Universidade do Minho

Escola de Engenharia

Cláudia Patrícia Longras Gomes Silva

Monitorização Contínua dos Controlos

Agosto de 2022

Monitorização Contínua dos Controlos

Cláudia Patrícia Longras Gomes Silva

UMinho | 2022

Universidade do Minho
Escola de Engenharia

Cláudia Patrícia Longras Gomes Silva
(a85246)

Monitorização Contínua dos Controlos

Dissertação de Mestrado
Mestrado integrado em Engenharia e Gestão de Sistemas de Informação

Trabalho efetuado sob a orientação da
Professora Doutora Helena Cristina Coutinho Duarte Rodrigues

Agosto de 2022

Agradecimentos

Finalizando esta etapa, quero deixar um agradecimento a todos os que me acompanharam e apoiaram ao longo destes cinco anos.

Em primeiro lugar, quero agradecer à minha família, sobretudo aos meus pais e irmã, por me terem apoiado e motivado ao longo de todo este percurso, assim como me apoiaram sempre em todas as etapas da minha vida.

Às minhas amigas e vizinhas Alexandra e Adriana com quem partilhei muitos e bons momentos. Espero que tenham muito sucesso ao longo da nossa vida.

Aos meus colegas e amigos que durante o percurso académico compreenderam a frustração dos obstáculos que tínhamos de superar e só com entreajuda conseguíamos ultrapassar essas barreiras.

À minha orientadora, professora Helena Rodrigues, por todo o apoio e disposição para me ajudar.

À equipa da Deloitte, especialmente ao meu orientador Telmo Nabais, por me proporcionarem esta oportunidade, pelo apoio dado e pela partilha de conhecimento. Também quero agradecer pelos desafios novos que me foram colocados, os quais me incentivaram a procurar aprender sempre mais.

DECLARAÇÃO DE INTEGRIDADE

Declaro ter atuado com integridade na elaboração do presente trabalho académico e confirmo que não recorri à prática de plágio nem a qualquer forma de utilização indevida ou falsificação de informações ou resultados em nenhuma das etapas conducente à sua elaboração.

Mais declaro que conheço e que respeitei o Código de Conduta Ética da Universidade do Minho.

Resumo

Monitorização Contínua dos Controlos

Atualmente, existem cada vez mais regulamentos e obrigações legais a serem aplicadas pelas organizações, que dependem da sua localização, indústria e geografia. Para verificar se estão a ser cumpridas as obrigações e regulamentos legais, a organização precisa de criar controlos e executar ativamente a revisão dos mesmos, resultando num aumento da carga de trabalho dos proprietários dos controlos. A solução de monitorização contínua de controlos emergiu da governação, risco e conformidade, ajudando a organização a reduzir a carga sobre os proprietários dos controlos, uma vez que não é preciso de fazer ativamente a revisão dos controlos. Esta solução permite aos proprietários dos controlos realizar mais atividades de valor acrescentado, ajudando a proporcionar melhorias significativas nos processos de negócio. A monitorização contínua de controlos pode ajudar a reduzir custos de conformidade e o risco de erros e fraudes involuntárias.

Para a implementação desta solução foi utilizado o ServiceNow, que fornece uma plataforma de aplicação como um serviço (*aPaaS – Application Platform-as-a-Service*). O ServiceNow fornece uma solução moderna, fácil de utilizar e de gestão de serviços na nuvem, que permite às organizações automatizarem processos manuais e repetíveis, padronizarem a prestação de serviços e concentrarem-se no negócio principal.

O objetivo desta dissertação é avaliar se a plataforma ServiceNow consegue implementar a monitorização contínua de controlos, permitindo ter uma visão integrada e em tempo real dos riscos e controlos empresariais em todos os processos. O resultado final foi positivo e através dele foi possível ter em tempo real o grau de *compliance* de um caso de uso de Gestão de Mudança.

Palavras chave: Governação das TI, Governação, Risco e Conformidade (GRC), Monitorização Contínua dos Controlos, ServiceNow

Abstract

Continuous Controls Monitoring

Currently, there are more and more regulations and legal obligations to be applied by organizations, which depend on their location, industry and geography. To verify that legal obligations and regulations are being met, the organisation needs to create controls and actively review them, resulting in an increase in the workload of the owners of the controls. The continuous control monitoring solution has emerged from governance, risk and compliance, helping the organisation to reduce the burden on control owners as there is no need to actively review controls. This solution enables control owners to perform more value-added activities, helping to deliver significant improvements in business processes. Continuous controls monitoring can help reduce compliance costs and the risk of unintentional errors and fraud.

For the implementation of this solution, ServiceNow was used, which provides an application platform as a service (aPaaS). ServiceNow provides a modern, easy-to-use, cloud service management solution that enables organizations to automate manual and repeatable processes, standardize service delivery, and focus on the core business.

The objective of this dissertation is to assess whether the ServiceNow platform can implement continuous monitoring of controls, enabling an integrated and real-time view of risks and business controls across all processes. The final result was positive and through it was possible to have in real time the compliance score of a Change Management use case.

Keywords: Continuous Controls Monitoring, Governance, Risk and Compliance (GRC), IT Governance, ServiceNow

Índice

Agradecimentos iv
DECLARAÇÃO DE INTEGRIDADE v
Resumo vi
Abstract vii
Lista de Abreviaturas x
1. Introdução 1
1.1. Enquadramento 1
1.2. Objetivos 1
1.3. Metodologia 2
1.4. Estrutura do documento 3
2. Estado da Arte 5
2.1. Governação, Risco e Conformidade (GRC) 5
2.2. Governação das TI 6
2.3. COBIT 8
2.4. Monitorização Contínua dos Controlos 10
3. ServiceNow 15
3.1. Módulo GRC: *Integrated Risk Management* 16
4. Conceptualização do problema a estudar 19
4.1. Critérios 22
5. Trabalho Desenvolvido 24
5.1. Primeira Implementação 26
5.2. Segunda Implementação 28
5.3. Terceira Implementação 29
5.4. Criação de um Issue 29
5.5. Dashboards 31
6. Discussão 33
7. Conclusões 35
8. Referências 36
9. Anexos 37
Código da primeira implementação 37
Código da segunda implementação 40

Script Include IssueUtilsCompliance 43
Business Rule “Create issue when control non-compliant” 45

Lista de Abreviaturas

DSR *Design Science Research*

TI Tecnologias de Informação

GRC Governação, Risco e Conformidade

COBIT *Control Objectives for Information and Related Technology*

P2P *Purchase-to-pay*

ERP *Enterprise Resource Planning*

aPaaS *Application Platform-as-a-Service*

CAB *Change Advisory Board*

ITSM *Information Technology Service Management*

ITOM *Information Technology Operations Management*

ITBM *Information Technology Business Management*

CMDB *Configuration Management Database*

Lista de Figuras

Figura 1 - Modelo de Design Research 2
Figura 2 - Arquitetura do módulo GRC: Integrated Risk Management 17
Figura 3 - Modelo de dados 21
Figura 4 - Diagrama de sequência 22
Figura 5 - Entity Filter 25
Figura 6 - Entity Filter 25
Figura 7 - Entity Type "Change Requests" 25
Figura 8 - Control Objective "Requester cannot be the same as the approver" 26
Figura 9 - Botão "Approve CCM" 27
Figura 10 - Código do botão "Approve CCM" 27
Figura 11 - Entity type Change Requests 28
Figura 12 - Objetivos de controlo 28
Figura 13 - Scheduled Job "GRC Change Request Compliance Monitoring" 29
Figura 14 - Business Rule "Create issue when control non-compliant" 30
Figura 15 - Código da Business Rule "Create issue when control non-compliant" 30
Figura 16 - Controlos do pedido de alteração CHG0030065 30
Figura 17 - Issue IPT0020025 31
Figura 18 - Dashboards 31
Figura 19 - Dashboards 32
Figura 20 - Dashboards 32

1. Introdução

1.1. Enquadramento

Esta dissertação aborda uma solução de monitorização contínua de controlos. A monitorização contínua dos controlos é a utilização de ferramentas automatizadas e de várias tecnologias que ajudam a assegurar a monitorização contínua das transações financeiras e outros tipos de aplicações transacionais. Esta monitorização melhora a postura geral de conformidade e reduz os custos e o tempo de regresso a uma situação de conformidade no caso de uma não conformidade (Deloitte, 2018).

Segundo Deloitte (2018), com a monitorização contínua dos controlos é possível ter uma avaliação contínua da postura de conformidade, auditorias eficientes e eficazes em termos de custos, revisão pró-ativa e uma monitorização a 100% das transações permitindo às organizações terem conhecimento sobre as transações existentes, reduzirem os custos desnecessários, antecipar problemas e possíveis ameaças livrando-se delas e evitando períodos de indisponibilidade. A monitorização contínua de controlos ajuda a organização a reduzir perdas de negócio por fraude ou falhas em seguir regras que regem as transações financeiras e proporciona à gestão uma visão acionável que permite análises mais aprofundadas que podem ajudar a gestão a tomar decisões corretas (Teeter, R. A., Brennan, G., Alles, M. G., & Vasarhelyi, M. A., 2008).

Hoje em dia, as empresas estão a passar de uma solução de monitorização contínua de controlos baseada em regras de *reporting* dependentes da perceção da pessoa para uma solução que de forma dinâmica toma estas perceções e aciona respostas em tempo real o que permite uma mudança comportamental em toda a empresa.

1.2. Objetivos

De forma que as organizações alcancem uma visão integrada e em tempo real dos riscos e controlos empresariais em todos os processos e aplicações empresariais deve ser aplicada a solução de monitorização contínua de controlos. Com esta solução é possível ter uma perspetiva empresarial dos controlos ao mesmo tempo que aumenta a eficiência, eficácia e agilidade na gestão dos controlos internos. A Deloitte escolheu a plataforma ServiceNow para ser aplicada a monitorização contínua de

controlos visto ser uma plataforma em crescimento no mercado. O objetivo desta dissertação é avaliar se o ServiceNow, como plataforma, consegue implementar uma solução de monitorização contínua de controlos, verificando o grau de *compliance* em tempo real (o mais perto possível de tempo real) de um conjunto de processos dentro da organização.

De modo a atingir o objetivo proposto, serão realizadas as seguintes tarefas:

1. Instanciar um processo conhecido de Governação das TI em ServiceNow;
2. Implementação de um processo de avaliação de *compliance* sob um processo de TI em ServiceNow usando o módulo de GRC (Governação, Risco e Conformidade)
3. Automatizar em ServiceNow as avaliações de *compliance* de um processo

1.3. Metodologia

A metodologia de investigação escolhida para o desenvolvimento da dissertação foi o *Design Science Research (DSR)*. Esta abordagem cumpre três objetivos, são eles a consistência associada com a literatura anteriormente analisada, fornecer um modelo de processo nominal para fazer DSR e fornecer um modelo mental para apresentar e avaliar investigações feitas na área dos Sistemas de Informação (SI). Segundo o artigo de 2007, dos autores Ken Peffers, Tuure Tuunanen, Marcus A. Rothenberger e Samir Chatterjee, o processo inclui seis passos, representados na figura 1 e explicados de seguida.

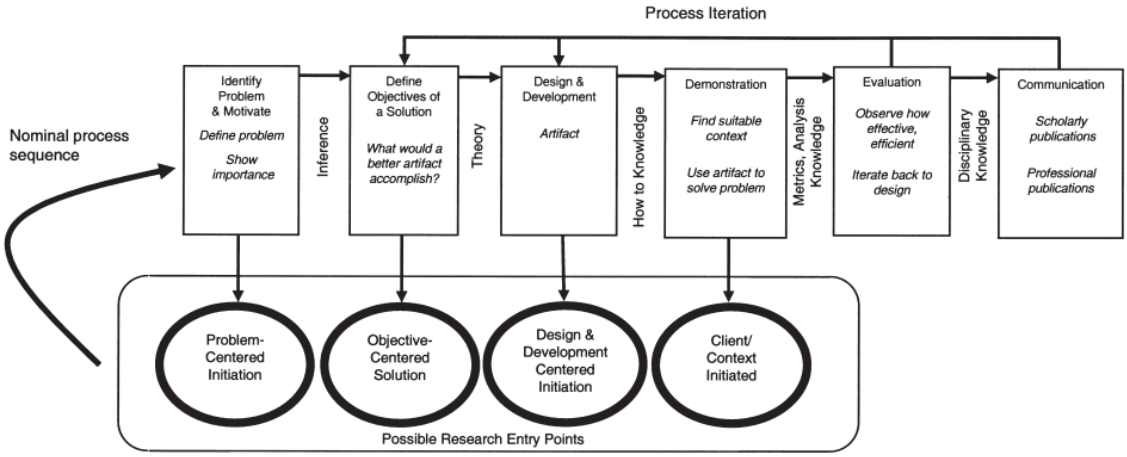

Figura 1 - Modelo de Design Research

1. **Identificação do problema e motivação** – define o problema específico de investigação e justifica o valor da solução. A definição do problema será utilizada para a criação de um artefacto que possa efetivamente fornecer uma solução.
2. **Definir os objetivos de uma solução** – inferir os objetivos da solução a partir da definição do problema e do conhecimento do que é possível e viável.

3. **Conceção e desenvolvimento** – criação do artefacto. Um artefacto de investigação de *design* pode ser qualquer objeto de *design* em que uma contribuição de investigação está incorporada no *design*. Também inclui a determinação da funcionalidade desejada do artefacto e da sua arquitetura e depois a criação do artefacto.
4. **Demonstração** – demonstrar a utilização do artefacto para a resolução de uma ou mais instâncias do problema. Isto pode envolver a sua utilização em experiências, simulações, casos de estudo ou outras atividades.
5. **Avaliação** – observar e medir o quão bem o artefacto suporta a solução para o problema. Esta atividade envolve a comparação dos objetivos da solução com os resultados observados do artefacto. É necessário ter conhecimento das métricas relevantes e técnicas de análise.
6. **Comunicação** – comunicar o problema e a sua importância, o artefacto, a sua utilidade e novidade, o rigor da sua conceção e a sua eficácia aos investigadores e outros públicos relevantes.

1.4. Estrutura do documento

O seguinte documento está dividido em sete capítulos, sendo eles o capítulo introdutório ao projeto, o estado da arte, a plataforma ServiceNow, conceptualização do problema a estudar, trabalho desenvolvido e por último as conclusões.

No primeiro capítulo, é feita a introdução desta dissertação, onde é feito o enquadramento relativo ao tema de investigação. É neste capítulo que se define a finalidade, objetivos, a abordagem metodológica e a estrutura do presente documento.

No segundo capítulo faz-se o enquadramento conceptual e apresentam-se os resultados do estado da arte, expondo os principais conceitos relevantes para a dissertação, nomeadamente, governação, risco e conformidade, governação das TI, COBIT e monitorização contínua de controlos.

No terceiro capítulo é apresentada a plataforma a utilizar para implementar a solução de monitorização contínua de controlos.

O quarto capítulo é a conceptualização do problema a estudar, sendo descrito o caso de uso em que a solução de monitorização contínua de controlos será aplicada.

No quinto capítulo é demonstrado como se desenvolveu a solução.

No sexto capítulo apresenta a discussão sobre o trabalho desenvolvido tendo em conta o objetivo da dissertação

No sétimo capítulo são apresentadas as conclusões da dissertação tendo em conta os resultados obtidos no sexto capítulo.

Finalizando os capítulos, surgem as referências bibliográficas que foram utilizadas durante a dissertação e os anexos.

2. Estado da Arte

2.1. Governação, Risco e Conformidade (GRC)

Governação, Risco e Conformidade (GRC) consiste numa estratégia que envolve a integração dos processos de uma empresa de maneira clara, unificada e segura. Esta estratégia tem como finalidade ajudar todas as partes interessadas a colaborar eficazmente, reduzir o risco global de negócio, garantir uma melhor conformidade e estabelecer vantagens competitivas no mercado (Gericke, A., Fill, H. G., Karagiannis, D., & Winter, R., 2009). GRC está assente em três conceitos, e cada um engloba um processo fundamental para regular a estrutura e atividades que a empresa deve executar como parte da realização de negócios.

A governação é um conjunto de políticas, leis, cultura e instituições que definem como uma organização deve ser gerida. Este processo também define papéis e expetativas de vários níveis de gestão e não-gestão. A gestão de risco é a coordenação de atividades que controlam uma organização, prevendo e gerindo os riscos que possam ter um impacto negativo no negócio. O processo de gestão de risco procura identificar, avaliar e medir o risco para em seguida desenvolver contramedidas para lidar com ele. Além disso, verifica a implementação das medidas de controlo utilizadas para reduzir o risco a um nível aceitável. Este processo coloca a organização numa posição em que não precisa de reagir a um problema depois de este ter ocorrido. A gestão de risco é um processo pró-ativo contínuo. A conformidade é o ato de aderir às leis, regulamentos, políticas, procedimentos corporativos e controlos de segurança internos. Antigamente, a conformidade de controlo de segurança era opcional, mas nos dias atuais é necessária para a realização de negócios. Atualmente, muitas organizações não assinam contratos com outras organizações que não oferecem provas de conformidade (Long, G., 2017).

As empresas, consultorias e fornecedores de *software* têm repensado abordagens convencionais devido ao crescente número de leis e regulamentos, ao aumento dos riscos com que as organizações têm de lidar e as crescentes preocupações de governação (Racz, N., Weippl, E., & Seufert, A., 2011).

As organizações que estão a integrar GRC têm atingido um melhor alinhamento dos objetivos com a missão, visão e valores da organização, melhor agilidade e confiança na tomada de decisões, desempenho sustentado e fiável, alocação de capital para as iniciativas certas no momento certo, responsabilidade de cima para baixo para objectivos-chave, riscos, requisitos e iniciativas relacionadas e redução significativa de custos dentro das capacidades integradas (Long, G., 2017).

Um processo eficaz de GRC pode ajudar uma empresa a transformar as suas operações de negócio e pode fazer previsões mais detalhadas sobre os seus processos de negócio. O principal impulsionador do negócio em questão é a capacidade de gerir a informação de ativos, comprovar a conformidade com as obrigações e regulamentos legais aplicáveis, reduzir o risco de processos judiciais, reduzir os custos de armazenamento, e comprovar a responsabilidade empresarial (Handoko, B. L., Riantono, I. E., & Gani, E., 2020).

2.2. Governação das TI

A governação das TI representa o quadro dos direitos e responsabilidades de decisão implementado através de processos, estruturas e mecanismos relacionais que permitem assegurar o alinhamento das atividades relacionadas com as TI com a estratégia e objetivos da organização (Riemer, K., Ciriello, R., Peter, S., & Schlagwein, D., 2020). Segundo P. Webb, C. Pollard e G. Ridley (2006), a governação das TI tem como objetivo assegurar que o desempenho das tecnologias de informação (TI) cumpre os seguintes pontos:

- As TI têm de estar alinhadas com a organização e realizar os benefícios prometidos.
- As TI têm de permitir à empresa explorar as oportunidades e maximizar os benefícios.
- Os recursos informáticos têm de ser utilizados de forma responsável.
- Os riscos relacionados com as TI têm de ser geridos adequadamente.

A governação das TI possui três dimensões fundamentais que traçam de perto a sua definição (Gregory, R. W., Kaganer, E., Henfridsson, O., & Ruch, T. J., 2018):

1) Foco da governação das TI (o que governar), que se refere a que atividades e artefactos relacionados com TI devem ser alinhados com a estratégia e objetivos organizacionais.
2) Âmbito da governação das TI (quem deve governar), que se refere aos intervenientes e partes interessadas que são responsabilizados por assegurar a contribuição de TI para a organização.
3) Padrões da governação das TI (como governar), que se refere aos mecanismos que são criados para assegurar atividades e resultados "desejáveis" relacionados com TI.

As organizações precisam de uma abordagem apropriada de governação das TI para acompanhar as mudanças nos seus ambientes legais e regulamentares, assegurar o cumprimento da regulamentação e assegurar a conformidade regularmente.

Ao conceber a governação das TI para uma organização, é importante reconhecer que esta está dependente de uma variedade de fatores internos e externos por vezes conflituosos. Determinar a combinação certa de mecanismos é um esforço complexo e deve ser reconhecido que o que funciona para uma organização pode não funcionar para outra. Isto significa que diferentes organizações podem precisar de uma combinação de diferentes estruturas, processos e mecanismos relacionais. As estruturas envolvem a existência de funções responsáveis, tais como executivos de tecnologias de informação e uma diversidade de comités de TI. Os processos referem-se a tomadas de decisões estratégicas e à monitorização. Os mecanismos relacionais incluem a participação empresarial ou TI, diálogo estratégico, conhecimento partilhado e comunicação adequada (De Haes, S., & Van Grembergen, W., 2004).

Segundo ISACA (2018), uma adoção bem-sucedida da governação das TI tem os seguintes resultados.

- **Realização de benefícios** - consiste em criar valor para a empresa através das TI, aumentar o valor derivado dos investimentos existentes em TI, e eliminar iniciativas e ativos de TI que não estão a criar valor suficiente. O valor que as TI oferecem deve estar alinhado com os valores nos quais o negócio está focado. Também deve ser medido de forma a mostrar o impacto e as contribuições dos investimentos habilitados para TI no processo de criação de valor da empresa.
- **Otimização de riscos** - implica abordar o risco de negócio associado ao uso, propriedade, envolvimento, influência e adoção de TI dentro de uma empresa. O risco de negócio relacionado com as TI consiste em eventos que envolvam as TI que podem ter potencial impacto no negócio. O risco deve ser medido de forma a mostrar o impacto e as contribuições da otimização do risco de negócio relacionado com as TI na preservação do valor.
- **Otimização de recursos** - garante que as capacidades adequadas para executar o plano estratégico estão em vigor e são fornecidos recursos suficientes, adequados e eficazes. A otimização de recursos garante que é fornecida uma infraestrutura de TI integrada e económica, novas tecnologias são introduzidas conforme exigido pelo negócio, e os sistemas desatualizados são atualizados ou substituídos. Também se foca em fornecer formação, promover a retenção e garantir a competência do pessoal chave das TI. Os dados e informações são um recurso importante por isso explorá-los para obter o melhor valor é outro elemento-chave da otimização de recursos.

Por exemplo, em 2020, Kai Riemer, Raffaele Ciriello, Sandra Peter e Daniel Schlagwein publicaram um artigo sobre a governação das TI para a ação coletiva em nível social da adoção do rastreio digital de

contatos na pandemia COVID-19. O rastreio digital de proximidade por *bluetooth-enabled* é uma medida para travar a propagação pandémica da SARS-CoV-2 ao mesmo tempo preservando a privacidade individual. Esta solução apenas funciona eficazmente se for adotada em toda a sociedade, o que traz o problema de ação coletiva, isto é, todos beneficiariam de um rastreio de proximidade generalizado, mas os benefícios individuais são indiretos e limitados. Para facilitar a ação coletiva a nível da sociedade, o artigo conceptualiza o espaço de opção das ações de governação de TI para a adoção da localização de proximidade ao longo de duas dimensões. Essas duas dimensões são as entidades decisórias, quem irá governar a implementação, e a aplicação da responsabilização, com que rigor será aplicada a adoção e utilização.

O artigo mostra que não existem abordagens globalmente ideais, mas apenas contextualizadas localmente que dependem do risco sanitário imediato, da experiência anterior com pandemias, dos valores sociais e da cultura nacional, do papel do governo, da confiança no governo e da confiança na tecnologia em cada sociedade.

2.3. COBIT

O COBIT (*Control Objectives for Information and Related Technology*) é uma *framework* de gestão de tecnologias de informação (TI) desenvolvida para ajudar as organizações a desenvolver, organizar e implementar estratégias relacionadas com a gestão e governação de informação. Tem como objetivo acrescentar valor à empresa, satisfazendo o interesse dos acionistas pois é utilizado como um meio para otimizar os investimentos de TI.

COBIT faz distinção entre governação e gestão, visto que englobam diferentes atividades, precisam de diferentes estruturas organizacionais e servem diferentes propósitos. Governação assegura que as necessidades, condições e opções das partes interessadas são avaliadas para determinar objetivos empresariais equilibrados e acordados, a direção é definida através da priorização e tomada de decisão, e o desempenho e conformidade são monitorizados contra a direção e objetivos acordados. A gestão planeia, constrói, executa e monitoriza atividades em alinhamento com a direção definida pelo órgão de governação, para alcançar os objetivos da empresa.

Segundo ISACA (2018) uma *framework* de governação deve seguir os seguintes princípios.

1. Deve ser baseada num modelo conceptual, identificar os componentes chave e as relações entre esses componentes, para maximizar a consistência e permitir a automatização.

2. Deve ser aberta, flexível e permitir a adição de novos conteúdos e a capacidade de abordar novas questões da forma mais flexível, mantendo ao mesmo tempo a integridade e a consistência.
3. Deve alinhar-se com as normas, quadros e regulamentos relevantes relacionados.

A *framework* foca-se em objetivos de controlo específicos e detalhados que foram classificados em cinco grandes domínios. Os objetivos de governança estão agrupados no domínio **Avaliar, Dirigir e Monitorizar**, que define as responsabilidades da alta direção para a avaliação, direcionamento e monitorização da utilização das TI para a criação de valor. Os objetivos de gestão estão agrupados nos outros quatro domínios:

- **Alinhar, Planear e Organizar** - Descreve como a utilização de TI ajuda a empresa a atingir os seus objetivos e metas. Administra o uso de táticas e estratégias para planear, comunicar e gerir as diferentes perspetivas em toda a organização.
- **Construir, Adquirir e Implementar** - As soluções de TI precisam de ser identificadas, desenvolvidas ou adquiridas para a concretização da estratégia de TI da organização. Abrange a implementação e integração destas soluções nos processos de negócio, assim como as alterações e manutenções nos sistemas existentes.
- **Entrega, Serviço e Suporte** - Foca-se na entrega da tecnologia da informação, assim como os processos de suporte permitindo a execução de forma eficiente e efetiva. Responsável também pela identificação e atribuição de custos e pela formação dos utilizadores.
- **Monitorizar e Avaliar** - Tem como objetivo monitorizar e avaliar regularmente a qualidade e cumprimento dos requisitos de controlo para todos os processos de informação.

Para satisfazer os objetivos de gestão e governação, uma empresa precisa estabelecer, adaptar e sustentar um sistema de governação construído a partir de uma série de componentes. Os componentes são fatores que contribuem para boas operações do sistema de governação da empresa sobre as TI e que interagem entre si, resultando num sistema de governação holístico para as TI.

- **Processos** - descreve um conjunto organizado de atividades e práticas para atingir determinados objetivos e produzir resultados que apoiem a realização de objetivos globais relacionados com as TI.
- **Estruturas organizacionais** - são as principais entidades que tomam decisões numa empresa.
- **Princípios, políticas e *frameworks*** - traduzem o comportamento desejado em orientação prática para a gestão do dia-a-dia.

- **Informação** - inclui toda a informação produzida e utilizada pela empresa. O COBIT centra-se na informação necessária para o funcionamento eficaz do sistema de governação da empresa.
- **Cultura, ética e comportamento** - quer do indivíduo ou da empresa são muitas vezes subestimados como fatores no sucesso das atividades de governação e gestão.
- **Pessoas, *skills* e competências** - são necessárias para boas decisões, execução de ações corretivas e conclusão bem-sucedida de todas as atividades.
- **Serviços, infraestruturas e aplicações** - incluem infraestruturas, tecnologia e aplicações que fornecem à empresa o sistema de governação para processamento de TI.

2.4. Monitorização Contínua dos Controlos

O aparecimento de tecnologias de análise de dados abriu oportunidade para as soluções de monitorização contínua de controlos. A monitorização contínua dos controlos é uma solução, emergente de governação, risco e conformidade (GRC), que utiliza ferramentas automatizadas e várias tecnologias que ajudam a assegurar a monitorização contínua das transações financeiras e outros tipos de aplicações transacionais.

A automatização dos controlos significa que o gestor não tem de executar ativamente a revisão e só é alertado quando necessário, com revisões subsequentes baseadas apenas em exceções. Isto reduz a carga sobre o proprietário do controlo e permite-lhe realizar mais atividades de valor acrescentado, podendo assim também ajudar a proporcionar melhorias significativas nos processos de negócio. É necessário automatizar os controlos para que estes possam ser incluídos numa solução de monitorização contínua de controlos (Hunt, R., & Jackson, M., 2010).

Uma solução de monitorização contínua de controlos pode ajudar a reduzir custos de conformidade, reforçar o controlo ambiente e reduzir o risco de erros e fraudes involuntárias. Também pode melhorar as operações do processo empresarial. Atualmente, a gestão e as partes interessadas exigem total precisão e integridade nos relatórios financeiros, por isso o não cumprimento não é uma opção viável. A monitorização contínua fornece um método eficiente e rentável para atingir este objetivo (Hunt, R., & Jackson, M., 2010).

Alguns benefícios da implementação desta solução são a automatização de controlos manuais previamente efetuados, eliminação de testes de controlos excessivos, manter a conformidade com um ou mais regulamentos, permitir que os resultados dos testes sejam reutilizáveis em múltiplos quadros

de conformidade, minimização do risco de perdas empresariais através de erros não intencionais ou atividades fraudulentas maliciosas, comunicando falhas de controlo à medida que acontecem e proporcionar um retorno do investimento através da melhoria das operações do processo empresarial (Hunt, R., & Jackson, M., 2010).

Alguns desafios para a solução de monitorização contínua dos controlos e como se deve lidar com eles são (Deloitte, 2018):

- Múltiplas fontes de dados e pobre qualidade de dados. Deve ser tomado especial cuidado para entender os dados de múltiplas fontes e armazená-los num espaço comum removendo redundâncias para uma comunicação fácil.
- Incapacidade de identificar um caso de negócio forte para uma solução monitorização contínua dos controlos. Os requisitos detalhados, incluindo o âmbito de aplicação, devem ser elaborados como parte do plano. Todos os *stakeholders* fundamentais têm de ser identificados e confiados antes de construírem a solução.
- Para assegurar a integralidade e precisão dos relatórios e *dashboards* da solução monitorização contínua dos controlos. A solução deve ser desenvolvida e mantida tendo em conta a importância de garantir a integralidade e a precisão dos *dashboards* e relatórios utilizados por vários utilizadores desta solução. Isto incluirá operações comerciais, gestão e auditores.

Um exemplo da implementação da solução de monitorização contínua de controlos foi executado pela empresa global de bioterapia e biotecnologia Premier Plasma Center com o objetivo de detetar fraquezas de controlos internos, erros e potenciais fraudes nas transações financeiras. Em primeiro lugar, a empresa começou por identificar quais as áreas mais críticas com necessidade de controlos internos reforçados. Madison Morgan, chefe executivo de auditoria, liderou a implementação da monitorização contínua de controlos e identificou o ciclo compra a pagar (*Purchase-to-pay, P2P*), que se refere aos processos de negócio que cobrem atividades de requisição, compra, recebimento, pagamento e contabilidade de bens e serviços, como prioridade máxima devido ao seu elevado risco de fraude. A empresa Premier identificou a ACL Analytics Exchange, conhecida pela sua liderança nas áreas de auditoria e gestão de risco, como a melhor solução para fornecer à empresa os recursos necessários para introduzir a sua tecnologia de monitorização contínua em todos os processos de negócio importantes. A ACL Services Ltd trabalhou com a direção, Madison, e a equipa de auditoria interna para desenvolver métricas personalizadas para cada elemento de testes P2P. A implementação da

monitorização contínua de controlos demorou cerca de um ano e beneficiou a Premier. Alguns dos resultados significativos da implementação são:

- Uma melhor responsabilização e uma gestão do controlo dos riscos da informação e da sua compreensão,
- Proteção acrescida dos fluxos de caixa significativos devido à monitorização automatizada e à aplicação das políticas,
- Melhor dissuasão da fraude devido a uma deteção mais rigorosa da fraude,
- Reforço das relações com os fornecedores, criando procedimentos mais eficazes,
- Controlos estabilizados,
- Controlos melhorados em todas as funções,
- Minimização do risco inerente,
- Uma maior capacidade de adaptação ao plano de auditoria a realizar em tempo real, resultando numa melhoria dos custos.

A automatização permite facilitar a manutenção e a supervisão dos controlos. Portanto, o objetivo final de Premier é continuar a estabelecer mais controlos que sejam eficientes e eficazes.

Outro exemplo da implementação da solução foi executado por Michael Alles, Gerard Brennan, Alexander Kogan, Miklos A. Vasarhelyi na Siemens Corporation, que presta serviços de auditoria interna de TI. Uma auditoria de TI é realizada periodicamente para fornecer uma avaliação de risco e testar os controlos dos sistemas ERP.

Os auditores internos seguiam um plano de auditoria que era composto por aproximadamente 300 folhas de ação de auditoria. Cada folha identificava objetivos de controlo e descrevia verificações e testes que deveriam ser realizados para verificar se os controlos internos estavam em vigor e funcionavam corretamente no sistema ERP. Esses testes incluíam entrevistas a utilizadores, avaliação de documentação e políticas, verificação do acesso dos utilizadores a áreas específicas do ERP, e verificação da separação de funções para determinadas funções (Teeter, R. A., Brennan, G., Alles, M. G., & Vasarhelyi, M. A., 2008).

A equipa de auditoria passava cerca de 70 dias a passar manualmente tabelas e pedidos de autorização no âmbito do sistema ERP. Para ajudar a equipa da Siemens, uma ferramenta analítica própria extraia informações das tabelas do ERP e apresentava os resultados dos testes de controlo individuais aos auditores para uma pequena parte dos testes. Os resultados de cada teste eram utilizados como prova

de que o sistema cumpria ou não cumpria os requisitos de certificação (Teeter, R. A., Brennan, G., Alles, M. G., & Vasarhelyi, M. A., 2008).

Antes de implementar a monitorização contínua de controlos os investigadores avaliaram e classificaram os requisitos de auditoria presentes na folha de ação de auditoria em graus de automatização. Depois criaram regras automatizadas baseadas nos requisitos. Antes e durante a implementação das regras de monitorização contínua de controlos realizaram uma avaliação para determinar quais os processos de auditoria presentes na folha de ação de auditoria poderiam ser formalizados e automatizados. Os testes utilizados no programa de auditoria de Siemens eram classificados em pelo menos numa das seguintes categorias (Teeter, R. A., Brennan, G., Alles, M. G., & Vasarhelyi, M. A., 2008):

- Autorização – testes utilizados para determinar que utilizadores estavam autorizados a manter certas funções no sistema ERP.
- Configuração – testes que consultaram o sistema para verificar se as definições refletiam as políticas da empresa.
- Separação de funções – identificavam os utilizadores que tinham acesso a ecrãs ou relatórios que estavam em conflito com os controlos de separação de funções.
- Transações – testes utilizados para verificar se as transações que apareciam numa tabela eram apropriadas e também verificar a frequência de códigos de transação específicos.
- Perceção da atividade do utilizador – testes que testavam os registos de auditoria avaliados para determinar os padrões de comportamento dos utilizadores no sistema. Estes testes verificavam se a atividade do utilizador se enquadrava dentro de uma gama normal de funções.
- Linha de base – testes que verificavam as alterações feitas às tabelas que se esperava terem valores estáticos, tais como Empresas e Área de Controlo. Destes testes resultaram relatórios sempre que estas tabelas eram alteradas.
- Manual – testes que consistiam em entrevistas e verificações de documentos que deviam ser realizados pelo auditor.

A implementação de uma instância da plataforma de monitorização contínua de controlos foi feita juntamente com os servidores de produção e de recursos humanos. Os servidores da monitorização contínua de controlos armazenaram diariamente *snapshots* dos servidores de produção e de recursos humanos e permitiram a captação de regras e testes de relatórios através de uma *interface Web*. No sistema foram atribuídos números e nomes de regras correspondentes aos objetivos da folha de ação de auditoria. As regras foram agrupadas em conjuntos de regras com base no módulo a que pertenciam.

Quando todas as regras de um módulo eram concluídas, todo o conjunto de regras era executado e os resultados eram comparados com os resultados da auditoria de TI. Quando as regras eram criadas e testadas passavam para a reengenharia dos testes de controlo. Nos casos em que os resultados da automatização não correspondiam aos resultados da extração manuais, as regras eram reavaliadas. As regras bem sucedidas eram indicadas na folha de cálculo e no final foi compilada uma lista de regras automatizadas e manuais (Teeter, R. A., Brennan, G., Alles, M. G., & Vasarhelyi, M. A., 2008).

3. ServiceNow

ServiceNow é construído sobre os alicerces fortes da Now Plataform que ajuda a reduzir a complexidade dos processos, transformando formas de trabalho manuais e antigas em fluxos de trabalho digitais modernos. A Now Plataform fornece uma plataforma de aplicação como um serviço (*aPaaS – Application Platform-as-a-Service*), significa que é um modelo informático baseado em nuvem que fornece a infraestrutura necessária para desenvolver, executar e gerir aplicações de um domínio específico. As aplicações que funcionam na Now Plataform utilizam um único sistema de registo e um modelo de dados comum para consolidar os processos empresariais das organizações (ServiceNow, 2022).

O ServiceNow fornece uma solução moderna, fácil de utilizar e de gestão de serviços na nuvem, permitindo às organizações automatizar processos manuais e repetíveis, padronizar a prestação de serviços e concentrar-se no negócio principal. O ServiceNow oferece tudo isto a partir de uma *interface* de utilizador configurável baseada na *web*, construída sobre um modelo de dados flexível. Este serviço é especializado em gestão de serviços de TI (ITSM), gestão de operações de TI (ITOM) e gestão de negócios de TI (ITBM) (ServiceNow, 2022).

As aplicações entregues pelo ServiceNow estão divididas em quatro fluxos de trabalho diferentes:

- Fluxos de trabalho em TI – Este fluxo de trabalho une as tecnologias de informação, gestão de riscos e operações de segurança numa única plataforma e também fornece serviços modernos e resilientes alinhados com as prioridades centradas no cliente. Com este fluxo de trabalho a organização pode otimizar as operações de serviço de TI, alinhar os investimentos com prioridades e gerir o risco, a segurança e o custo.
- Fluxos de trabalho dos empregados – Este fluxo de trabalho permite a organização aumentar o envolvimento e produtividade dos colaboradores, gerir um local de trabalho seguro e eficiente e aumentar a eficiência operacional.
- Fluxos de trabalho do cliente – Os fluxos de trabalho do cliente permitem estender o serviço para além do centro de contacto e das operações de escala automatizando o trabalho em todos os departamentos. Com as aplicações deste fluxo é possível capacitar os clientes com *self-service* personalizado, dar visibilidade aos agentes para antecipar as necessidades dos clientes e otimizar o serviço de campo.

- Fluxos de trabalho do criador – Com este fluxo de trabalho é possível criar experiências intuitivas que os utilizadores adoram e ativar aplicações interempresas e de baixo código que fornecem serviços ágeis em escala.

A arquitetura da Now Plataform cuida de todos os requisitos de infraestrutura das aplicações, tais como disponibilidade de serviços, *backups* e segurança. Isto permite à organização concentrar-se na construção, execução e gestão de grandes aplicações (ServiceNow, 2022).

Existem três maneiras de interagir com Now Plataform, em que cada uma proporciona uma *interface* diferente que direciona diferentes dispositivos e propósitos e todas acedem o mesmo sistema único de registo e modelo de dados comum da Now Plataform. As três *interfaces* da Now Plataform são:

- Next Experience Unified Navigation
- Now Mobile App
- Service Portal

A *interface* Next Experience Unified Navigation é a principal forma de interagir com as aplicações e a informação numa instância ServiceNow por isso foi utilizada nesta dissertação.

3.1. Módulo GRC: *Integrated Risk Management*

O ServiceNow tem vários módulos disponíveis que permitem personalizar as aplicações que são desenvolvidas. Um desses módulos é o *GRC: Integrated Risk Management,* permitindo às organizações incorporar gestão de risco, atividade de conformidade e automatização inteligente em processos de negócio digitais para monitorizar e priorizar continuamente o risco. Com este módulo a organização tem uma visão integrada de como gere o seu conjunto único de riscos permitindo melhorar a tomada de decisões e o desempenho da mesma (ServiceNow, 2022).

Com o GRC, as organizações têm uma melhor visibilidade das atividades que estão em alto risco e em não-conformidade, isto é possível utilizando a monitorização contínua e a gestão da continuidade do negócio. O módulo ajuda as organizações a melhorar o desempenho, evitando interrupções de trabalho incorporando a gestão de risco em atividades interfuncionais automatizadas e também permite reduzir erros e custos, ao mesmo tempo que aumenta o foco em tarefas de valor mais elevado. Outro benefício do módulo é a comunicação do risco de forma eficaz, uma vez que simplifica e acelera o reporte a todos

os níveis com *insights* em tempo real e *dashboards* que integram informação sobre risco e resiliência (ServiceNow, 2022).

Para implementar a solução de monitorização contínua de controlos é necessário instalar este módulo na instância do ServiceNow e perceber como funciona a arquitetura do mesmo. Na figura seguinte está representada a arquitetura do módulo *GRC: Integrated Risk Management* (ServiceNow, 2022).

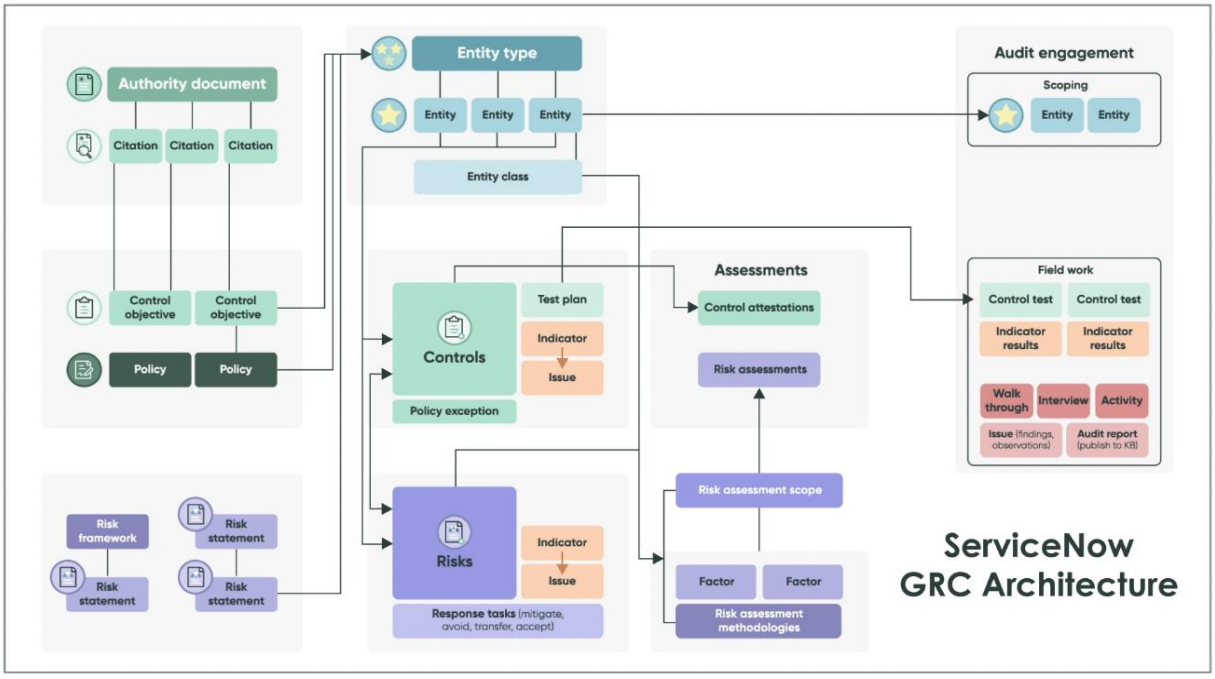

Figura 2 - Arquitetura do módulo GRC: Integrated Risk Management

Na tabela *Authority Document* são armazenados documentos que consistem normalmente em parágrafos descrevendo atividades que uma organização deve fazer para se manter em conformidade. Os registos da tabela *Policies* ajudam a definir a cultura da empresa, como o acesso a instalações, diversidade, segurança, ou sustentabilidade. Estes registos também ajudam as organizações a cumprir os regulamentos. Um registo da tabela *Citations* define uma secção de um *authority document* a que uma organização deve obedecer. A tabela *Control Objectives* guarda registos que podem ser objetivo, norma ou direção que funciona como orientação para as interações e operações da empresa. *Authority Document* e *Citations* catalogam requisitos externos na organização enquanto *Policies* e *Control Objective* documentam como a organização está a lidar com esses requisitos.

Um *Risk statemet* ajuda a definir o impacto para a organização se um risco ocorrer. *Risk framework* é considerado um grupo de *risk statement*. As tabelas *Entity Type, Entity* e *Entity Class* representam as pessoas, ativos, processos de negócio, localizações ou coisas que são utilizadas para gerir controlos e riscos. Os registos da tabela *Entity Type* são aplicados a *risk statements* e *control objectives*, gerando

registos adicionais, que são guardados nas tabelas *Risks* e *Controls*. Depois de serem gerados os controlos paras as *entities*, os proprietários dos controlos precisam validar que um controlo é implementado antes de avaliar a sua eficácia. Para verificar se um controlo foi implementado são criados *control attestation,* que são inquéritos que reúnem provas para provar que um controlo é implementado. Os registos da tabela *Indicators* são utilizados para medir se um controlo é eficaz ou não, são os passos manuais ou automatizados executados para medir a eficácia do processo, sistema, ou método identificado no *control attestation*.

Os *control tests* podem fazer parte de uma auditoria ou de um processo de conformidade utilizado para validar se o método de controlo é efetivamente concebido e operacionalmente eficaz. Na tabela *Issues* são guardadas as tarefas que permitem aos utilizadores finais acompanhar a resposta para remediar ou aceitar o problema. Estes registos podem ser gerados pelo sistema ou criados manualmente e podem incluir eventos de risco operacional, violações de conformidade regulamentar, violações de segurança, ou quaisquer outros resultados negativos.

4. Conceptualização do problema a estudar

O problema a estudar nesta dissertação consiste na avaliação do ServiceNow para implementar a monitorização de controlos de uma organização continuamente, comprovando a conformidade da mesma com as obrigações e regulamentos legais aplicáveis em tempo real. Numa altura em que existem cada vez mais regulamentos que as organizações precisam de aplicar, é indispensável controlar se estes estão a ser cumpridos. Para tal, a implementação de uma solução de monitorização contínua de controlos é importante numa organização, visto que ajuda a mesma a monitorizar automaticamente e em tempo real (ou numa aproximação de minutos) os controlos, mantém a conformidade com os regulamentos e minimiza o risco de perdas e atividades de fraude.

O caso de uso que será implementado é o caso de uso de gestão de mudança no contexto de TI. A gestão de mudança proporciona uma abordagem sistemática para controlar o ciclo de vida de todas as alterações ao ambiente de operações de produção desde o início até à sua conclusão. O objetivo do processo da gestão de mudança é permitir que sejam feitas alterações benéficas com a interrupção mínima das operações comerciais, garantindo assim a manutenção dos melhores níveis possíveis de qualidade e disponibilidade do serviço. Deve ser aplicada uma abordagem consistente à avaliação de riscos, à continuidade do negócio, ao impacto da mudança, aos requisitos de recursos e à aprovação de alterações. A abordagem deve manter o equilíbrio adequado entre a necessidade de uma mudança e o calendário da sua integração no ambiente vivo. O âmbito do caso de uso inclui:

- alterações dos utilizadores que envolvam a manutenção de infraestruturas que necessitam de uma alteração ou substituição de *hardware* ou *software*,
- alterações de utilizadores que envolvam resolução ou recuperação de um ou mais serviços que tenha um incidente aberto e exigirá uma alteração ou substituição de *hardware* ou *software*,
- alterações nos serviços, processos, *hardware* ou *software* considerados na produção ou itens de configuração que são geridos na base de dados de gestão de configuração (*Configuration Management Database – CMDB*),
- introdução de novos itens de configuração ou serviços na produção.

Este caso de uso é iniciado pela solicitação de um pedido de alteração. Um pedido de alteração consiste em informação detalhada da alteração, como a razão da alteração, o risco, o tipo de alteração, o plano de implementação e a infraestrutura a ser modificada. Um pedido de alteração requer duas fases de aprovação. A primeira fase consiste na aprovação por parte do grupo que a alteração foi designada. A

segunda fase consiste na aprovação por parte de um grupo composto por indivíduos que são capazes de avaliar o panorama global de uma mudança normal no que diz respeito à compreensão dos riscos, impactos e implicações financeiras do negócio. Este último grupo é designado por Conselho Consultivo de Alterações (*Change Advisory Board – CAB*).

O caso de uso de gestão de mudança definido assenta principalmente nas condições para cumprimento da separação de funções (*Segregation of Duties*). A separação de funções determina que cada função necessária à conclusão de uma tarefa deve ser atribuída a uma pessoa diferente. A separação de funções é um controlo administrativo utilizado pelas organizações para evitar fraudes, sabotagem, uso indevido de informações e outros comprometimentos de segurança. Depois de analisar o caso de uso, verificou-se que existem três funções importantes no ciclo de vida do pedido de alteração. Essas três funções são a solicitação do pedido, a aprovação por parte do grupo que a alteração foi designada e por fim a aprovação por parte do Conselho Consultivo de Alterações. As condições que a organização deve cumprir para manter-se em conformidade foram definidas tendo em consideração as três funções identificadas, como se pode ver de seguida:

- O aprovador por parte do grupo a que foi designado o pedido de alteração não pode ser o mesmo de quem solicitou o pedido.
- O aprovador do Conselho Consultivo de Alterações não pode ser o mesmo de quem solicitou o pedido de alteração.
- Por último, o aprovador do Conselho Consultivo de Alterações não pode ser o mesmo aprovador por parte do grupo a que o pedido foi designado.

As condições definidas serviram de base a conceção de um processo de avaliação de *compliance* do processo de Gestão de Mudança, tendo sido criado na plataforma um objetivo de controlo para cada uma. Estes objetivos de controlo ao serem relacionados com os pedidos de alteração originam controlos, que permitem verificar se o pedido cumpre a condição. Estes controlos têm dois possíveis estados que consistem nos seguintes:

- *Compliant* – se a condição associada ao pedido de alteração estiver a ser cumprida.
- *Non-compliant* – se a condição associada ao pedido de alteração não estiver a ser cumprida.

A figura 3 representa o modelo de dados da monitorização de controlos do processo de Gestão de Mudança da plataforma do ServiceNow. Este modelo de dados é apenas uma parte da arquitetura do módulo presente na secção 3.1. Módulo GRC: Integrated Risk Management.

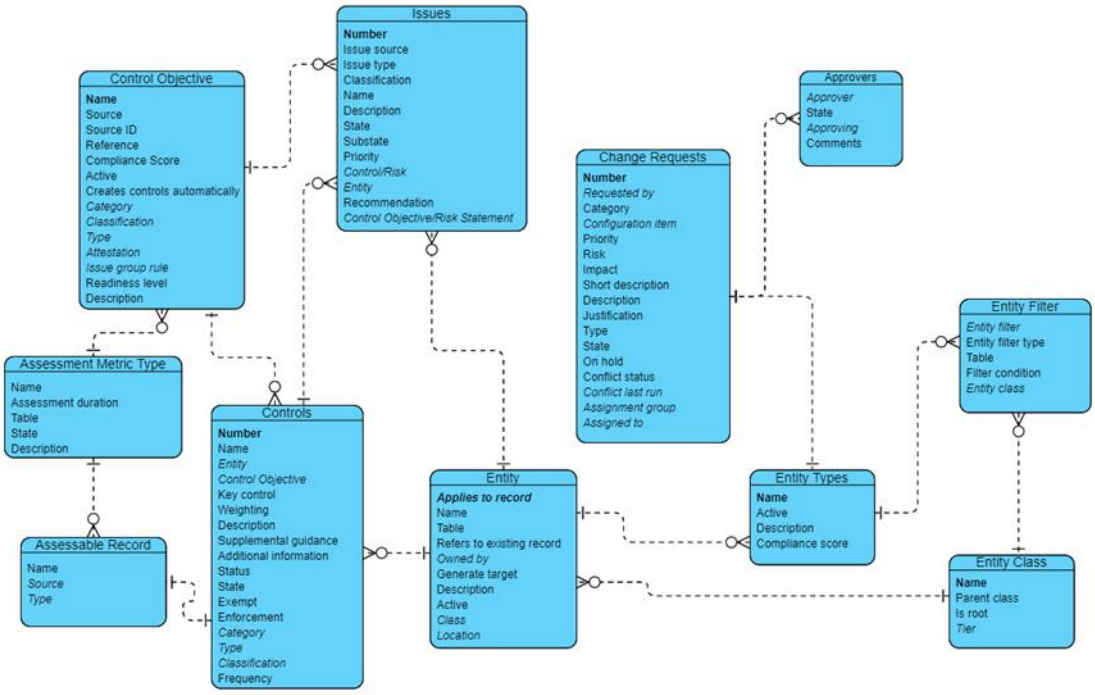

Figura 3 - Modelo de dados

A figura 4 apresenta o diagrama de sequência do caso de uso com monitorização de controlos. Este diagrama tem como atores os utilizadores, o aprovador e o aprovador do Conselho Consultivo de Alterações (CAB - *Change Advisory Board*) e como objetos tem *Change Request*, *Entity* da classe "Change Request", *Controls*, *Attestation* e *Issue*. Existem três controlos uma vez que cada um corresponde a uma condição que o pedido de alteração necessita de cumprir. Assim temos a seguinte distinção:

- **Control1** – controlo que verifica se o aprovador é o mesmo utilizador que pediu a alteração.
- **Control2** – controlo que verifica se o aprovador CAB é o mesmo utilizador que pediu a alteração.
- **Control3** – controlo que verifica se o aprovador CAB é o mesmo utilizador que aprovou o pedido de alteração na primeira fase de aprovação.

O diagrama está dividido em duas secções, Change Management e GRC. Na primeira secção faz parte os atores associados ao processo de pedido de alteração e o pedido de alteração (*Change Request*). Na segunda secção faz parte os objetos pertencentes ao módulo GRC, que permitem monitorizar os controlos existentes. Existe o utilizador2 que corresponde à pessoa que irá verificar se os controlos estão em conformidade com os regulamentos e obrigações da organização. Neste caso o ator precisa de verificar se existe a separação de funções (*Segregation of Duties*).

Para verificar se existe a separação de funções, o utilizador2 tem de passar o controlo para o estado *Attest* criando um *Attestation* que precisa de ser respondido pelo mesmo e dependendo do que responder o controlo pode estar em conformidade ou não com as condições definidas. O objetivo da implementação da monitorização contínua de controlos é a eliminação da etapa do questionário, permitindo a redução da carga de trabalho da pessoa responsável por verificar os controlos.

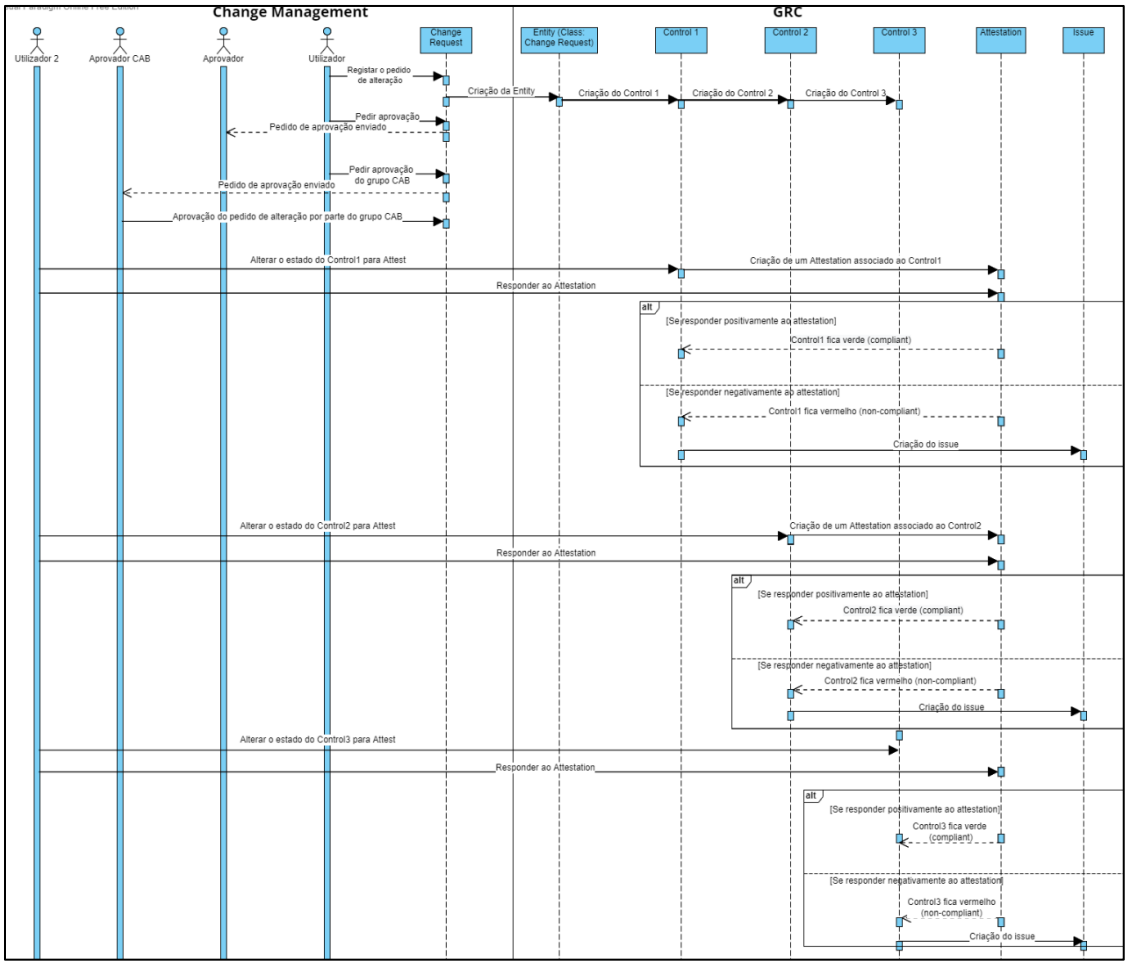

Figura 4 - Diagrama de sequência

4.1. Critérios

Os critérios para avaliar o ServiceNow como plataforma para implementação da solução de monitorização contínua de controlos foram definidos do seguinte modo:

- Implementação - a implementação da solução deve ser rápida, fácil, e ser o menos intrusiva nos processos existentes.

- Facilidade de utilização - a *interface* da solução deve ser de fácil utilização e ter uma *interface* intuitiva e moderna, não dificultando a utilização da mesma por parte do utilizador e possibilitando um aumento na eficiência da organização.
- *Dashboards* e relatórios - a solução deve proporcionar uma clara visibilidade dos riscos da organização e da postura de conformidade, permitindo aos gestores verificar quais os riscos que precisam de resolver e encontrar soluções para eles o mais rápido possível. Também permite verificar quais os regulamentos e obrigações que as pessoas não têm cumprido.

5. Trabalho Desenvolvido

Depois de estudar o módulo *GRC: Integrated Risk Management* do ServiceNow e o caso de uso que será implementado, verificou-se que serão utilizadas as seguintes tabelas pertencentes ao módulo.

- **Entity** – são pessoas, espaços, objetos, ou coisas que precisam de ser monitorizadas para gerir riscos, controlar a conformidade, e rever como parte dos compromissos de auditoria.
- **Entity type** – são categorias dinâmicas que contêm uma ou mais *entities*.
- **Entity filter** – define a tabela a partir da qual os dados são puxados para cada *entity type*. As *entities* são criadas com base nas condições definidas no *entity filter*.
- **Control objective** – objetivo, direção ou norma que funciona como orientação para as interações e operações da empresa.
- **Control** – implementação de um objetivo de controlo para uma entidade de âmbito.
- **Issue** – são criados quando a verificação da conformidade é concluída e indica que o controlo não é implementado uma vez que está *non-compliant*.

Para além das tabelas listadas também foi utilizada a tabela *Change Request*, onde são criados os pedidos de alteração e a tabela *Approvers*, onde são criados os registos de aprovação dos pedidos de alteração.

Em seguida, verificou-se que existem três possíveis implementações da solução de monitorização contínua de controlos. As três possíveis implementações analisadas foram:

- Implementar a solução no processo de aprovação do pedido de alteração,
- Implementar a solução num *Scheduled Job* que será executado de minuto a minuto,
- Implementar um *listener*.

Antes de começar a desenvolver as possíveis implementações foi necessário criar alguns registos fundamentais para a solução de monitorização contínua de controlos.

Em primeiro lugar, foi criada uma *entity class* designada “Change Request”. Depois foi criado um *entity filter* associado à *entity class* criada anteriormente e à tabela *Change Request,* que se encontra representado nas figuras 5 e 6. Este *entity filter* foi associado à *entity type*, representado na figura 7, com o nome “Change Requests” para serem criadas *entities* associadas aos pedidos de alteração existentes e que serão criados futuramente.

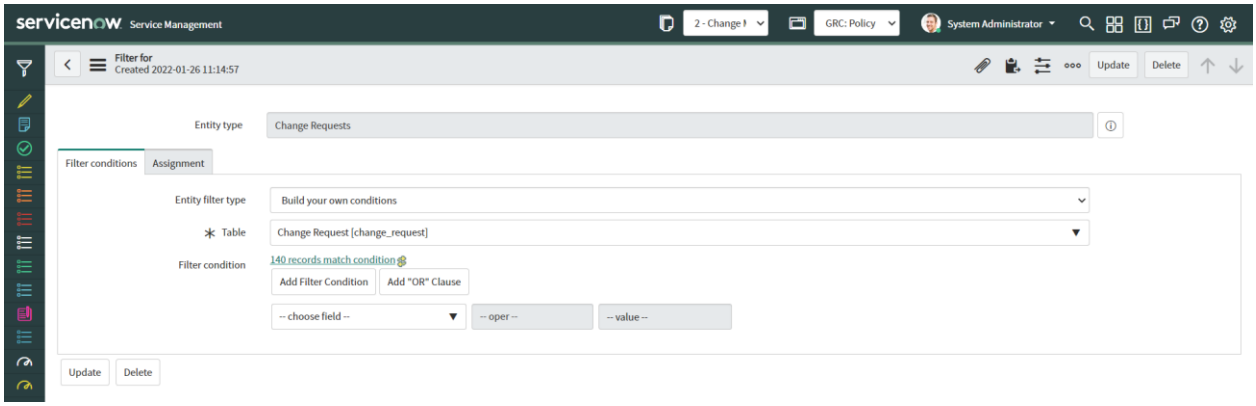

Figura 5 - Entity Filter

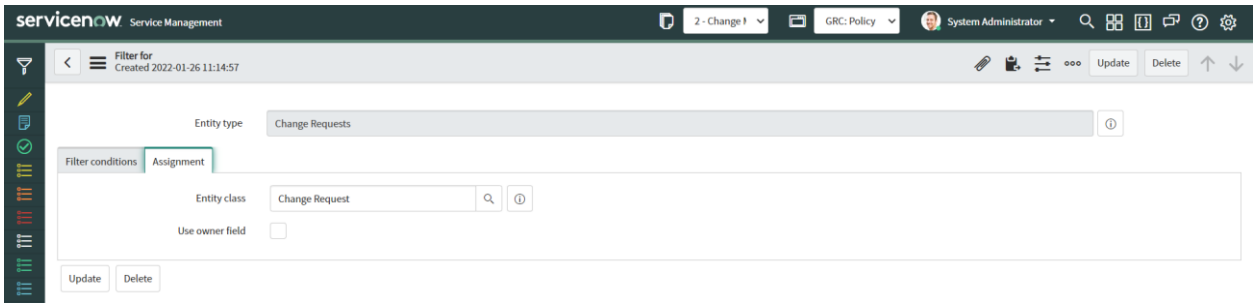

Figura 6 - Entity Filter

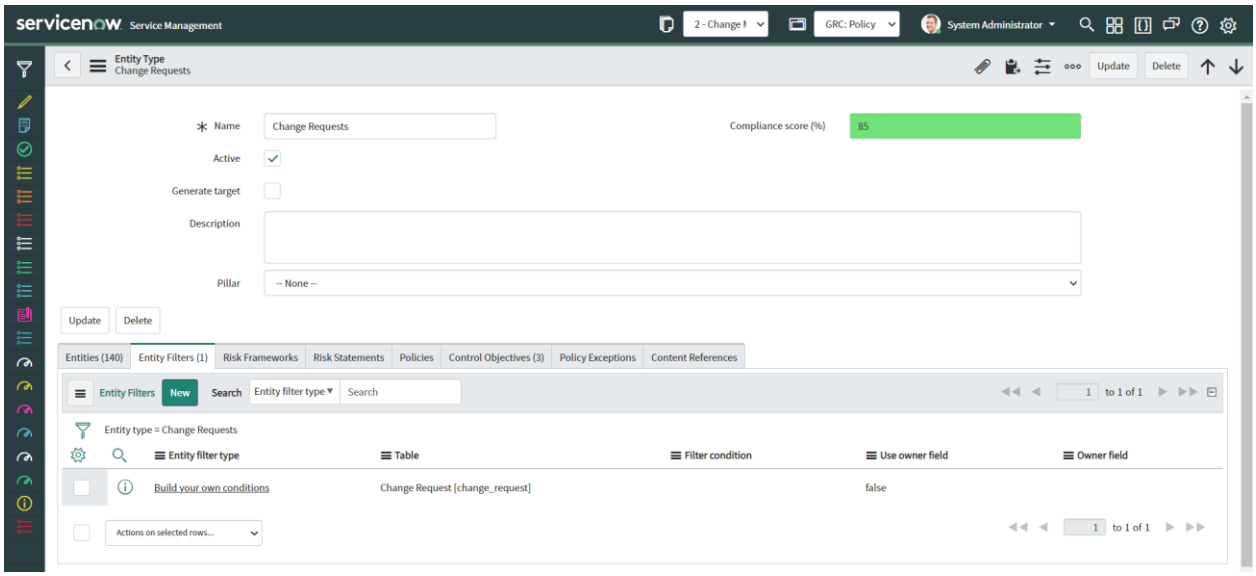

Figura 7 - Entity Type "Change Requests"

Em segundo lugar, foram criados três *control objectives* que correspondem às condições que a organização deve cumprir para se manter em conformidade. Estes *control objectives* foram designados por:

- “Requester cannot be the same as the approver” que corresponde à primeira condição em que o solicitador do pedido de alteração não pode ser o mesmo que o aprovador do grupo a que foi designado.
- “Requester cannot be the same as the CAB approver" que corresponde à segunda condição em que o solicitador do pedido de alteração não pode ser o mesmo que o aprovador do Conselho Consultivo de Alterações.
- "Approver cannot be the same as the CAB approver" que corresponde à terceira condição em que o aprovador do grupo a que o pedido de alteração foi designado não pode ser o mesmo que o aprovador do Conselho Consultivo de Alterações.

Na figura 8 é possível ver um dos *control objectives* criados e ver a associação à *entity type*.

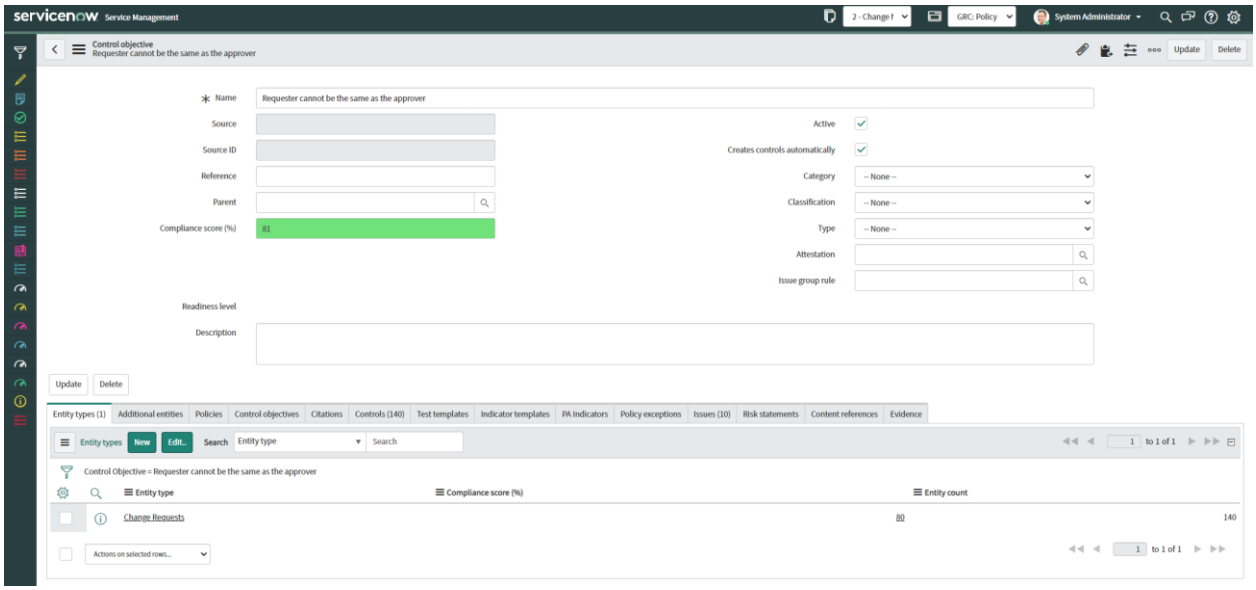

Figura 8 - Control Objective "Requester cannot be the same as the approver"

Depois de criados os *control objectives*, estes foram associados à *entity type* “Change Requests” resultando na criação de três controlos para cada *entity.*

Por último passou-se ao desenvolvimento de cada possível implementação.

5.1. Primeira Implementação

Nesta primeira implementação, a solução foi desenvolvida dentro do processo de aprovação do pedido de alteração, ou seja, ao aprovar o pedido o utilizador verifica ao mesmo tempo se os controlos associados à *entity* correspondente ao pedido que está a ser aprovado está em conformidade ou não.

Para isto foi criada uma cópia do botão de aprovação da tabela *Approvers* designado "Approve CCM", que se encontra representado nas figuras 9 e 10. Neste botão foi desenvolvido o código necessário para verificar se os controlos estão em conformidade. O código desenvolvido encontra-se na secção Código da primeira implementação.

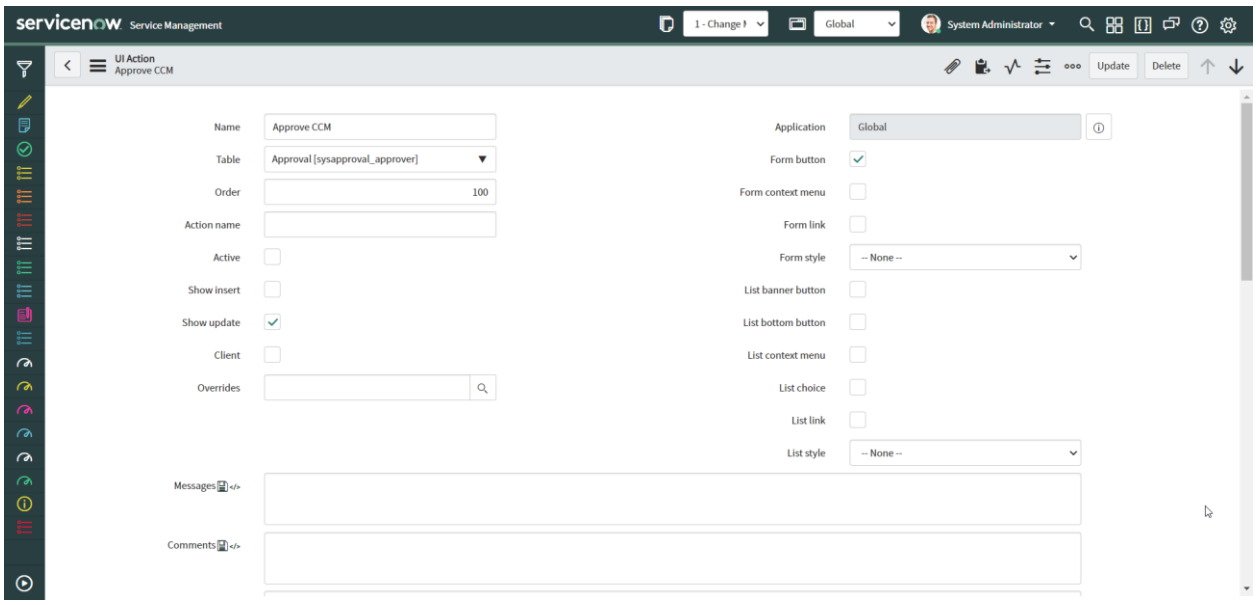

Figura 9 - Botão "Approve CCM"

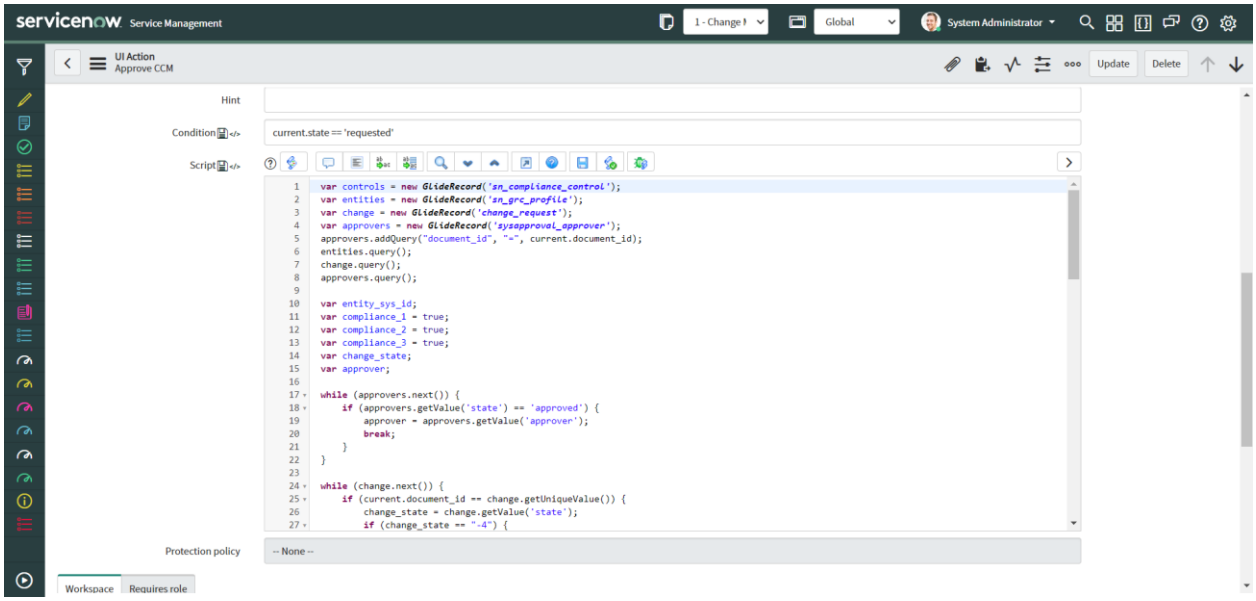

Figura 10 - Código do botão "Approve CCM"

Depois de desenvolvida a primeira implementação verificou-se que os controlos eram atualizados em tempo real, uma vez que ao aprovar o pedido de alteração era feita a verificação do processo de avaliação de *compliance* dos controlos associados à *entity* que estava a ser aprovada. É possível verificar na figura 11 o grau de *compliance* da *entity* CHG0030052 (67%) e também o grau de *compliance* dos pedidos de alteração que é de 85%.

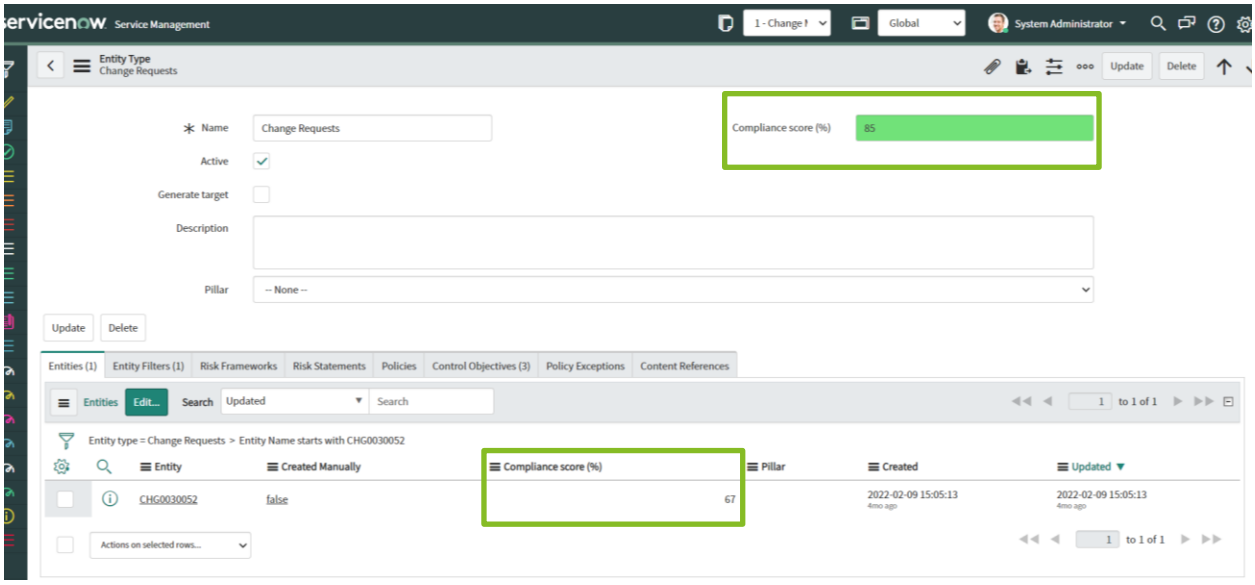

Figura 11 - Entity type Change Requests

Na figura 12 é possível verificar o grau de *compliance* de cada um dos objetivos de controlo que foram definidos para o caso de uso.

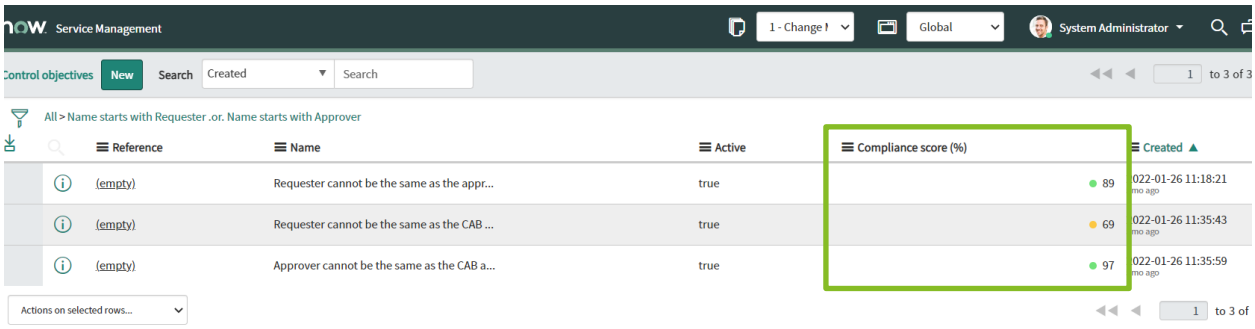

Figura 12 - Objetivos de controlo

Esta implementação tem como vantagem o facto de ser uma forma fácil de em tempo real termos atualizados os graus de *compliance* dos controlos, mas uma grande desvantagem é que quebra as barreiras de abstração uma vez que está a ser configurado dentro do processo e devia ser configurado no GRC.

5.2. Segunda Implementação

Nesta segunda implementação, a solução foi desenvolvida num *Scheduled Job* que foi criado e designado por "GRC Change Request Compliance Monitoring", representado na figura 13. Os *Scheduled Jobs* são tarefas automatizadas que podem ser realizadas num horário específico ou num horário recorrente. Neste *Scheduled Job* foi desenvolvido código que executa de minuto a minuto para verificar

quais os controlos necessários atualizar e verificar para esses controlos estão em conformidade ou não. O código desenvolvido neste *Scheduled Job* encontra-se na secção Código da segunda implementação.

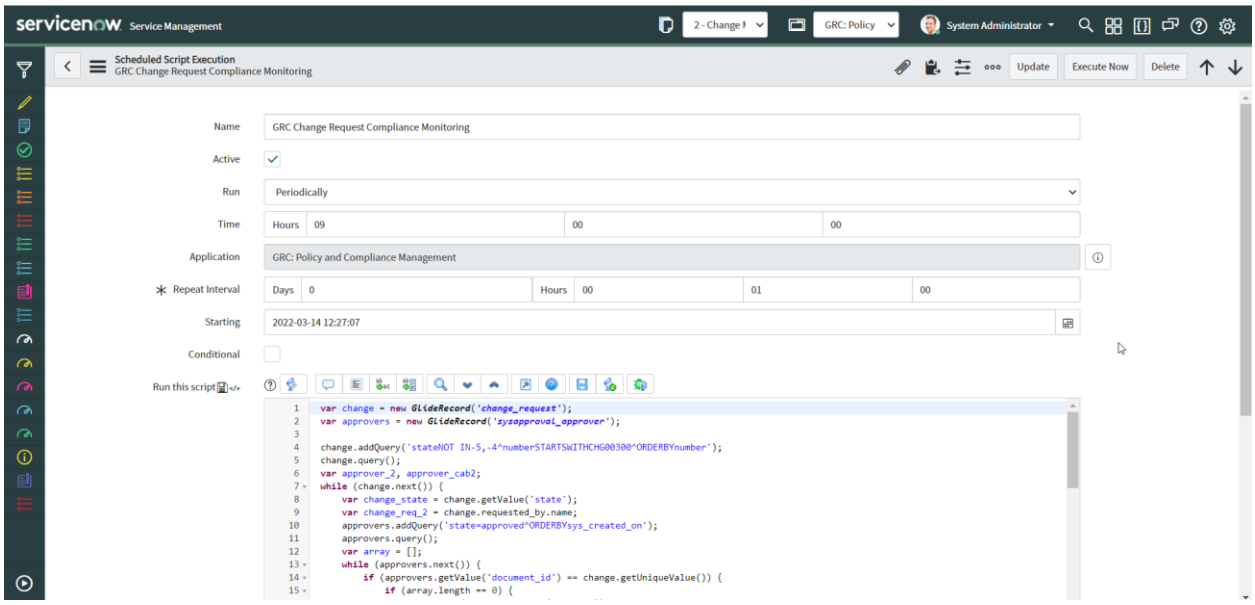

Figura 13 - Scheduled Job "GRC Change Request Compliance Monitoring"

5.3. Terceira Implementação

Depois de desenvolvidas as outras duas implementações, foi analisada melhor a possibilidade de implementar um *listener* para verificar se os controlos estão em conformidade ou não. Desta pesquisa verificou-se que o *listener* não pode ser implementado para as *entities* e os controlos, por isso esta implementação foi impossível de desenvolver.

5.4. Criação de um Issue

Após a implementação da monitorização contínua de controlos, verificou-se a necessidade de criar um *issue* cada vez que um controlo não esteja em conformidade com a condição a que está associado. Para isto foi criada uma *business rule,* representada nas figuras 14 e 15, em que verifica se o estado de um controlo está *non-compliant*. Nesse caso é criado um *issue* em que a origem dele é "Control Compliance Failure".

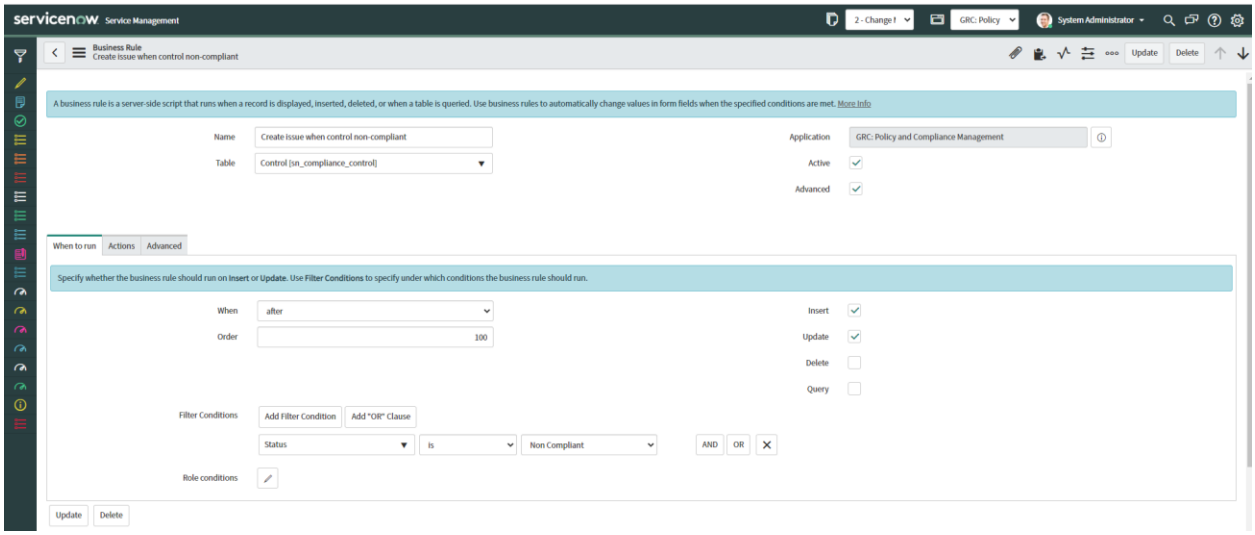

Figura 14 - Business Rule "Create issue when control non-compliant"

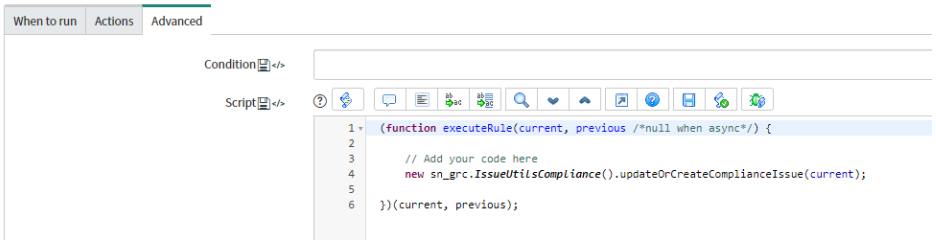

Figura 15 - Código da Business Rule "Create issue when control non-compliant"

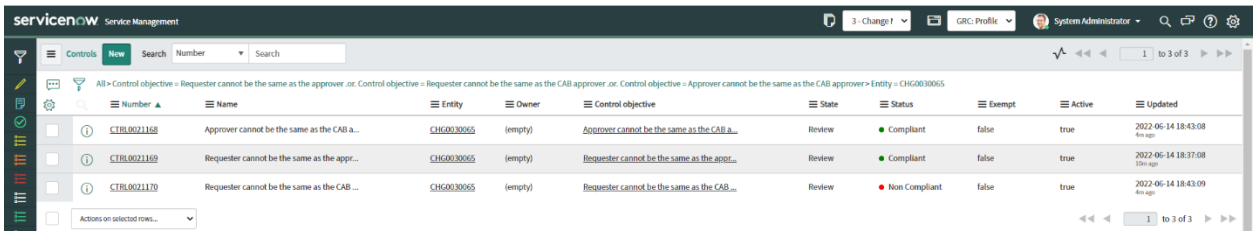

Figura 16 - Controlos do pedido de alteração CHG0030065

Pela figura 16 é possível ver que o pedido de alteração CHG0030065 tem um controlo associado ao objetivo de controlo "Requester cannot be the same as the CAB approver" com o estado *non-compliant*. Como o controlo está *non-compliant* foi criado um *issue,* representado na figura 17, associado ao controlo e à *entity.*

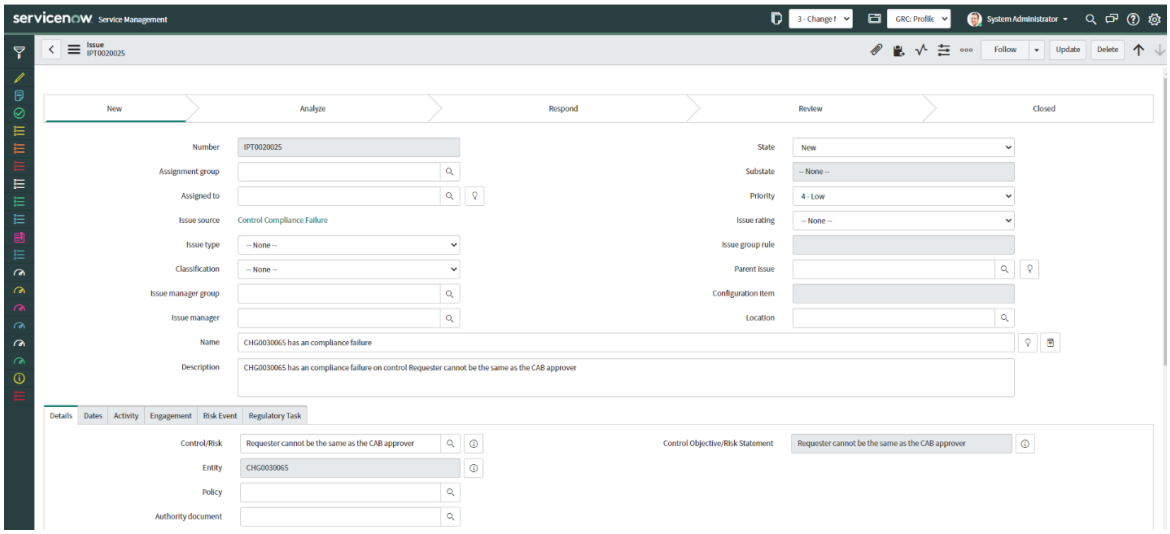

Figura 17 - Issue IPT0020025

5.5. Dashboards

No final de desenvolver as implementações da monitorização contínua de controlos, foi desenvolvida uma página com alguns gráficos para entender melhor o grau de *compliance* da organização quanto aos pedidos de alteração.

Na figura 18 é possível ver que nos três primeiros gráficos está representada informação dos pedidos de alteração, tais como, o estado, o tipo e o departamento a que o solicitador do pedido pertence.

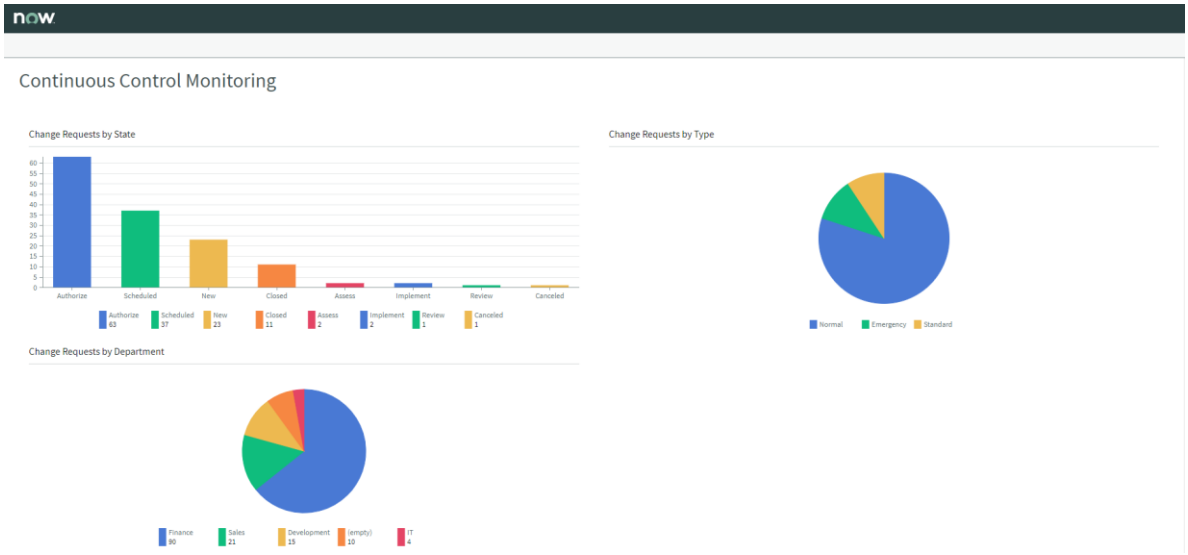

Figura 18 - Dashboards

Nas figuras 19 e 20 estão representadas informações sobre as *entities* associadas aos pedidos de alteração, os objetivos de controlo e os controlos correspondentes. Também podemos ver informação

sobre os *issues* abertos e associados aos controlos que não estão em conformidade. Na primeira figura é possível verificar que atualmente a organização tem um grau de *compliance* de 80% quanto aos pedidos de alteração.

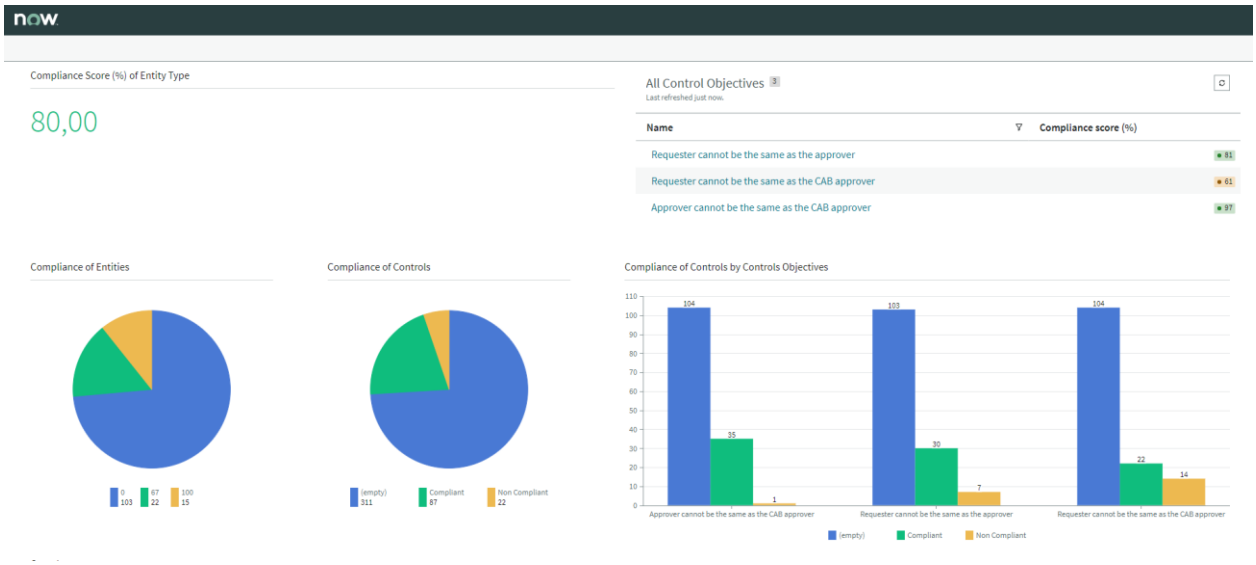

Figura 19 - Dashboards

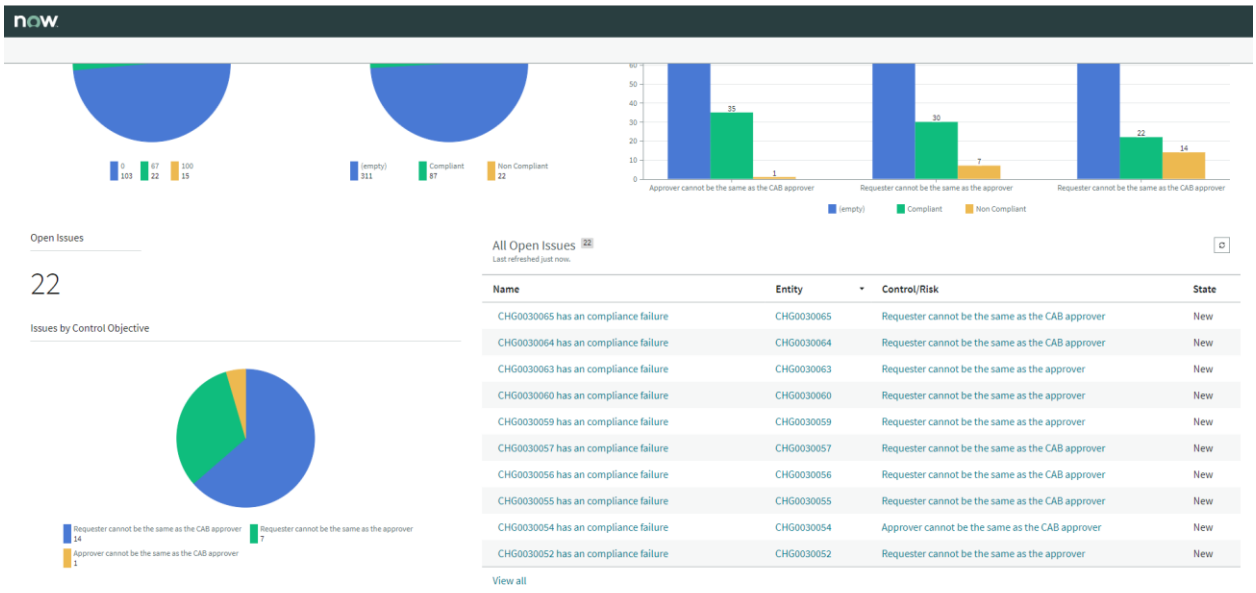

Figura 20 - Dashboards

6. Discussão

Nesta dissertação foi desenvolvido duas possíveis implementações da solução de monitorização contínua de controlos. Numa primeira implementação foi feito uma cópia do botão de aprovação e adicionado código para verificar se os controlos associados à *entity* que estava a ser aprovada estavam a cumprir os objetivos de controlo. A outra implementação consistiu na criação de um *Scheduled Job* que era executado minuto a minuto e verificava se todos os controlos estavam a cumprir o objetivo de controlo a que estava associado.

A vantagem da primeira implementação é o facto de termos os graus de *compliance* dos controlos em tempo real, visto ser efetuado ao mesmo tempo que se aprova o pedido de alteração. Infelizmente uma grande desvantagem desta implementação é que quebra as barreiras de abstração visto que a verificação dos graus de *compliance* está a ser configurada dentro do processo de TI e devia ser configurado no módulo de GRC.

A segunda implementação tem como vantagens o facto de não quebrar a barreira de abstração, uma vez que foi configurado fora do processo de TI, e de termos os graus de *compliance* dos controlos em quase tempo real (minuto a minuto). O intervalo de tempo que o *Scheduled Job* é executado pode ser alterado para menos ou mais de um minuto dependendo do que a organização precisa.

Tendo em conta as vantagens e desvantagens das duas implementações pode-se concluir que a segunda é a melhor para configurar a solução de monitorização contínua de controlos na plataforma ServiceNow.

A finalização da dissertação é avaliar se a plataforma ServiceNow consegue implementar a solução de monitorização contínua de controlos. Para avaliar a plataforma foram selecionados três critérios. O primeiro critério consiste em avaliar se a implementação da solução foi rápida, fácil e o menos intrusiva nos processos existentes na plataforma. Como discutido anteriormente, na primeira implementação este não foi completamente cumprido uma vez que quebrou a barreira de abstração, tendo sido configurado no processo existente de Gestão de Mudança.

Na segunda implementação, *Scheduled Job*, este critério foi cumprido visto que foi configurado fora dos processos existentes da plataforma, não quebrando a barreira de abstração.

O segundo critério é sobre a facilidade de utilizar a *interface* e de esta ser intuitiva e moderna. A plataforma ServiceNow é intuitiva, moderna e de fácil utilização por isso este critério é cumprido nas duas implementações.

O terceiro critério é sobre as *dashboard* e relatórios, devendo proporcionar uma clara visibilidade do risco da organização e da postura de conformidade da mesma. Depois de implementar a solução de monitorização contínua de controlos foi possível criar *dashboards* e relatórios com informações sobre os pedidos de alteração, o grau de *compliance* da organização quanto aos pedidos de alteração, os controlos que estão em conformidade e quais os *issues* abertos que precisam de ser resolvidos, tendo a plataforma cumprido este critério.

Em suma, a plataforma ServiceNow cumpre todos os critérios definidos para a avaliar, apenas se for desenvolvida a primeira implementação é que a plataforma não cumpre o primeiro critério, sendo a melhor opção para implementar a solução de monitorização contínua de controlos a segunda implementação.

7. Conclusões

A finalidade desta dissertação consistiu na avaliação da plataforma ServiceNow para implementar a solução de monitorização contínua de controlos. Para cumprir esta finalidade, no início foi definido um conjunto de tarefas, as quais foram sendo cumpridas conforme se explica de seguida.

Inicialmente foi feito um estado da arte sobre os principais temas relacionados com a monitorização contínua de controlos e a plataforma utilizada. De seguida foi cumprida a primeira tarefa que consistia em instanciar um processo conhecido da Governação das TI em ServiceNow. O processo escolhido para instanciar foi a Gestão de Mudança, que proporciona uma abordagem sistemática para controlar o ciclo de vida de todas as alterações ao ambiente de operações de produção desde o início até à sua conclusão com a interrupção mínima das operações comerciais.

Na etapa seguinte foram definidas algumas condições para serem verificadas pelo módulo *GRC: Integrated Risk Management.* Nesta segunda tarefa foram criados os controlos necessários para verificar as condições definidas.

Na terceira tarefa foram desenvolvidas duas implementações da solução de monitorização contínua de controlos, automatizando assim a verificação dos controlos criados na etapa anterior. Destas duas implementações verificou-se que a segunda implementação é melhor opção para desenvolver visto que não quebra a barreira de abstração, isto é, não é configurada no processo de TI, Gestão de Mudança.

Durante a realização das tarefas também foram definidos três critérios para avaliar a plataforma ServiceNow, quanto à possibilidade de implementar a monitorização contínua de controlos.

Em suma, a plataforma ServiceNow cumpre todos os critérios definidos, sendo possível implementar a solução de monitorização contínua de controlos e ter resultados sobre o grau de *compliance* da organização, podendo verificar quais os processos não estão a cumprir os regulamentos e leis que a organização tem de aplicar. Com a implementação solução, a organização tem uma visão geral da gestão de riscos.

8. Referências

De Haes, S., & Van Grembergen, W. (2004). IT governance and its mechanisms. *Information systems control journal*, *1*, 27-33.

Deloitte (2018). Next Wave of Continuous Control Monitoring solution A Point of View For Private circulation only. Disponível em: https://www2.deloitte.com/content/dam/Deloitte/in/Documents/risk/in-ra-next-wave-of-continuous-control-monitoring-soluntion-noexp.pdf

Gericke, A., Fill, H. G., Karagiannis, D., & Winter, R. (2009). *Situational method engineering for governance, risk and compliance information systems. In Proceedings of the 4th international conference on design science research in information systems and technology* (pp. 1-12).

Gregory, R. W., Kaganer, E., Henfridsson, O., & Ruch, T. J. (2018). IT Consumerization and the Transformation of IT Governance. Mis Quarterly, 42(4), 1225-1253.

Handoko, B. L., Riantono, I. E., & Gani, E. (2020). Importance and Benefit of Application of Governance Risk and Compliance Principle. *Systematic Reviews in Pharmacy*, *11*(9), 510-513.

Hunt, R., & Jackson, M. (2010). An introduction to continuous controls monitoring. *Computer Fraud & Security*, *2010*(6), 16-19.

ISACA. (2018). *COBIT® 2019 Framework: Introduction and Methodology.*

Long, G. (2017). The Importance of GRC in the Enterprise. *Available at SSRN 2951123*.

Peffers, K., Tuunanen, T., Rothenberger, M. A., & Chatterjee, S. (2007). A design science research methodology for information systems research. *Journal of management information systems*, 24(3), 45-77.

Racz, N., Weippl, E., & Seufert, A. (2011). *Governance, risk & compliance (GRC) software-an exploratory study of software vendor and market research perspectives. In 2011 44th Hawaii International Conference on System Sciences* (pp. 1-10). IEEE.

Riemer, K., Ciriello, R., Peter, S., & Schlagwein, D. (2020). Digital contact-tracing adoption in the COVID-19 pandemic: IT governance for collective action at the societal level. *European Journal of Information Systems*, *29*(6), 731-745.

ServiceNow. "GRC - Governance Risk and Compliance - ServiceNow." www.servicenow.com/products/governance-risk-and-compliance.html. Accessed 21 Feb. 2022.

ServiceNow. "About ServiceNow - Who We Are and What We Do - ServiceNow." www.servicenow.com/company.html. Accessed 31 Jan. 2022.

Teeter, R. A., Brennan, G., Alles, M. G., & Vasarhelyi, M. A. (2008). Aiding the audit: using the IT audit as a springboard for continuous controls monitoring. *Unpublished working paper, Rutgers business school.*

Webb, P., Pollard, C., & Ridley, G. (2006). Attempting to Define IT Governance: Wisdom or Folly? Proceedings of the 39th Annual Hawaii International Conference on System Sciences (HICSS'06). https://doi.org/10.1109/hicss.2006.68

9. Anexos

Código da primeira implementação

```
var controls = new GlideRecord('sn_compliance_control');
var entities = new GlideRecord('sn_grc_profile');
var change = new GlideRecord('change_request');
var approvers = new GlideRecord('sysapproval_approver');
approvers.addQuery(''document_id'', ''='', current.document_id);
entities.query();
change.query();
approvers.query();

var entity_sys_id;
var compliance_1 = true;
var compliance_2 = true;
var compliance_3 = true;
var change_state;
var approver;

while (approvers.next()) {
    if (approvers.getValue('state') == 'approved') {
        approver = approvers.getValue('approver');
        break;
    }
}

while (change.next()) {
    if (current.document_id == change.getUniqueValue()) {
        change_state = change.getValue('state');
        if (change_state == ''-4'') {
```

```
            if (current.approver == change.getValue('requested_by')) {
                compliance_1 = false;
            } else {
                compliance_1 = true;
            }
        } else if (change_state == "-3") {
            if (current.approver == change.getValue('requested_by')) {
                compliance_2 = false;
            } else {
                compliance_2 = true;
            }
            if (current.approver == approver) {
                compliance_3 = false;
            } else {
                compliance_3 = true;
            }
        }
        break;
    }
}

while (entities.next()) {
    if (entities.applies_to == current.document_id) {
        entity_sys_id = entities.getValue('sys_id');
        break;
    }
}

controls.addQuery("profile", "=", entity_sys_id);
controls.query();
while (controls.next()) {
```

```
    if (change_state == '-4') {
        if (controls.content == "4a9e83911b5541105cbdcb74604bcb67") { //Requester cannot be the same as the approver
            if (compliance_1) {
                controls.setValue("status", "compliant");
            } else {
                controls.setValue("status", "non_compliant");
            }
        }
    } else if (change_state == '-3') {
        if (controls.content == "4a9e83911b5541105cbdcb74604bcb67") { //Requester cannot be the same as the approver
            if (controls.status == "") {
                if (compliance_1) {
                    controls.setValue("status", "compliant");
                } else {
                    controls.setValue("status", "non_compliant");
                }
            }
        }
        if (controls.content == "62f257d51b5541105cbdcb74604bcbf3") { //Requester cannot be the same as the CAB approver
            if (compliance_2) {
                controls.setValue("status", "compliant");
            } else {
                controls.setValue("status", "non_compliant");
            }
        }
        if (controls.content == "d6031bd51b5541105cbdcb74604bcb79") { //Approver cannot be the same as the CAB approver
            if (compliance_3) {
                controls.setValue("status", "compliant");
```

```
            } else {
                controls.setValue(''status'', ''non_compliant'');
            }
        }
    }
    controls.setValue('state', 'review');
    controls.update();
}
```

```
current.state = ''approved'';
current.update();
new ApprovalUserFeedback().approved(current);
```

Código da segunda implementação

```
var change = new GlideRecord('change_request');
var approvers = new GlideRecord('sysapproval_approver');

change.addQuery('stateNOT IN-5,-4^numberSTARTSWITHCHG00300^ORDERBYnumber');
change.query();
var approver_2, approver_cab2;
while (change.next()) {
    var change_state = change.getValue('state');
    var change_req_2 = change.requested_by.name;
    approvers.addQuery('state=approved^ORDERBYsys_created_on');
    approvers.query();
    var array = [];
    while (approvers.next()) {
        if (approvers.getValue('document_id') == change.getUniqueValue()) {
            if (array.length == 0) {
```

```
                array.push(change.getValue('number'));
            }
            array.push(approvers.approver.name);
        }
    }

    if (change_state == -3) {
        approver_2 = array[1];
    } else if (change_state >= -2 && array.length == 3) {
        approver_2 = array[1];
        approver_cab2 = array[2];
    } else if (change_state >= -2 && array.length == 2) {
        approver_2 = '';
        approver_cab2 = array[1];
    }
    var entities = new GlideRecord('sn_grc_profile');
    entities.addQuery('applies_to', change.sys_id);
    entities.query();

    if (entities.next()) {
        var controls = new GlideRecord('sn_compliance_control');
        controls.addQuery('profile=' + entities.sys_id + '^ORDERBYnumber');
        //controls.addNullQuery('status');
        controls.query();

        while (controls.next()) {
            var content = controls.getValue('content');
            if (change_state == -3 && content == '4a9e83911b5541105cbdcb74604bcb67') {
//status==Authorize && Requester cannot be the same as the approver
                if (approver_2 == change_req_2) {
                    controls.setValue('status', 'non_compliant');
```

```
            controls.setValue('state', 'review');
        } else {
            controls.setValue('status', 'compliant');
            controls.setValue('state', 'review');
        }
    } else if (change_state >= -2) { //status==Scheduled,Implement,Review, Close, Canceled
        if (content == '4a9e83911b5541105cbdcb74604bcb67') { //Requester cannot be the same as the approver
            if (approver_2 == change_req_2) {
                controls.setValue('status', 'non_compliant');
                controls.setValue('state', 'review');
            } else {
                controls.setValue('status', 'compliant');
                controls.setValue('state', 'review');
            }
        }
        if (content == '62f257d51b5541105cbdcb74604bcbf3') { //Requester cannot be the same as the CAB approver
            if (approver_cab2 == change_req_2) {
                controls.setValue('status', 'non_compliant');
                controls.setValue('state', 'review');
            } else {
                controls.setValue('status', 'compliant');
                controls.setValue('state', 'review');
            }
        }
        if (content == 'd6031bd51b5541105cbdcb74604bcb79') { //Approver cannot be the same as the CAB approver
            if (approver_2 == approver_cab2) {
                controls.setValue('status', 'non_compliant');
                controls.setValue('state', 'review');
            } else {
```

```
                controls.setValue('status', 'compliant');
                controls.setValue('state', 'review');
            }
        }
    }
    controls.update();
  }
  gs.info(change.getValue('number') + ': Requested - ' + change_req_2 + ', Approver - ' +
approver_2 + ', CAB Approver - ' + approver_cab2 + '\n');
 }
}
```

Script Include IssueUtilsCompliance

```
var IssueUtilsCompliance = Class.create();
IssueUtilsCompliance.prototype = {
 initialize: function() {
 },

    updateOrCreateComplianceIssue: function(control) {
  return this._updateOrCreateComplianceIssue(control);
 },

    _updateOrCreateComplianceIssue: function(control) {
 var issueSource = 'compliance';
 var issueComment = '';
 var existingIssue = new sn_grc.IssueUtilsBase().findExistingOpenIssue(control.getUniqueValue());
 if (existingIssue) {
  if (control.profile) {
   issueComment = gs.getMessage('{0} has compliance failure on control {1}',
[control.profile.name.toString(), control.getValue('name')]);
  } else {
```

```
            issueComment = gs.getMessage('There is an compliance failure on control {0}',
[control.getValue('name')]);
        }
        this._addIssueSource(existingIssue, issueSource, issueComment);
    } else {
        var issue = {};
        if (control.profile) {
            issue.short_description = gs.getMessage('{0} has an compliance failure',
control.profile.name.toString());
            issue.description = gs.getMessage('{0} has an compliance failure on control {1}',
[control.profile.name.toString(), control.getValue('name')]);
        } else {
            issue.short_description = gs.getMessage('Compliance failure on control {0}',
[control.getValue('name')]);
            issue.description = gs.getMessage('There is an compliance failure on control {0}',
[control.getValue('name')]);
        }

        issue.item = control.getUniqueValue();
        issue.assignment_group = control.getValue('owning_group');
        issue.assigned_to = control.getValue('owner');
        issue.profile = control.getValue('profile');
        issue.created_manually = false;
        var newIssue = new sn_grc.IssueUtilsBase().generateIssue(issue, issueSource);
        if (!newIssue) {
            gs.addErrorMessage(gs.getMessage('Unable to create a issue for {0}',
indicatorResult.indicator.number.toString()));
        }
    }
},

    type: 'IssueUtilsCompliance'
};
```

Business Rule “Create issue when control non-compliant”

```
(function executeRule(current, previous /*null when async*/) {

    // Add your code here
    new sn_grc.IssueUtilsCompliance().updateOrCreateComplianceIssue(current);

})(current, previous);
```