canalizam fundos excedentários dos mutuantes (isto é, empresas ou particulares que pretendem investir o seu dinheiro) para os mutuários (ou seja, quem necessita de capital).

[68] Tais como bancos e companhias de seguros, que indirectamente fazem a ligação entre mutuantes e mutuários, se bem que os mutuários também possam obter fundos directamente dos mercados financeiros mediante a emissão de títulos, por exemplo, acções e obrigações.

[69] Os mercados que possibilitam a transferência de pagamentos, bem como a transacção, compensação e liquidação de títulos.

[70] Este sector insere-se na actividade das instituições de crédito, que recebem depósitos e outros fundos reembolsáveis do público para os aplicarem na concessão de crédito.

[71] Este mercado insere-se no mercado financeiro e permite o acesso directo ao mercado, através da emissão e negociação de valores mobiliários, titulados ou não titulados, e os serviços de investimento ligados a esses mercados e valores sem intermediação financeira das instituições de crédito, sendo que neste caso os investidores assumem o risco das suas aplicações de forma directa ou através de instituições especializadas (instituições de investimento colectivo).

[72] Este sector insere-se nas actividades de cobertura de riscos mediante o pagamento de prémios, garantindo este um pagamento em caso de ocorrência de uma determinada contingência.

298/92 estabelece que os bancos são considerados instituições de crédito em Portugal. O Decreto-Lei n° 201/2002, de 26 de Setembro, define no Artigo n° 2, as instituições de crédito, nomeadamente os bancos, como empresas cuja actividade consiste em receber do público depósitos ou outros fundos reembolsáveis (alocação do capital), a serem aplicados por conta própria, mediante a concessão de crédito, tendo deste modo um papel fundamental no financiamento das actividades económicas para o desenvolvimento da sociedade portuguesa.

O Banco de Portugal, e de acordo com a Lei Orgânica do Banco de Portugal - aprovada pela Lei n.º 5/98, de 31 de Janeiro, e com alteração introduzida pelo Decreto-Lei n.º 118/2001, de 17 de Abril, para além da faculdade de apresentar propostas de diplomas legislativos à aprovação do governo, dispõe de competência própria para criar Avisos, Circulares ou Instruções. Para além dos poderes de regulamentação do Banco de Portugal ainda tem outros poderes de supervisão como o de autorizar, dar instruções, inspeccionar e sancionar, de modo a evitar que o impacto de uma falha de um Banco a actuar em Portugal possa gerar através do efeito dominó uma crise que afecte o sistema e, por consequência, o desenvolvimento económico e social em Portugal. Com a supervisão o Banco de Portugal pretende avaliar, em toda a sua extensão, as implicações, nomeadamente em matéria de assunção de risco, em estruturas complexas, de modo a garantir que os correspondentes riscos se encontram correctamente reflectidos no balanço das instituições e cobertos por adequados fundos próprios. "*Os bons resultados de uma instituição financeira não dispensam uma permanente indagação sobre essa mesma instituição, nomeadamente sobre a solidez dos seus fundamentos, os riscos futuros e a sua representação no balanço da instituição supervisionada*" (COSTA, 2010). A operacionalização desta abordagem pelo Banco de Portugal passa por uma supervisão permanente e de proximidade através das equipas do Banco de Portugal, já instaladas intramuros, das principais instituições do Sector Bancário. O objectivo do Banco de Portugal é o de alcançar um conhecimento mais directo e mais profundo da entidade supervisionada e do respectivo perfil de risco, no contexto que a banca não pode ser entregue à auto-regulação sendo necessário prosseguir e reforçar a supervisão permanente das Instituições Financeiras.

Anexo B - COSO

O COSO é uma organização dedicada a melhorar a qualidade do reporte financeiro, através da ética de negócio, controlos internos efectivos e governo cooperativo. A framework elaborada pelo COSO em 1992, denominada "*Internal Control – Integrated Framework*" (COSO, 1994), fornece um modelo de avaliação do controlo interno das Organizações que é reconhecido e aceite de forma generalizada, como referência para o Controlo Interno. Com o acordo de Basileia II, não está apenas em questão uma simples norma de proporções contabilísticas a aplicar pelo Sector Bancário, mas, sobretudo, de instrumentos de gestão e de competitividade, estando em causa: (i) Análise da exposição aos riscos; (ii) Capacidade de definição e execução de estratégias de gestão de riscos; (iii) Capacidade de fixação e vigilância de limites de risco adequados; (iv) Capacidade e consistência na análise de performance; (v) Controlo e supervisão. Desde então, a referida *framework* foi incorporada em políticas, normas e regulamentos adoptados por muitas organizações, nomeadamente as do Sector

Financeiro para controlar melhor as suas actividades visando o cumprimento dos objectivos estabelecidos.

A "*Internal Control – Integrated Framework*" do COSO (COSO, 1994) é constituída por cinco componentes: (C1) Ambiente de Controlo; (C2) Avaliação de Risco; (C3) Actividades de Controlo; (C4) Informação e Comunicação; (C5) Monitorização. Por outro lado, é constituída por três categorias de objectivos: (O1) A *Compliance* (fundamenta-se no cumprimento dos Requisitos de Conformidade); (O2) As Operações (utilização eficaz e eficiente dos recursos); (O3) O Reporte Financeiro (relacionado com a confiabilidade[73] dos relatórios).

O COSO em 2004, devido à necessidade de uma estratégia sólida capaz de identificar, avaliar e administrar riscos, criou o COSO-ERM - Enterprise Risk Management - Integrated Framework (COSO, 2007) com o objectivo de ajudar as organizações a perceber o que é o risco, e de que modo este está presente na Organização. O COSO-ERM (COSO, 2007) baseia-se na integração de oito componentes e quatro categorias de objectivos que podem ser aplicadas a qualquer tipo de Organização. COSO-ERM (COSO-ERM, 2004) herda da "*Internal Control – Integrated Framework*" do COSO (COSO, 1994) cinco componentes: Ambiente Interno, Avaliação dos Riscos, Actividades de Controlo, Informação e Comunicação, Monitorização; e acrescenta mais três componentes: (C6) Definição de Objectivos; (C7) Identificação de Eventos; (C8) Resposta ao Risco. Por outro lado, herda as três categorias e acrescenta mais um, o (O4) Estratégico.

Anexo C - COBIT 4.1

O COBIT 4.1 (ITGI, 2007) foi desenvolvido pelo ISACA e disponibiliza um modelo genérico de referência dos processos, que são normalmente executados para gerir os SI/TIC. As boas práticas referenciadas representam o consenso de peritos e focam-se fortemente no controlo e menos na execução, ajudando a optimizar os investimentos possíveis em SI/TIC, assegurando as entregas de serviços e providenciando uma medida quanto a qual podem ser avaliados. O COBIT 4.1 (ITGI, 2007) proporciona mecanismos para o alinhamento do Negócio com os SI/TIC através da ligação entre as metas de negócio e as metas dos SI/TIC, proporcionando métricas e modelos de maturidade[74] para medir a sua realização e identificar as responsabilidades associadas aos donos do negócio e dos processos de SI/TIC.

A estrutura do COBIT 4.1 (ITGI, 2007) é ilustrada por um modelo de processos que subdivide as TI em 34 processos e 318 actividades de controlo, com responsabilidades nas áreas do planeamento, construção, execução e monitorização, proporcionando uma visão holística para a gestão dos SI/TIC.

Anexo D - Basileia II

O acordo de Basileia II (BIS, 2006) é baseado em três Pilares: 1. Requisitos de Capital, 2. Revisão da Supervisão e 3. Disciplina de Mercado. Com o acordo de Basileia II, não está apenas em questão

[73] Confiabilidade – é o fornecimento de informação fiável (ITGI, 2007).

[74] Para maior detalhe sobre o modelo de maturidade do processo COBIT4.1: ME3 consultar o Anexo - Modelo de Maturidade do processo COBIT 4.1: ME3.

uma simples norma de âmbito contabilístico a aplicar pelo Sector Bancário, mas, sobretudo, de instrumentos de gestão e de competitividade, estando em causa: (i) Análise da exposição aos riscos; (ii) Capacidade de definição e execução de estratégias de gestão de riscos; (iii) Capacidade de fixação e vigilância de limites de risco adequados; (iv) Capacidade e consistência na análise de performance; (v) Controlo e supervisão. Com este acordo, as instituições financeiras são encorajadas a identificar, medir e gerir internamente os riscos da sua actividade, permitindo-lhes calcular, com base em modelos internos, o capital necessário para assegurar um nível mínimo de solvabilidade.

Anexo E - Modelo de Maturidade do processo COBIT 4.1: ME3

A Maturidade é um indicador que mostra o grau de confiança e de dependência que o negócio pode ter relativamente a um processo poder ou não atingir os seus objectivos, ou seja nível de confiança, eficácia e eficiência de um processo, actividade, função, organização, entre outros. O Modelo de Maturidade do COBIT 4.1 (ITGI, 2007, p.6), também conhecido por Capability Maturity Model (CMM), baseado no modelo de avaliação da maturidade de 5 níveis proposto pela Universidade Carnegie-Mellon para o SEI (Software Engineering Institute), é uma ferramenta de governo dos SI/TIC usada para medir o nível de maturidade dos processos. Em termos práticos, os graus de maturidade mostram até que ponto é que os processos e as actividades da Organização estão documentados, controlados, monitorizados, optimizados e disseminados pela Organização. O modelo de maturidade apresentado pelo ISACA para o processo do COBIT 4.1: ME3 (ITGI, 2007, p.164) é definido da seguinte forma:

0 – Não Existe: Há pouca consciência sobre Requisitos de Conformidade que afectam os SI/TIC.

1 – Inicial: Há consciência do impacto dos Requisitos de Conformidade na organização. São adoptados processos informais para manter a *Compliance*, mas só quando surge a necessidade em novos projectos ou em resposta às auditorias ou análises críticas.

2 – Repetitivo: Existe um entendimento da necessidade, mas ainda não existem processos formais para assegurar a aderência aos Requisitos de Conformidade. Existe grande confiança no conhecimento e na responsabilidade das pessoas, subsistindo a probabilidade de erros. Há formação informal sobre Requisitos de Conformidade e matérias de *Compliance*.

3 – Definido - Foram desenvolvidos, documentados e comunicados as políticas, planos e procedimentos para assegurar a aderência aos Requisitos de Conformidade, no entanto, estes podem estar desactualizados, ou serem impraticáveis de implementar, a monitorização é limitada, mas é realizada formação.

4 – Gerido – Existe um total entendimento para assegurar a aderência aos Requisitos de Conformidade assente numa função centralizada, existindo um responsável definido com responsabilidades claras, que fornece orientações para toda a Organização. O processo de *Compliance* inclui mecanismos de identificação de novos requisitos ou alteração aos existentes, bem como monitorização para a implementação de acções correctivas. São realizadas acções de formação regularmente.

5 – Optimizado - Existe um total entendimento para assegurar a aderência aos Requisitos de Conformidade assente numa função centralizada, existindo um responsável definido com

responsabilidades claras, que fornece orientações para toda a Organização. Existe um bom conhecimento e aplicação das melhores práticas sobre os requisitos aplicáveis, incluindo tendências futuras, antecipação de alterações e necessidade de novas soluções. Existe um sistema corporativo de monitorização centralizada do processo de *Compliance*. A cultura organizacional de gestão relativamente ao processo de *Compliance* é suficientemente sólida, e o processo correctamente desenvolvido, o que permite que as acções de formação sejam aplicadas a um grupo de novos colaboradores e somente quando há alterações significativas ao processo de *Compliance*.

Anexo F - Relacionamento entre Objectivos e Métricas do processo COBIT 4.1: ME3

O ISACA identifica através do COBIT 4.1 (ITGI, 2007, p.165) três níveis de objectivos**:** (1) TI; (2) Processos; (3) Actividades – sendo estes avaliados pelas suas métricas. O ISACA identifica através do COBIT 4.1 (ITGI, 2007) dois tipos de métricas, as medidas do resultado (saídas), indicando se os objectivos foram alcançados, e os indicadores de performance, indicando se as metas podem ser alcançadas. As medidas do resultado, como são obtidas após a execução do processo são considerados indicadores históricos, por outro lado, os indicadores de desempenho são obtidos previamente, por este motivo denominam-se indicadores futuros, definindo as medidas que determinam quão bem os negócios, as funções dos SI/TIC ou os processos de TI estão a ser executados para permitir que os objectivos sejam atingidos. Na figura 9 apresenta-se o relacionamento entre os processos, objectivos e métricas do processo COBIT 4.1: ME3 (ITGI, 2007, p.165).

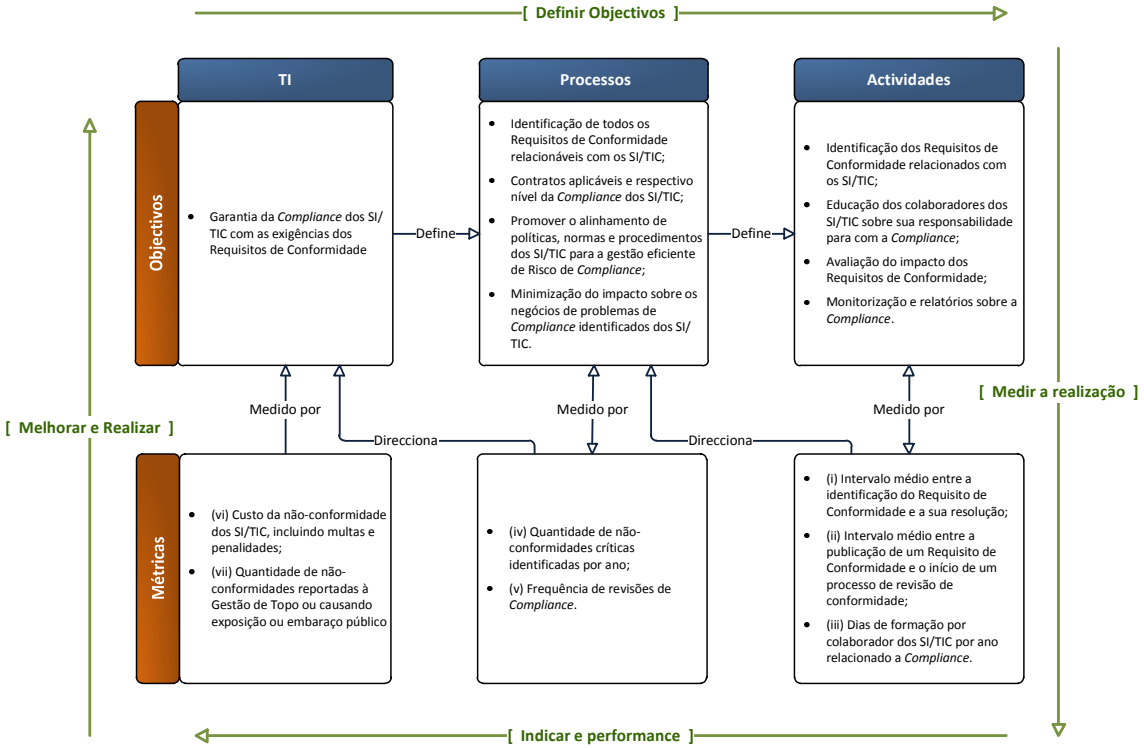

Figura 9 – Objectivos e métricas do processo COBIT 4.1: ME3

Anexo G - Estudo de Caso: Auditoria à Situação Inicial

Na tabela 26 apresenta-se o questionário da auditoria à situação inicial, que foi baseada no ficheiro de Excel disponibilizado pelo ITIG[75] e tendo como referência o modelo de maturidade proposto pelo ISACA no processo COBIT 4.1 - ME3 (ITGI, 2007) (Secção 2.3.1).

#	Afirmação	Nível de Maturidade	Nível Alinhamento				Tipo de sentença[76]	Mínimo		Valores
			Não Alinhado	Pouco	Bastante	Completamente		Falso	Verdadeiro	
1	Existe uma consciencialização limitada dos Requisitos de Conformidade que afectam os SI/TIC, não existindo um processo para avaliação da *Compliance* com os Requisitos de Conformidade.	0		X			N		X	1/3
2	Existe uma consciencialização sobre os Requisitos de Conformidade que têm impacto na Organização.	1			X		P		X	2/3
3	São adoptados processos informais para promover a *Compliance* nos casos em que essa necessidade surge em novos projectos, ou como resposta a processos de revisão ou auditoria.	1			X		P		X	2/3
4	Existe um entendimento da necessidade de aderir aos Requisitos de conformidade e essa necessidade é comunicada.	2			X		P		X	2/3
5	Nas situações em que a *Compliance* é um requisito recorrente como, por exemplo, em requisitos financeiros e legislação sobre privacidade, foram desenvolvidos e são aplicados anualmente procedimentos individuais de conformidade.	2			X		P		X	2/3
6	Não existe uma abordagem padronizada.	2			X		N	X		2/3
7	Existe uma grande dependência relativamente ao conhecimento e responsabilidades individuais, sendo provável a ocorrência de erros.	2		X			N		X	1/3
8	Existe formação informal sobre os Requisitos de conformidade e de *Compliance*.	2		X			N		X	1/3
9	Foram desenvolvidos, documentados e comunicados as políticas, planos e procedimentos para assegurar a aderência aos Requisitos de Conformidade . No entanto, alguns destes procedimentos podem não ser sempre seguidos, estarem desactualizados, ou serem impraticáveis de implementar.	3		X			P	X		1/3
10	A monitorização efectuada é limitada e alguns dos requisitos legais podem não estar a ser endereçados.	3			X		N	X		2/3
11	São realizadas acções de formação, sobre os requisitos legais e normativos externos com impacto na Organização e no processo de *Compliance* definido.	3		X			P	X		1/3
12	Existem contratos e processos legais padronizados para minimizar os riscos associados a perdas contractuais.	3			X		P		X	2/3

[75] O ITIG disponibiliza mesmo um ficheiro de excel para o devido efeito em www.isaca.org.

[76] Relaciona-se com o sentido da resposta P- positivo e N- negativo, afetando deste modo o valor da maturidade a alcançar.

13	Há um total entendimento das questões relacionadas com os Requisitos de conformidade e da necessidade de assegurar a *Compliance* a todos os níveis.	4		X			P	X		1/3
14	Existe um plano de formação formal que assegura que todos os colaboradores estão cientes das suas obrigações de *Compliance*.	4		X			P	X		1/3
15	Existe um responsável definido pelo processo de *Compliance* e as suas responsabilidades são claras.	4		X			P	X		1/3
16	O processo de *Compliance* inclui a revisão do ambiente legal para identificar Requisitos de conformidade e respectivas alterações.	4		X			P	X		1/3
17	Há um mecanismo implementado para monitorizar falhas de *Compliance* com Requisitos de Conformidade, reforçar as práticas internas e implementar acções correctivas.	4		X			P	X		1/3
18	As questões de não *Compliance* são analisadas para identificar a origem da situação de forma padronizada, com o objectivo de definir soluções sustentáveis.	4		X			P	X		1/3
19	As práticas internas são utilizadas para necessidades específicas, como regulamentação base e contratos de serviços recorrentes.	4		X			P	X		1/3
20	Encontra-se implementado e reforçado um processo organizado e eficiente de *Compliance* com os Requisitos de Conformidade, assente numa função centralizada, que fornece orientações para toda a Organização.	5		X			P	X		1/3
21	Existe um conhecimento extenso sobre os Requisitos de Conformidade aplicáveis, incluindo tendências futuras, antecipação de alterações e necessidade de novas soluções.	5	X				P	X		0
22	A Organização participa em discussões externas com grupos de regulamentação e Indústria, para perceber e influenciar os Requisitos de Conformidade que afectam a Organização.	5		X			P	X		1/3
23	As melhores práticas são desenvolvidas garantindo uma *Compliance* eficaz com os Requisitos de Conformidade, tendo como resultado a existência de poucas excepções de *Compliance*.	5		X			P	X		1/3
24	Existe um sistema corporativo de monitorização centralizada do processo de *Compliance*, permitindo à Gestão documentar o fluxo de informação e avaliar e melhorar a qualidade e eficiência do processo.	5		X			P	X		1/3
25	Encontra-se implementado e alinhado com as melhores práticas um processo de auto-avaliação dos Requisitos de Conformidade.	5	X				P	X		0
26	A cultura organizacional de gestão relativamente ao processo de *Compliance* é suficientemente sólida, e o processo correctamente desenvolvido, que permite que as acções de formação sejam aplicadas a um grupo de novos colaboradores e somente quando há alterações significativas ao processo de *Compliance*.	5		X			P	X		1/3

Tabela 26 - Questionário da auditoria à situação inicial.

Na tabela 27 apresenta-se o nível de maturidade alcançado, após registo das evidências no questionário da auditoria à situação inicial.

Nível de Maturidade	Somas dos Alinhamentos	# Afirmações	Média dos Alinhamentos de Cada Nível de Maturidade	Contribuição Ponderada com a Média dos Níveis de Maturidade	Contribuição Aferida com o Nível de Maturidade
0	0,33	1	0,33	0,13	0,00
1	1,33	2	0,67	0,26	0,26
2	2,67	5	0,53	0,20	0,41
3	2,00	4	0,50	0,19	0,58
4	2,33	7	0,33	0,13	0,51
5	1,67	7	0,24	0,09	0,46
			2,60	**1,00**	**2,21**

Tabela 27 - Nível de maturidade determinado pela auditoria à situação inicial.

Anexo H – Requisito de Conformidade - Lei nº 36/2010

A Lei n.º 36/2010, de 2 de Setembro, alterou o artigo 79.º do Regime Geral das Instituições de Crédito e Sociedades Financeiras (RGICSF), modificando a alínea d) do nº 2 e introduzindo um novo nº 3. Este diploma insere-se num conjunto de leis dirigidas à prevenção e ao combate à corrupção, aprovadas pela Assembleia da República. A criação da Base de Dados de Contas do Sistema Bancário (BCB) pressupõe a implementação de um sistema de recolha e armazenamento de informação, em ordem a permitir o seu fornecimento às autoridades judiciárias, quando solicitado. Através da Carta-Circular n.º 8/2011/DET foi divulgada a Instrução n.º 7/2011 do Banco de Portugal, que regulamentou a BCB, na qual constam os titulares de todas as contas, indicando qual a informação que todas as entidades autorizadas a abrir contas bancárias, seja de que tipo for, devem enviar ao Banco de Portugal.

Anexo I - Estudo de Caso - Indicação dos impactos (Domínio Organizacional)

Como a informação a enviar é de acesso restrito e confidencial no BANCO, foram determinadas as recomendações (R) para assegurar a segurança da informação, tendo para tal sido consideradas as boas práticas relacionadas com a - Gestão de Operações e Comunicações, da ISO/IEC 27002 (Código de Prática para a Segurança da Informação) (ISO/IEC 27002, 2005).

- R1 – Devem existir procedimentos para evitar que a Informação trocada seja interceptada, copiada, modificada, perdida ou destruída;

- R2 - Devem existir procedimentos para proteger os anexos electrónicos com informação sensível ou crítica;
- R3 - Devem ser utilizadas técnicas criptográficas para proteger a integridade, autenticidade, e confidencialidade da Informação;
- R4 - Devem ser definidos procedimentos que garantam que as infra-estruturas utilizadas na troca de Informação cumprem as exigências do Requisito de Conformidade;
- R5 - Devem existir procedimentos relativos a acordos de trocas de Informação que garantam que a Segurança da Informação requerida corresponde à sensibilidade da Informação de Negócio que é necessário proteger;
- R6 - Devem existir procedimentos relativos a acordos de trocas de Informação que estabeleçam a necessidade de assegurar a rastreabilidade e a não repudiação;
- R7 - Devem existir procedimentos relativos a acordos de trocas de Informação que estabeleçam a necessidade de identificar as implicações relativas à perda de dados e outros incidentes de Segurança da Informação, atribuindo responsabilidades para cada caso;
- R8 - Devem existir procedimentos relativos a acordos de trocas de Informação que estabeleçam a necessidade de definir funções e responsabilidades na protecção de dados;
- R9 - Devem existir procedimentos que impeçam o não repúdio de mensagens electrónicas;
- R10 - Devem existir procedimentos que assegurem que as mensagens electrónicas com Informação sensível são encriptadas;
- R11 – Deve ser evitada a partilha de Informação e documentos sensíveis entre sistemas, se estes não possuírem níveis de protecção adequados;
- R12 - Devem ser conhecidos os requisitos e os procedimentos de recuperação antes de partilhar a Informação;
- R13 - Deve ser garantido que os donos dos recursos documentam e identificam explicitamente a sensibilidade/criticidade dos seus sistemas.

As boas práticas com base nos objectivos de controlo e actividades de controlo propostos pelo ISACA no processo COBIT 4.1 - ES5: Garantia de Segurança nos Sistemas (ITGI, 2007b) tendo como objectivos de controlo:

- ES5.11 - Troca de Dados Sensíveis - A troca de dados sensíveis só deve ser efetuada através de um canal seguro ou no mínimo com controlos que garantam a autenticidade do conteúdo, a prova de submissão, prova de recepção e o não repúdio da origem.

e como actividades de controlo:

- ES.5.11.1 – Estabelecer a forma de proteger a informação durante a troca de dados, com base na classificação da informação estabelecida;
- ES.5.11.2 – Implementar controlos adequados para proteger a informação durante a troca de dados;

- ES.5.11.3 – Os controlos implementados para proteger a informação durante a troca de dados devem ter como base a sua classificação e a tecnologia utilizadas.

Anexo J - Estudo de Caso: Diagnóstico da Situação Pós Implementação

Na tabela 28 apresenta-se o questionário da auditoria à situação inicial, que foi baseada no ficheiro de Excel disponibilizado pelo ITIG[77] e tendo como referência o modelo de maturidade proposto pelo ISACA no processo COBIT 4.1 - ME3 (ITGI, 2007) (Secção 2.3.1).

#	Afirmação	Nível de Maturidade	Nível Alinhamento				Tipo de sentença[78]	Mínimo		Valores
			Não Alinhado	Pouco	Bastante	Completamente		Falso	Verdadeiro	
1	Existe uma consciencialização limitada dos Requisitos de Conformidade que afectam os SI/TIC, não existindo um processo para avaliação da *Compliance* com os Requisitos de Conformidade.	0	X				N		X	0
2	Existe uma consciencialização sobre os Requisitos de Conformidade que têm impacto na Organização.	1			X		P		X	2/3
3	São adoptados processos informais para promover a *Compliance* nos casos em que essa necessidade surge em novos projectos, ou como resposta a processos de revisão ou auditoria.	1	X				P	X		0
4	Existe um entendimento da necessidade de aderir aos Requisitos de conformidade e essa necessidade é comunicada.	2			X		P		X	2/3
5	Nas situações em que a *Compliance* é um requisito recorrente como, por exemplo, em requisitos financeiros e legislação sobre privacidade, foram desenvolvidos e são aplicados anualmente procedimentos individuais de conformidade.	2		X			P	X		1/3
6	Não existe uma abordagem padronizada.	2	X				N		X	0
7	Existe uma grande dependência relativamente ao conhecimento e responsabilidades individuais, sendo provável a ocorrência de erros.	2		X			N		X	1/3
8	Existe formação informal sobre os Requisitos de conformidade e de *Compliance*.	2	X				N		X	0
9	Foram desenvolvidos, documentados e comunicados as políticas, planos e procedimentos para assegurar a aderência aos Requisitos de Conformidade . No entanto, alguns destes procedimentos podem não ser sempre seguidos, estarem desactualizados, ou serem impraticáveis de implementar.	3			X		P		X	2/3
10	A monitorização efectuada é limitada e alguns dos requisitos legais podem não estar a ser endereçados.	3			X		N	X		2/3
11	São realizadas acções de formação, sobre os requisitos legais e normativos externos com impacto na Organização e no processo de *Compliance* definido.	3	X				P	X		0

[77] O ITIG disponibiliza mesmo um ficheiro de excel para o devido efeito em www.isaca.org.

[78] Relaciona-se com o sentido da resposta P- positivo e N- negativo, afetando deste modo o valor da maturidade a alcançar.

12	Existem contratos e processos legais padronizados para minimizar os riscos associados a perdas contractuais.	3			X		P		X	2/3
13	Há um total entendimento das questões relacionadas com os Requisitos de conformidade e da necessidade de assegurar a *Compliance* a todos os níveis.	4			X		P		X	2/3
14	Existe um plano de formação formal que assegura que todos os colaboradores estão cientes das suas obrigações de *Compliance*.	4	X				P	X		0
15	Existe um responsável definido pelo processo de *Compliance* e as suas responsabilidades são claras.	4				X	P		X	1
16	O processo de *Compliance* inclui a revisão do ambiente legal para identificar Requisitos de conformidade e respectivas alterações.	4			X		P		X	2/3
17	Há um mecanismo implementado para monitorizar falhas de *Compliance* com Requisitos de Conformidade, reforçar as práticas internas e implementar acções correctivas.	4			X		P		X	2/3
18	As questões de não *Compliance* são analisadas para identificar a origem da situação de forma padronizada, com o objectivo de definir soluções sustentáveis.	4			X		P		X	2/3
19	As práticas internas são utilizadas para necessidades específicas, como regulamentação base e contratos de serviços recorrentes.	4			X		P		X	2/3
20	Encontra-se implementado e reforçado um processo organizado e eficiente de *Compliance* com os Requisitos de Conformidade, assente numa função centralizada, que fornece orientações para toda a Organização.	5			X		P		X	2/3
21	Existe um conhecimento extenso sobre os Requisitos de Conformidade aplicáveis, incluindo tendências futuras, antecipação de alterações e necessidade de novas soluções.	5		X			P	X		1/3
22	A Organização participa em discussões externas com grupos de regulamentação e Indústria, para perceber e influenciar os Requisitos de Conformidade que afectam a Organização.	5			X		P		X	2/3
23	As melhores práticas são desenvolvidas garantindo uma *Compliance* eficaz com os Requisitos de Conformidade, tendo como resultado a existência de poucas excepções de *Compliance*.	5			X		P		X	2/3
24	Existe um sistema corporativo de monitorização centralizada do processo de *Compliance*, permitindo à Gestão documentar o fluxo de informação e avaliar e melhorar a qualidade e eficiência do processo.	5			X		P		X	2/3
25	Encontra-se implementado e alinhado com as melhores práticas um processo de auto-avaliação dos Requisitos de Conformidade.	5		X			P	X		1/3
26	A cultura organizacional de gestão relativamente ao processo de *Compliance* é suficientemente sólida, e o processo correctamente desenvolvido, que permite que as acções de formação sejam aplicadas a um grupo de novos colaboradores e somente quando há alterações significativas ao processo de *Compliance*.	5		X			P	X		1/3

Tabela 28 - Questionário da auditoria à situação pós implementação.

Na tabela 29 apresenta-se o nível de maturidade alcançado, após registo das evidências no questionário da auditoria à situação pós implementação.

Nível de Maturidade	Somas dos Alinhamentos	# Afirmações	Média dos Alinhamentos de Cada Nível de Maturidade	Contribuição Ponderada com a Média dos Níveis de Maturidade	Contribuição Aferida com o Nível de Maturidade
0	0,00	1	0,00	0,00	0,00
1	0,67	2	0,33	0,15	0,15
2	1,33	5	0,27	0,12	0,24
3	2,00	4	0,50	0,22	0,67
4	4,33	7	0,62	0,28	1,10
5	3,67	7	0,52	0,23	1,17
			2,24	**1,00**	**3,33**

Tabela 29 - Nível de maturidade determinado pela auditoria à situação pós implementação.