

Auditoria Da Informação

António Graça
30000497@students.ual.pt

Pedro Simões
30007732@students.ual.pt

Abstract — Auditing is a recognized management technique providing managers with an overview of the present situation regarding specific resource(s) and services within an organization. Many different types of audits currently exist in the commercial world, including audits of information resources. Currently, as far as the researchers could determine, there exists no single accepted methodology for performing an information audit. In view of this, the researchers investigate whether it is possible (and desirable) to develop a standardized information auditing methodology. Investigating the nature and characteristics of the information audit as well as how a number of other audit types do this, e.g., the financial audit, the communication audit. The researchers conclude that none of these are the same as the information audit, although similarities exist. Various information audit methodologies are discussed, evaluated, and classified. The researchers conclude that even though the principles of the financial audit cannot be used to develop a standardized methodology for information auditing, information professionals can look towards the accounting profession for support in developing a standardized, universally accepted method for accurately determining the value of information entities. Guidelines for a standardized information audit methodology are identified.

Security; ISO; Information Security; ISO Standards; Security Of Data; Information Security Management System; ISO 27001; ISMS; ISO27001:2005; ISO 27001; (key words)

Nos dias de hoje, o compartilhamento e tratamento de dados e informação é inevitável, pelo que se levou a criação de normas e procedimentos de segurança. Na verdade, estas normas e procedimentos podem não ser obrigatórios e apesar da aplicação não ser gratuita e até mesmo poderem apresentar custos elevados, são extremamente recomendados para uma gestão de dados apropriada.

A norma 27001 é a norma mais conhecida deste tópico e cria uma normalização para proteção de dados e resiliência informática em conjunto com o

resto da família 27000, pelo que será relevante tratar deste mesmo assunto dentro do tema “Auditoria de Informação” dentro deste documento, relatando o que é, para que serve e em que consiste.

Ainda sobre este tema existem várias ferramentas e aplicações que ajudam na aplicação da norma 27001. Este documento irá tratar também de uma dessas aplicações de nome “Pentana Audit Software”, relatando o porquê de a usar, os seus benefícios e uma explicação de como funciona usando exemplos tirados da interface da mesma.

O objetivo final deste documento será deixar o leitor com conhecimentos gerais e aplicáveis sobre o tema, seja por uma questão de académica ou por uma questão de eventual aplicação no mundo real.

I. NORMA ISO-27001

Este documento tem como tema geral a Auditoria de Informação, pelo que é relevante desenvolver o tema da norma ISO 27001. Esta norma internacional é utilizada para a gestão da Segurança da Informação e será descrita nos próximos pontos.

A. O que é?

A norma ISSO 27001 é o padrão e a referência internacional para a gestão da Segurança da Informação. Esta norma tem vindo, de forma continuada, a ser melhorada ao longo dos anos e deriva de um conjunto anterior de normas: a ISO-27001 e a BS7799. Teve origem, na realidade, num documento publicado em 1992 por um departamento do governo britânico que estabelecia um código de práticas relativas à gestão da Segurança da Informação. Milhares de profissionais contribuíram para o estabelecimento de um standard estável e maduro ao longo dos anos, mas que continuará a evoluir. O princípio geral da norma é a adoção pela organização de um conjunto de requisitos, processos e controlos com o objetivo de mitigarem e gerirem adequadamente o risco. A utilização das práticas documentadas no Standard está presente em milhões de entidades mundiais, que usufruem dos benefícios da sua adoção, sendo que, as entidades que assim o desejem podem também se certificarem, demonstrando assim de forma idónea que cumprem os requisitos e os

processos constantes na norma. Determinadas organizações obrigam que os seus fornecedores ou parceiros detenham certificações, como garante do cumprimento dos princípios estabelecidos pela mesma. As organizações que adotam e se certificam nesta norma, atribuem especial importância à proteção da informação.

B. Para que serve?

A adoção da norma ISO-27001 serve para que as organizações adotem por um modelo adequado de estabelecimento, implementação, operação, monitorização, revisão e gestão de um Sistema de Gestão de Segurança da Informação (SGSI). Este SGSI é, de acordo com os princípios da norma, um modelo holístico de abordagem à segurança e independe de marcas e fabricantes tecnológicos. É holístico por ser uma abordagem 360º à segurança da informação, tratando de múltiplos temas tais como telecomunicações, segurança aplicacional, proteção do meio físico, recursos humanos, continuidade de negócio, licenciamento, etc. É independente de fabricantes porque se destina ao estabelecimento de processos e procedimentos que depois podem ser materializados à realidade de cada organização de forma diferente e com a especificidade de cada ambiente tecnológico e organizacional.

C. Em que consiste?

A norma ISO 27001 é composta por duas componentes distintas:

1) A primeira componente é onde são definidas as regras e os requisitos de cumprimento da norma. Nesta componente, são endereçados os aspetos explícitos na seguinte figura:

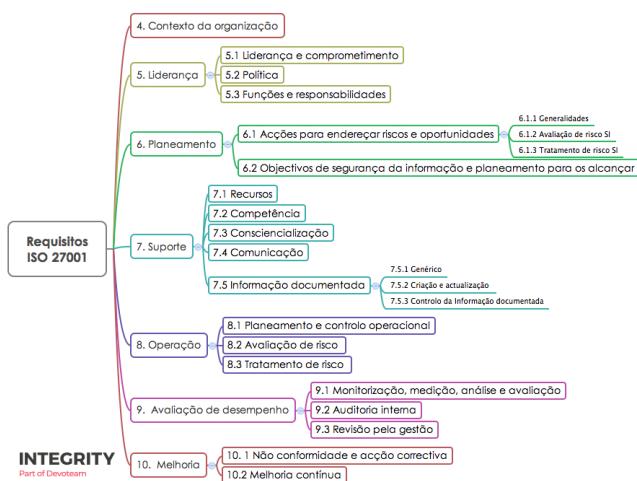


Imagen 1 — Requesitos ISO-27001

2) A segunda componente da norma, é denominada de Anexo A e é na realidade composta por um conjunto de controlos que as organizações devem adotar em diferentes temas:



Imagen 2 — Controlos ISO-27001

A estrutura global da norma ISO-27001 pode ser apresentada da seguinte forma:

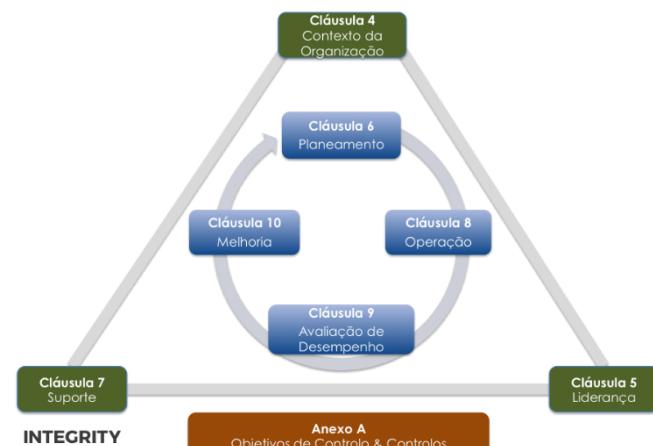


Imagen 3 — Estrutura Global Da Norma ISO-27001

Em que as cláusulas com os requisitos correspondentes ao ciclo de melhoria continua estão representados a azul, as cláusulas com os requisitos gerais do SGSI encontram-se a verde e o anexo com os objetivos de controlo e controlos aparecem a laranja.

D. Benefícios para adotantes

A adoção das práticas de gestão documentadas representa um conjunto de benefícios, nomeadamente:

- Demonstra um compromisso dos Executivos da Organização para com a segurança da informação;
- Aumenta a fiabilidade e a segurança da informação e dos sistemas, em termos de confidencialidade, disponibilidade e integridade;

- Garante a realização de investimentos mais eficientes e orientados ao risco;
 - Incrementa os níveis de sensibilidade, participação e motivação dos colaboradores da Organização para com a Segurança da Informação;
 - Identifica e endereça de forma continuada a oportunidade para melhorias;
 - Aumenta a confiança e satisfação dos clientes e parceiros;
 - A implementação dos controlos provenientes da norma e da análise de risco, melhora o desempenho operacional das organizações;
 - Providenciar à organização de um sistema de controlo da gestão, incrementando a eficácia da mesma.
 - Benefícios para clientes, fornecedores e/ou parceiros
 - As entidades “pares” de uma entidade certificada também obtêm benefícios na interação com a organização certificada.
 - Uma das grandes preocupações da atualidade é efetivamente a confiança no tratamento adequado da informação sensível da sua organização.

A implementação da norma ISO-27001 providencia um elevado compromisso com a proteção da informação, o que representa um nível considerável de conforto para as organizações que interagem com a entidade certificada. Assim, os clientes, parceiros e fornecedores desta entidade sabem que a informação da sua organização será tratada de acordo com elevados padrões de gestão e proteção ao nível da Segurança da Informação, já que a empresa certificada foi auditada por uma entidade externa e idónea.

E. Tempo para a preparação da certificação

A preparação da certificação requer a implementação e adoção dos requisitos, políticas, procedimentos, controlos e práticas requeridas pela norma, ajustadas ao âmbito e à realidade tecnológica e organizacional de cada entidade. Assim, o tempo de implementação varia de acordo com a realidade, maturidade e dimensão de cada organização. Um roadmap típico de implementação é, por exemplo:

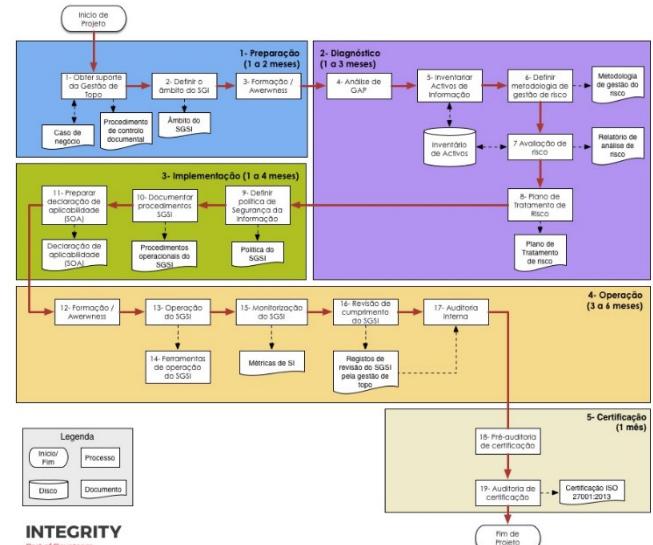


Imagen 4 — Típico Roadmap De Implementação

F. Custo estimado da implementação

O custo da implementação e da certificação varia de acordo com a realidade organizacional e especificidades de cada entidade, nomeadamente o processo sobre o qual incide a certificação, o número de colaboradores intervenientes nesse processo, o número de locais envolvidos e o número de ativos de informação a considerar o âmbito da certificação.

Existe sempre a possibilidade de pedir um orçamento a uma entidade certificadora, que irá estimar o potencial custo.

No que toca a certificação, pode-se estimar um custo típico associado. As certificações implicam auditorias. Uma empresa pequena com menos de 50 empregados pode, tipicamente, ter entre três a seis auditorias e custaria entre \$5000 e \$10000. O custo por auditoria varia entre entidades de certificação, mas uma estimativa razoável seria de \$1500 por auditoria.

No entanto, as auditorias são apenas uma pequena parte da certificação. A preparação para a auditoria de certificação pode custar entre \$5000 e \$75000. Este custo está relacionado com:

- Escrita de políticas que reduzem o risco enfrentado pelos utilizadores;
 - Decisão sobre a metodologia de avaliação de risco;
 - Escrita de uma declaração de aplicação, resumindo as medidas de segurança e declarações lógicas sobre as medidas não consideradas;
 - Escrita de um plano de tratamento de riscos que clarifica onde se encontram os riscos e

- como serão lidados, com datas-limites, dependências, e responsabilidade de empregados;
- Definição de como será medido o sucesso do controlo e em que níveis;
 - Condução de uma auditoria interna: relatórios, revisões, e correção de problemas.

Uma auditoria interna pode rondar os \$7500. Existem, depois, os custos de implementação como o treino e certificação, custos de produtividade, manutenção de licenças de software e ferramentas, custo do gestor de implementação e certificação. Os custos relacionados podem rondar em mais de \$100000. Anualmente.

Finalmente, tem-se os custos de manutenção, que estão relacionados a custos depois da certificação. Após certificação, é necessário haver auditorias internas e auditorias de supervisão após dois e três anos, respectivamente. Cada uma poderá custar \$7500.

II. PENTANA AUDIT SOFTWARE

No tema de Auditoria de Informação existem muitas ferramentas e aplicações que ajudam na aplicação da Norma ISO 27001. Neste documento foi escolhida Pentana Audit. Esta providencia um ciclo de vida de auditorias completo e integrado, desenhado por auditores para auditores.

A. O que é? Informações gerais.

Pentana é um sistema de gestão integrada de riscos e auditorias, que permite ao utilizador desenvolver uma variedade de atividades, ajudando-o nos importantes passos da sua missão. A aplicação permite, num primeiro passo, a determinação do universo de entidades para auditoria, pela coleta de dados da organização em questão. Associado com a etapa de planeamento, Pentana oferece uma avaliação global dos riscos da entidade e o planeamento do trabalho de auditoria, também chamado de calendário de auditoria.

Ainda neste passo de auditoria, a aplicação permite a realização da avaliação de riscos específicos e os respetivos controlos. Cada risco tem uma “pontuação” associada, calculada a partir de dois componentes: a probabilidade de risco e o impacto associado. Durante a etapa de “teste de execução de auditoria”, o Pentana planeia e realiza testes de auditoria e memoriza os resultados significantes obtidos. Os pontos de situação finais e conclusões de cada etapa serão a base para gerar um relatório de auditoria em que são dadas recomendações necessárias.

Pentana destingue-se por uma abordagem nova: não realiza uma análise detalhada dos dados do cliente, mas enfatiza documentação de todas as etapas da missão de auditoria e a preservação do histórico.

B. Porquê Pentana? Quais os benefícios para as partes interessadas?

O software Pentana oferece vários benefícios e valor adicionado para todos os tipos de utilizadores.

1) Terceira linha de defesa

a) Comité de auditoria e CAE

- Mantém e melhora a metodologia de auditoria existente;
- Visão geral gráfica dos indicadores chave;
- Universo bidimensional de auditoria sobreposto com cobertura de auditoria;
- Identificação de departamentos sem resposta e ações atrasadas.

b) Gestores de auditoria

- Normalização e profissionalismo aumentado;
- Planeamento de auditorias de base no risco;
- Dashboards e relatórios interativos;
- Entregáveis de auditorias normalizados e automatizados;
- Qualidade garantida a partir de revisões documentadas;
- Gravação e relatórios de timesheets;
- Monitorização de ações normalizada e automatizados.

c) Auditores

- Planos de trabalho estruturados e normalizados;
- Compartilhamento de conhecimentos e experiência de auditorias;
- Trabalho offline;
- Documentação de trabalho de campo incluindo formatação de texto;
- Anexos drag-and-drop;
- Várias dashboards interativas.

2) Segunda linha de defesa

a) Conformidade, SOX e IC officers

- Gestão de incidentes e atribuição de ações;
- Controlo de autoavaliações com revisões;
- Ciclo de avaliações regulares com lembretes por email;
- Controlo de cobertura e análises de matriz.

b) Gestores de risco

- Gestão de problemas chave e ligação com riscos operacionais;
- Autoavaliação de riscos com revisões;
- Ciclo de avaliações regulares com lembretes por email;
- Análise de exposição de risco e heat map.

3) Primeira linha de defesa

a) Gestores, entidades auditadas, proprietários de ações

- Documentação de incidentes via interface web;
- Seguimento de ações baseado na web com lembretes por email.

b) Departamento informático

- Deployment eficiente com tecnologia Click-Once;
- Autenticação transparente e segura via sign-on singular.

C. Interface do software Pentana

1) Home Screen

O **Home Screen** é a interface inicial apresentada quando se inicia o software. O utilizador pode configurar esta interface com até vinte “**tiles**” pré-definidos com informação relevante.

No topo da aplicação é onde se localiza o “**ribbon**” que apresenta botões para várias funções e links configuráveis para aplicações e ficheiros externos. A navegação é feita por diferentes módulos via “navegador” (“**spine**”) na esquerda.

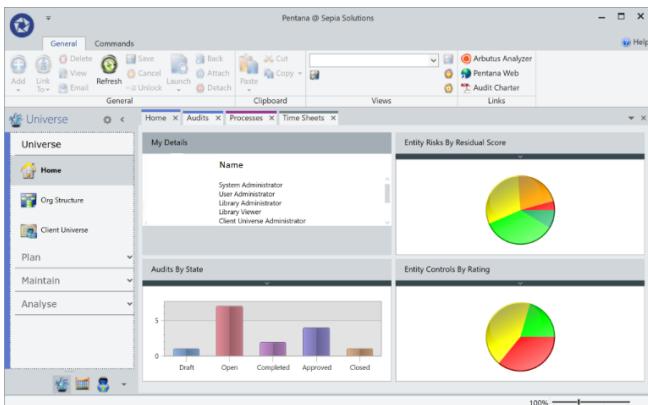


Imagen 5 – Home Screen do software Pentana

2) Módulos

A interface inclui mais de setenta e cinco módulos (ecrãs funcionais) por defeito. Estes módulos são organizados em seis grupos distintos: universo, trabalho da entidade, período de planeamento,

“biblioteca” (**Library**) e administrador. Cada um dos grupos contém vários “**ecrãs**” ou “**módulos**”.

Por via de permissões (**Permissions**), utilizadores chave (**key users**) podem esconder os botões que interligam para esses ecrãs, e assim apresentarem uma interface de utilizador simplificada contendo apenas os módulos relevantes.

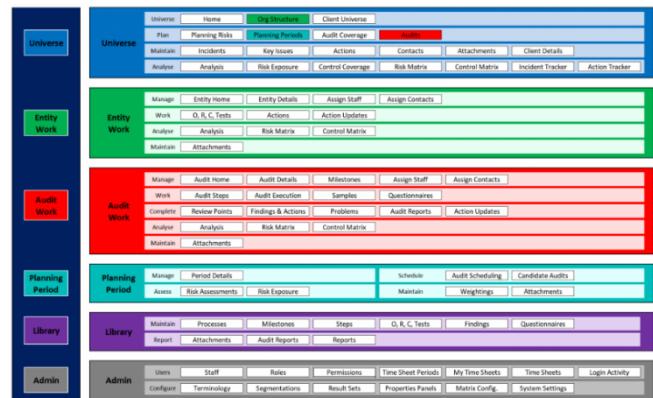


Imagen 6 - Módulos de interface

3) Vistas

As vistas (**views**) são extremamente versáteis e flexíveis. O utilizador pode modificar todas as vistas em todos os módulos de acordo com os requisitos de dados. Não só pode mostrar ou esconder, mas também pode agrupar e filtrar registos. Finalmente, várias funções como **count**, **total** e **average** estão disponíveis nos campos numéricos.

Os utilizadores chave (**key users**) podem definir boas vistas básicas em todos os ecrãs frequentemente visualizados. Podem também compartilhar essas vistas funcionais com os seus colegas de trabalho.

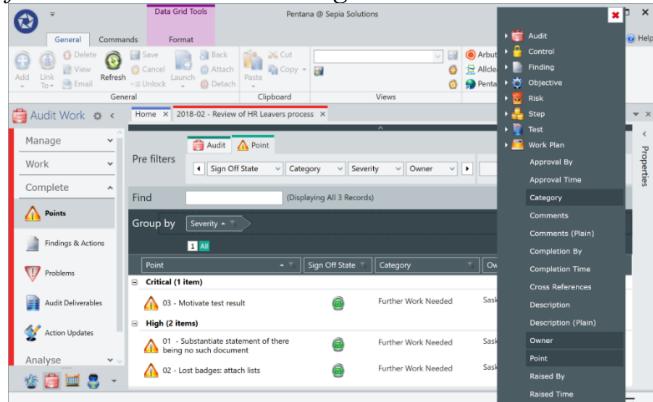


Imagen 7 – Menu de modificação de vistas

D. Modelação do universo da auditoria ou GRC

1) Staff & Contactos

a) Staff

Os **staff users** são tipicamente constituídos pelos utilizadores principais como os auditores, oficiais de conformidade e gestores de risco.

Os administradores configuraram as contas para o staff e podem incluir parâmetros como nome, iniciais, email, contacto, entre outros, como vários campos relacionados com o acesso e permissões.

Imagen 8 – Vista de administrador

b) Contactos

Os contactos (**contacts**) são tipicamente pessoas “do negócio” (como entidades auditadas, gestores, proprietários de ações, entre outros) que são documentados no Pentana e são opcionalmente ligados a elementos como incidentes, achados ou ações. Os administradores ou utilizadores chave (**key users**) podem gerir todos os parâmetros para estes utilizadores. Os contactos podem (se for configurado) interagir com o sistema via email, templates two-way, interface web ou mesmo pela interface do software. Quando este tipo de utilizadores podem interagir diretamente, o seu acesso terá de ser configurado apropriadamente.

Imagen 9 – Vista de contactos

2) Entidades

As **entidades (entities)** representam tipicamente partes das organizações como departamentos ou localizações e são organizados em hierarquias.

Entidades fazem parte de uma dimensão do universo bidimensional e são “mapeadas” para os processos (**processes**) (segunda dimensão).

Várias análises e ecrãs de relatório como exposição de risco (**risk exposure**), cobertura de controlo (**control coverage**), matriz de risco (**risk matrix**) e matriz de controlo (**control matrix**) usam a informação armazenada no nível de entidades.

Imagen 10 – Vista de entidades

3) Processos

Os processos (**processes**) fazem parte da segunda dimensão do universo bidimensional e são a chave para componentes ligados como objetivos, riscos, controlo e testes.

A combinação de entidade-processo (**entity-process**) é crucial para mapear elementos como âmbito de auditoria (**audit scope**), âmbito de incidente (**incident scope**), problemas chave (**key issues**), riscos de planeamento (**planning risks**), problemas (**issues**), achados (**findings**) e ações (**actions**).

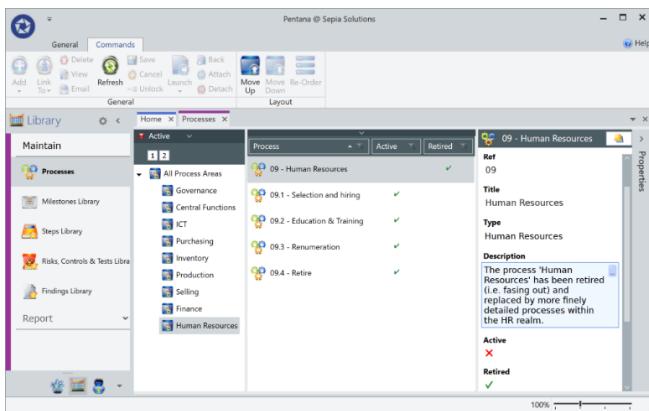


Imagen 11 – Biblioteca de processos

a) Mapeamento entidade-processo

Reunindo as duas dimensões do universo, os administradores ou utilizadores chave (**key users**) “mapeiam” quais processos ocorrem com cada entidade. Isto diz ao Pentana “o que” acontece “onde”. Os administradores podem usar parâmetros adicionais para cada secção como frequência fixa de auditoria (**fixed audit frequency**), esforço de orçamento (**budget effort**), proprietário (**owner**), proprietário de negócio (**business owner/contact**) e comentários.

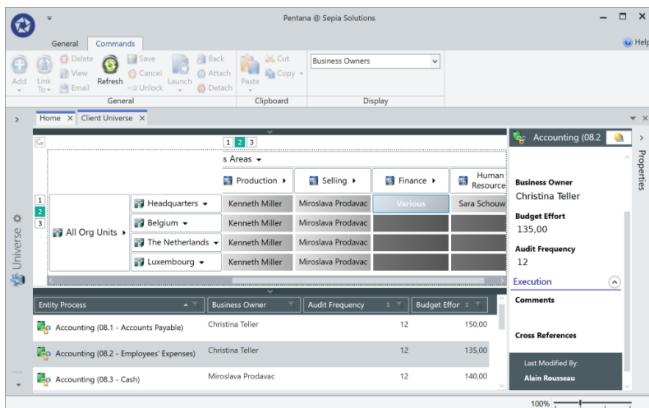


Imagen 12 – Mapeamento entidade-processo

4) Bibliotecas

a) Milestones

As **milestones** são usadas para guardar as datas chave para a auditoria, que são documentadas e relatadas comparando as datas planeadas e datas reais.

Os utilizadores chave (**key users**) as milestones. Estas milestones são automaticamente relacionadas à auditoria quando a auditoria é criada.

As milestones podem ser usadas para informar em várias maneiras. Uma delas é mostrar próximas milestones ou milestones atrasadas no Home Screen.

Outra maneira é relatar a variância entre o planeado e as datas reais.

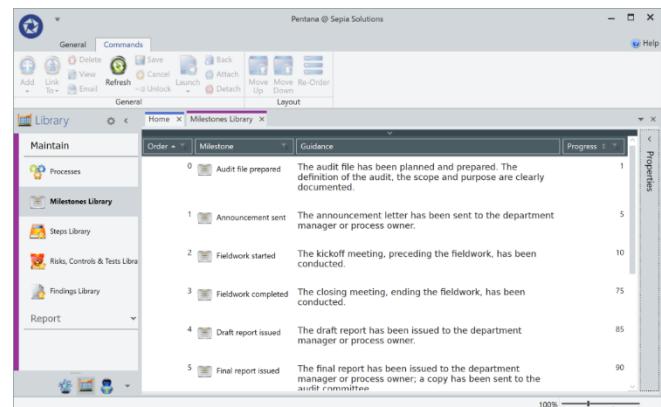


Imagen 13 – Biblioteca de milestones

b) Etapas

Esta biblioteca tipicamente reflete o manual de auditoria e contém uma série de fases (**phases**) e etapas (**steps**) de auditoria. Estas fases e etapas podem estar ligadas ao tipo de auditoria (**audit type**) para que quando a auditoria é criada somente as etapas apropriadas são extraídas da biblioteca.

Parâmetros como ref, título, descrição e orientação (**guidance**) são tipicamente armazenados nestes componentes.

O campo de orientação (**guidance**) em particular, é um campo em que os conhecimentos de auditores experientes podem ser armazenados, documentando não só “o que”, mas também o “como” ou outras informações que poderão ajudar os colegas de trabalho.

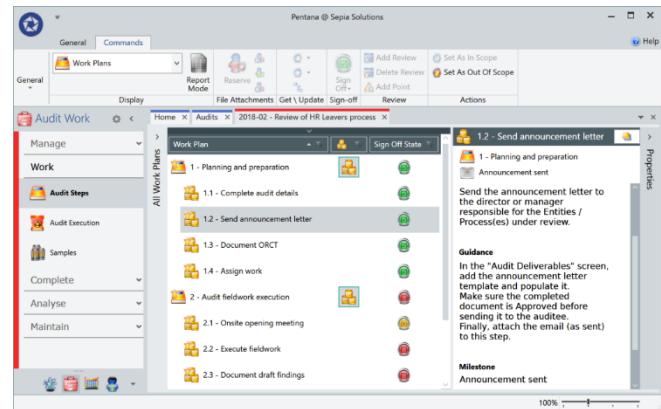


Imagen 14 – Biblioteca de etapas

c) Objetivos, riscos, controlo e testes

Esta biblioteca começa com a estrutura de objetivos (**objectives**) ligados a processos específicos.

Vários riscos podem estar anexados a cada objetivo. A mesma ligação um-para-muitos é usada para elementos filho (riscos, controlo e testes).

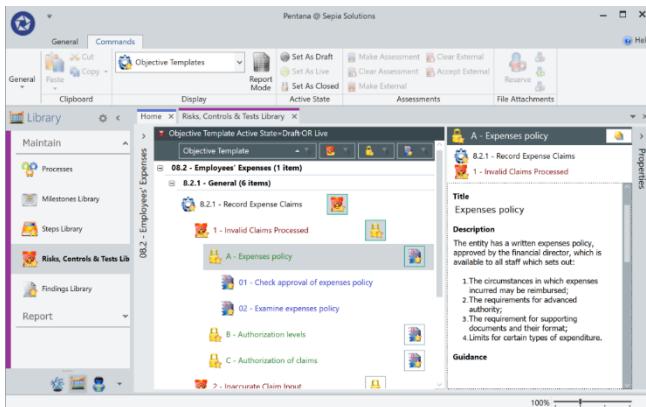


Imagen 15 – Biblioteca de objetivos, riscos, controlo e testes

E. Suporte à primeira e segunda linha de defesa

1) Gestão de incidentes

Incidentes (incidents) e eventos de perda (loss events ou near misses) são a base da gestão de riscos operacionais e, de uma maneira mais geral, gestão de risco organizacional. Os incidentes podem ser documentados no Pentana baseando-se em vários parâmetros incluindo valor monetário que reflete perda real ocorrida na organização e pode ser opcionalmente ligado a um âmbito (entity-processes) e riscos de entidade (entity risks). Para gerir incidentes, podem ser criadas ações e ser parte do seguimento de ações (action follow-up).

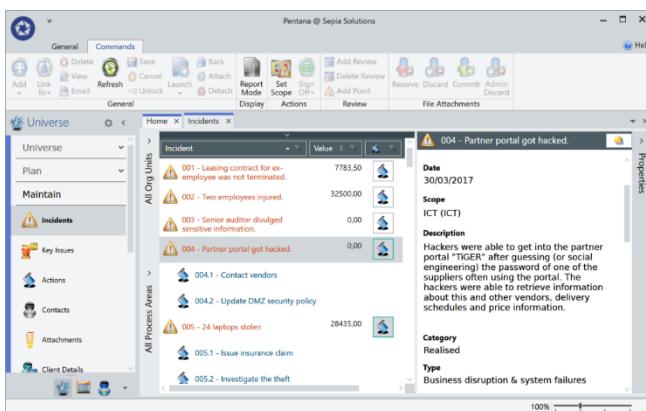


Imagen 16 - Gestão de incidentes

2) Riscos de entidade e controlo

Quando o universo é criado, podem ser documentados os objetivos, riscos, controlo e testes (ORCT) dentro de entidades.

Existe uma estrutura hierárquica destes componentes ORCT e para cada componente existem vários parâmetros com o objetivo de documentar detalhes relevantes. Podem ainda ser adicionados anexos (attachments) a estes componentes.

Opcionalmente, pode ser definido um proprietário (owner) a estes elementos ORCT, dando a esse indivíduo acesso aumentado para gerir esses elementos, fazer autoavaliações (self-assessments) ou fazer revisões (reviews).

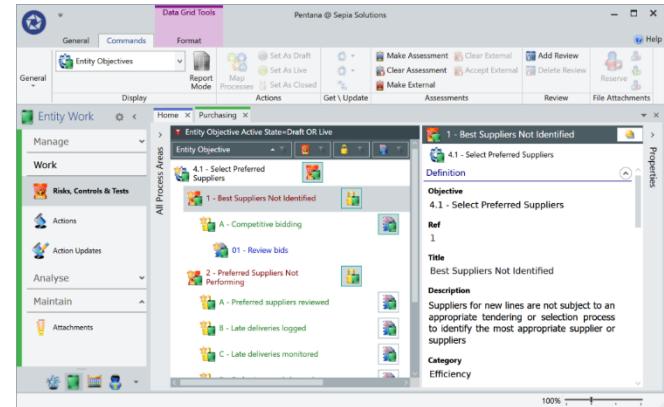


Imagen 17 – Riscos de entidades e controlo

3) Autoavaliações

a) Interface de utilizador

As avaliações (assessments) podem ser feitas para riscos e controlo. Para riscos a probabilidade (likelihood) e o impacto (impact) são documentados para ambos riscos inerentes (inherent) em risco residual (residual), enquanto que os controlos (controls) são pontuados com base no design e operação (operation).

Pentana permite duas perspetivas para estas pontuações, tipicamente uma é usada para documentar autoavaliações. Estas autoavaliações podem ser feitas via software ou via interface web.

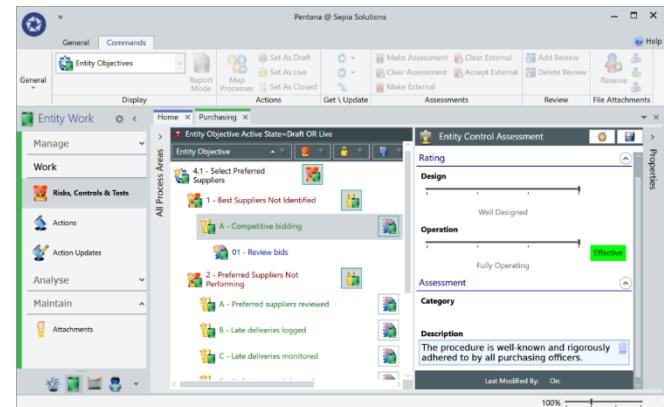


Imagen 18 - Autoavaliações via software

b) Browser/Interface web

Quando o sistema e utilizadores tiverem sido configurados, os utilizadores de negócio (**business users**) podem documentar o risco e controlar autoavaliações (**self-assessments**) pela interface web sem necessitar instalar software ou plugins adicionais. Adicionalmente, as autoavaliações podem fazer parte do ciclo regular (mensal, trimestral, anual) onde o sistema convida os utilizadores via email para documentar essas avaliações.

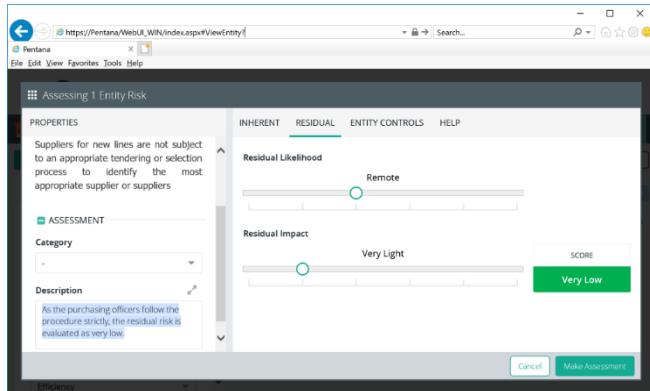


Imagen 19 - Autoavaliações via interface web

4) Riscos chave/Problemas chave

Os problemas chave (**key issues**) são usados para modelar estratégias ou macro riscos (**strategic or macro risks**) de alto nível que afetam toda a organização. Estes requerem atenção, gestão e, frequentemente, gestores de riscos operacionais em níveis baixos pelo negócio. Os problemas chave são definidos ao nível do universo e podem estar ligados a múltiplos riscos de entidade (**entity risks**) e/ou problemas de auditoria (**audit problems**).

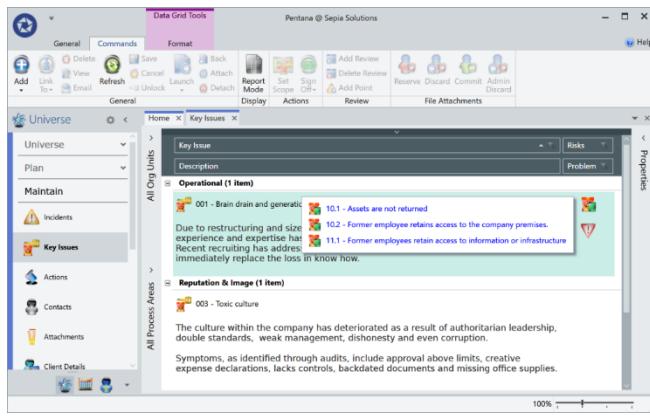


Imagen 20 – Riscos chave/Problemas chave

5) Tolerância de riscos

a) Tolerância de riscos versus Pontuação real

Por dois campos personalizados (**custom fields**) adicionados ao Pentana pela Sepia Solutions, os utilizadores podem documentar a tolerância da organização para cada problema chave (**key issue**), bem como a pontuação real estimada baseada na análise e julgamento profissional.

Naturalmente, os problemas chave com a pontuação (**score**) acima do nível de tolerância devem ser abordados pela organização. O Pentana pode desempenhar um papel fundamental na identificação destes riscos.

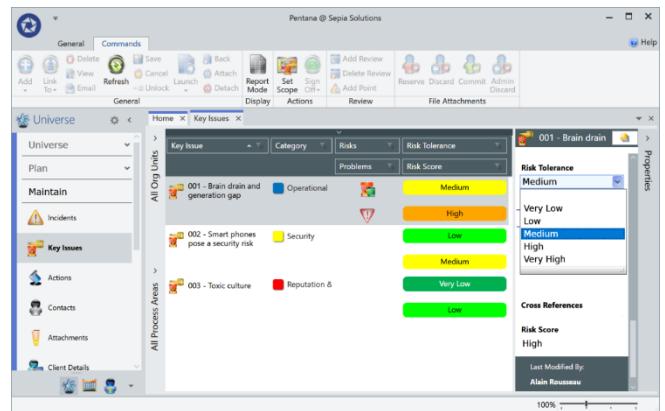


Imagen 21 - Tolerância de riscos

b) Comparação de riscos chave com riscos de entidade

Com o uso do “**Report Mode**”, ambos os problemas chave (**key issues**) e os riscos de entidade (**entity risks**) ligados podem ser apresentados. Deste modo, cada pontuação de riscos de entidades (**entity risk scores**) pode ser comparada com o nível de tolerância de risco (**risk tolerance**) como definido no problema chave.

Isto pode permitir a identificação individual de riscos de entidade que necessitam de atenção. Este ecrã também providencia informação pertinente para estimar a pontuação de risco geral do problema chave.

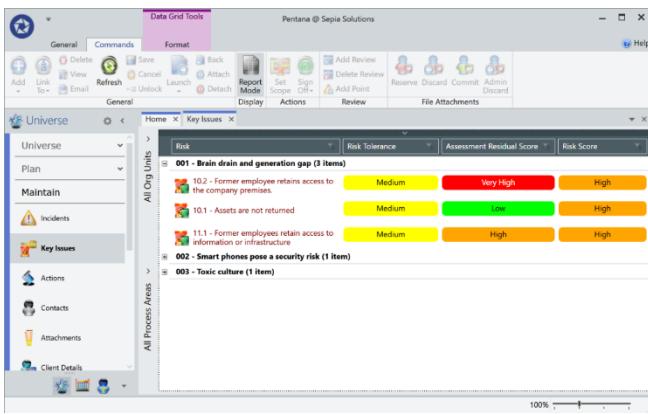


Imagen 22 — “Report Mode”

F. Suporte à auditoria interna

1) Auditorias

a) Visão Geral

O ecrã de auditorias (**audits**) lista todas a auditorias ou projetos semelhantes armazenados no Pentana e providencia a maneira mais fácil de criação.

Enquanto entidades (**entity**) modelam partes da organização que são relativamente estáveis ao longo do tempo, auditorias são projetos que começam e acabam para que ao longo do tempo várias auditorias cobrem o mesmo âmbito novamente.

A auditoria torna-se num recipiente para muitos outros componentes como etapas (**steps**), objetivos (**objectives**), riscos (**risks**), controlos (**controls**), entre outros.

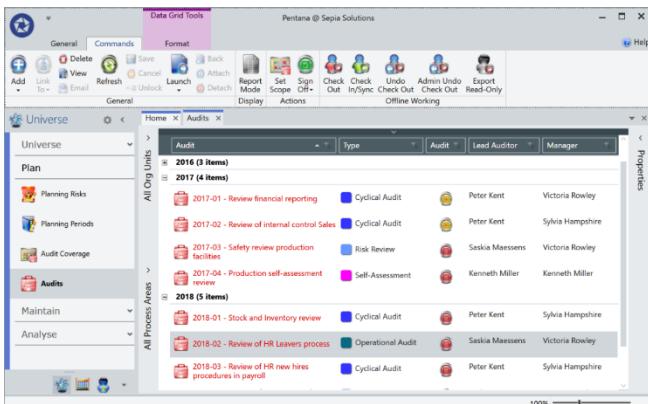


Imagen 23 — Interface de Auditorias

b) Detalhes de auditorias

Por defeito, existem aproximadamente trinta propriedades que podem ser armazenadas no registo da auditoria. Estes incluem ref, nome, tipo, descrição, propósito, âmbito, gestor, entre outros.

Campos como a descrição, propósito e conclusão são “campos de texto ricos” que podem armazenar uma

quantidade de texto quase infinita. Este texto pode ser formatado.

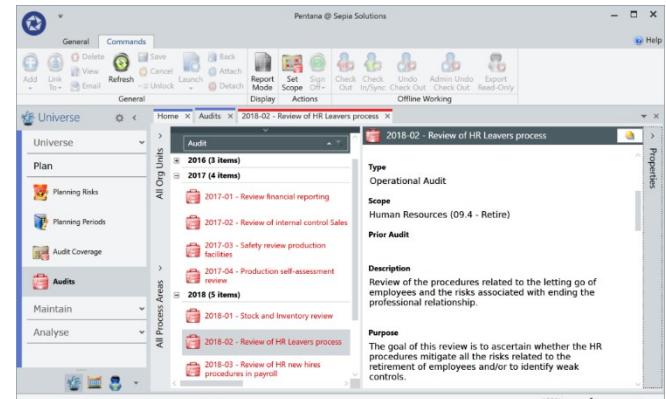


Imagen 24 — Painel de detalhes de auditorias

2) Metodologia de auditoria

Tipicamente, uma grande parte da metodologia de auditoria é capturada nas etapas de auditoria (**audit steps**).

Os utilizadores chave (**key users**) configuram as fases (**phases**) e etapas (**steps**) para cada tipo de auditoria (**audit type**) na biblioteca e quando os auditores começam a trabalhar nas auditorias, estas são automaticamente adicionadas.

Anexos apropriados são também extraídos e adicionados.

Quando uma etapa é realizada, o auditor pode documentar algo no campo de comentários, adicionar notas ou anexar documentos antes de marcar a etapa com completa (**completed**).

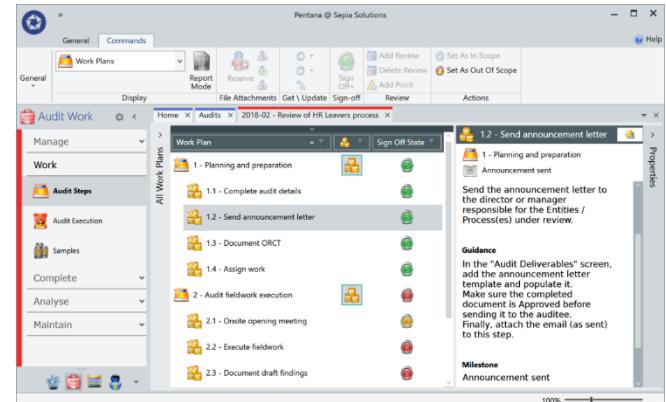


Imagen 25 — Painel de passos da auditoria

3) Carta de comunicado

O modelo de carta de comunicado (**announcement letter model**) pode ser armazenado como anexo numa etapa, ou como ficheiro especial (“Entregável de Auditoria”). Este pode ser o modelo atualmente usado pelo departamento de auditoria.

A Sepia Solutions pode adaptar o modelo para popular automaticamente com informação armazenada no Pentana. Isto resulta numa criação eficiente de normalização de documentos e relatórios.

4) Trabalho Offline

a) Check Out

Os auditores podem dar “check out” em uma ou mais auditorias para continuar a trabalhar enquanto estão offline. Durante o check out, podem selecionar que informação desejam levar com eles como “Read Only”, e partes que desejam editar (Check Out). Para prevenir potenciais conflitos na atualização, mais nenhum utilizador pode atualizar componentes que foram checked out. O auditor pode, posteriormente, trabalhar nos dados offline e dar “Check-In” ou sincronizar os dados quando se conectar de novo.

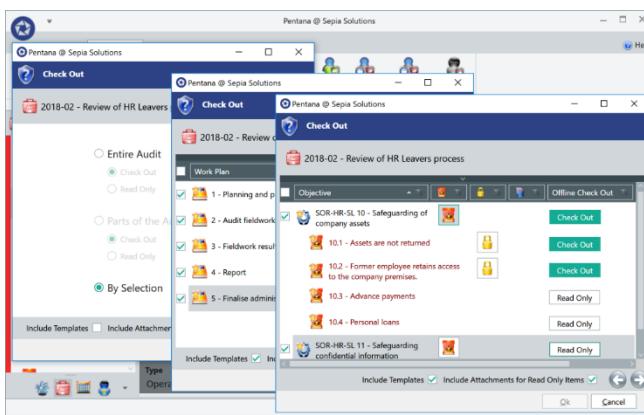


Imagen 26 — Como exportar componentes de uma auditoria com check-out ou read-only

b) Exportar read-only

Uma funcionalidade deste software é a possibilidade de exportar múltiplas auditorias como um todo, como um ficheiro ZIP. O ficheiro ZIP gerado inclui o pacote inteiro do software. Desta maneira, é possível exportar a auditoria completa para terceiros como auditores externos ou organizações supervisoras. Os componentes exportados são também ideias para apresentações ou sessões de formação, ilustrando as capacidades do Pentana sem arriscar mudanças nos dados da auditoria.

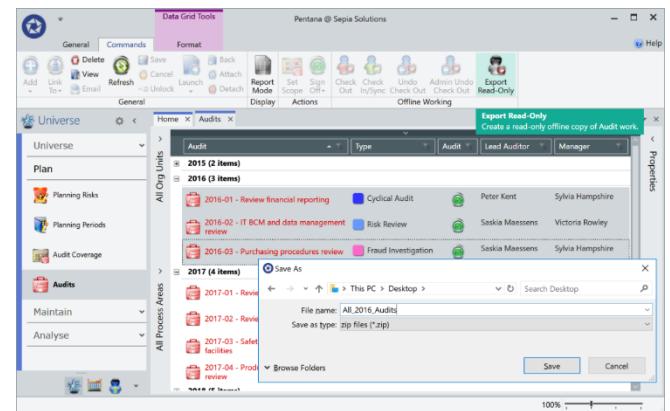


Imagen 27 — Como exportar uma auditoria completa como read-only

5) Trabalho de campo e documentação

a) Executar testes de trabalho de campo

O real trabalho de auditoria ou trabalho de campo é tratado no ecrã de execução de auditoria (**audit execution**) e é estruturado como **ORCT (Objetivos, Riscos, Controlo e Testes)**. Esta estrutura faz com que seja fácil considerar os vários aspectos do processo em questão e conduz logicamente para “como” o auditor pode verificar a eficácia dos controlos internos.

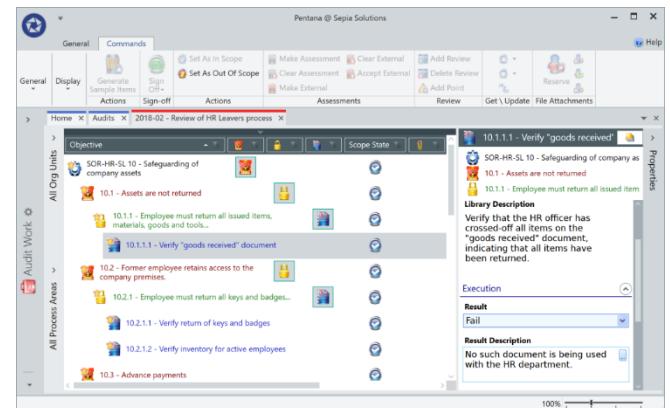


Imagen 28 — Execução de testes

Nesta imagem o teste “Verify the goods received document” falha visto que o documento não está a ser usado pelos recursos humanos. O auditor marca o resultado do teste como falhado e adiciona comentários que motivam a escolha.

b) Avaliação de controlo

Baseando-se nos testes, o auditor pode fazer uma avaliação informada sobre os controlos. Definindo definições sobre os níveis de design e operação na secção de avaliação de controlo (**control assessment**), a eficácia é calculada com base na matriz pré-definida. Idealmente, o auditor motiva os valores de avaliação. Podem ser adicionados anexos a qualquer

componente **ORCT** para documentar as razões para a avaliação documentada.

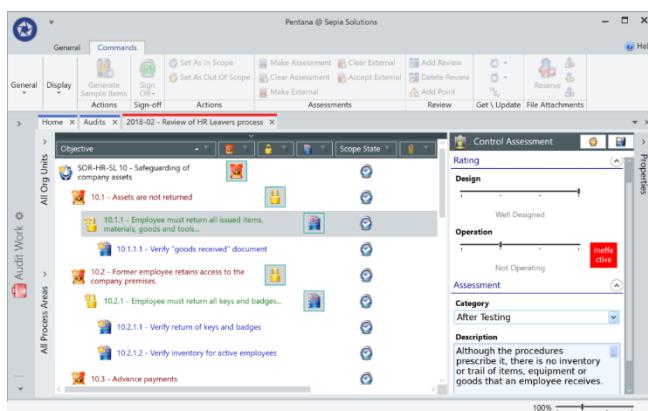


Imagen 29 — Avaliação de controlo

c) Avaliação de risco

Baseando-se na avaliação de controlo, o auditor pode fazer uma avaliação de risco (**risk assessment**) informada. A avaliação de risco baseia-se na probabilidade (**likelihood**) e impacto (**impact**). Em grande parte, a avaliação é baseada no julgamento profissional e por isso aconselha-se que o auditor motive a avaliação no campo de texto.

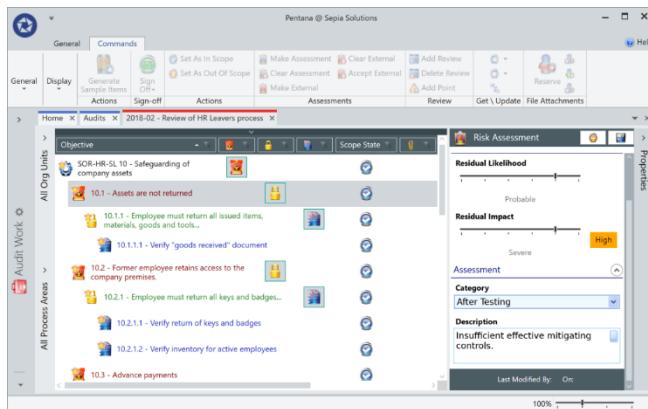


Imagen 30 — Avaliação de risco

d) Visão geral e resultados de trabalho de campo

Cada utilizador pode definir vistas (**views**) para apresentarem os dados da maneira que preferem, ou utilizadores chaves (**key users**) podem preparar vistas úteis para a equipa. Desta forma, todos os resultados e avaliações podem ser facilmente apresentadas em uma vista geral, ajudando o auditor a formular comentários opcionais para objetivo (**objective**), documentar achados (**findings**), ou fazer um rascunho

de conclusão de auditoria (**audit conclusion**). É também de referir que componentes **ORCT** podem ser marcados como “Fora de Âmbito” (**out of scope**) se não forem relevantes.

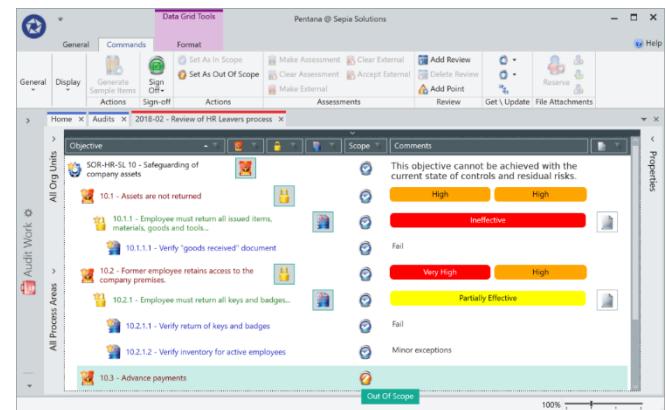


Imagen 31 — Visão geral e resultados dos campos de trabalho

6) Achados & Problemas

a) Achados

O auditor pode documentar achados (**findings**) ligados ao processo revisado, ou a um objetivo, risco, controlo ou teste individual. Um achado inclui campos como ref., título, descrição e recomendação, bem como severidade (**severity**), categoria (**category**), causa (**cause**) e efeito (**effect**). Também existem campos disponíveis para capturar a resposta da entidade auditada perante o achado.

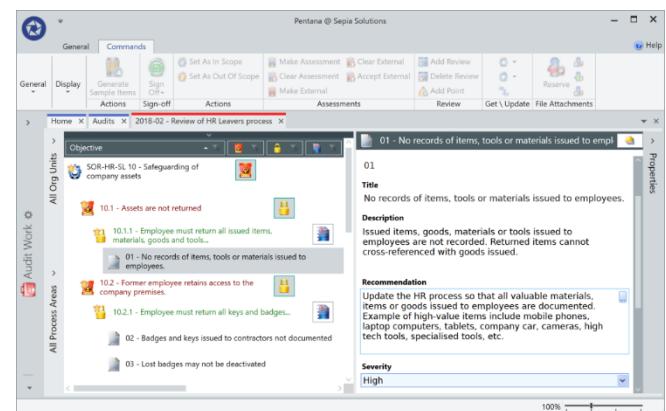


Imagen 32 — Achado

b) Problemas

O Pentana também providencia meios para consolidar vários achados em um ou mais problemas. Múltiplos problemas podem referir ao mesmo achado (**finding**) enquanto cada problema (**problem**) pode estar ligado a múltiplas ações (**actions**). Esta é uma maneira de

documentar problemas abrangentes descobertos durante a auditoria. Estes problemas podem ser incluídos no inicio do relatório de auditoria (**audit report**) como parte do resumo executivo.

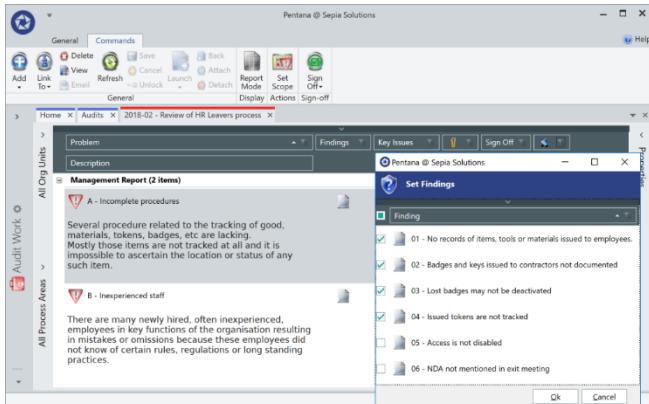


Imagen 33 — Adicionar achados a problemas

7) Medidas corretivas

Achados (**findings**) tipicamente resultam de uma ou mais medidas corretivas documentadas para a entidade auditada implementada. Um achado pode levar a múltiplas ações com diferentes deadlines e atribuídas a proprietários de ações. As ações incluem propriedades como ref, título, descrição, data-limite (**deadline**), proprietário (**owner**) e prioridade (**priority**). Estas ações são tipicamente discutidas com a entidade auditada e levam seguidamente como parte da abordagem da auditoria, no entanto não é típico acontecer durante a auditoria.

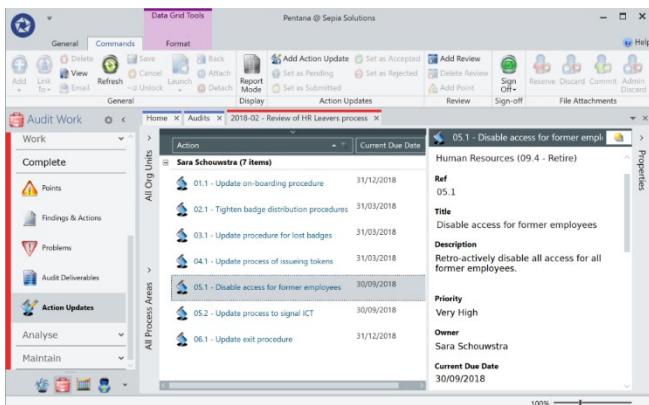


Imagen 34 — Medidas correctivas

8) Relatórios de auditoria automatizados

Os modelos de rascunho e do relatório final de auditoria podem ser armazenados como anexos nas etapas (**steps**), ou como “Entregáveis de Auditorias”.

A maneira de automatização destes relatórios é muito parecida com a automatização da carta de comunicado.

9) Garantia de qualidade

a) Pontos

O auditor procede com o trabalho de campo e dá “sign off” aos componentes enquanto procede. Idealmente o auditor líder ou gestor faz a revisão do trabalho antes de gerar o rascunho do relatório de auditoria. Se necessário o revisor documenta um ponto (**point**). Estes pontos têm um ciclo de vida e têm também de ser aprovados antes que a auditoria possa ser marcada de completa. O proprietário (**owner**) ou recipiente do ponto de revisão pode também ver o mesmo no home screen. Opcionalmente, a Sepia Solutions pode desenvolver uma regra de email para automaticamente enviar alertas para informar o proprietário do ponto.

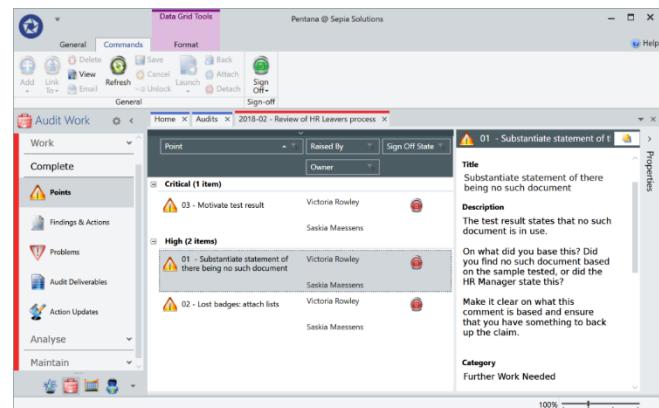


Imagen 35 — Criação e detalhes de pontos

b) SignOff

Pentana atua como guardião, na maneira de que não permite que a auditoria seja marcada como completa (**completed**) até os componentes fundamentais sejam marcados como aprovados.



Imagen 36 — é uma ilustração, tirada dos materiais de formação desenvolvidos pela Sepia Solutions, visualiza esta verificação por icons verdes nas bordas das células. A ilustração também destaca que componentes da auditoria são editáveis (texto preto) ou read-only (texto cinzento) em cada estado de auditoria (audit states).

G. Rastreamento de ações/Seguimento de ações

1) Ciclo de seguimento

a) Ciclo de seguimento de ações

As partes automatizadas do ciclo de seguimento consistem em três tarefas:

- Criação de atualizações de ações;
- Notificações por email para proprietários da ação;
- Lembretes por email para proprietários da ação.

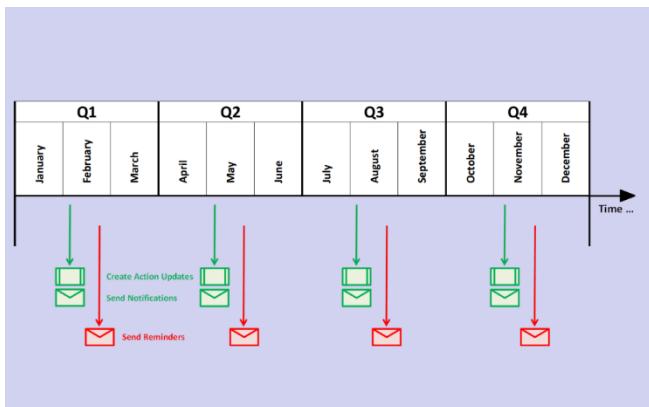


Imagen 37

O ciclo pode ser ajustado à maneira de trabalho da organização por configuração destas tarefas. Neste exemplo é assumido que o ciclo de rastreamento é começado no início de cada segundo mês de cada trimestre e completado até ao fim desse mês.

b) Registos de atualização de ação

Uma ação pode existir por um longo período de tempo antes de ser completamente implementada ou fechada e durante esse tempo é necessário documentar o progresso. No entanto, não é inteligente simplesmente fazer um “overwrite” no estado prévio da ação. O Pentana permite a criação de registos adicionais chamados de atualizações de ação (**action updates**). A criação destas atualizações pode ser manual, mas tipicamente é automatizada como parte do ciclo de seguimento de ação (**action follow-up cycle**).

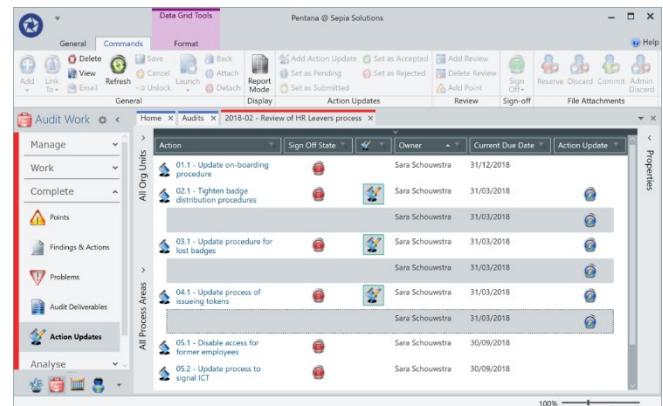


Imagen 38 — Action follow-up cycle

Neste exemplo, as atualizações de ação são criadas apenas para ações que estão quase na data-limite (só três atualizações foram criadas).

2) Fornecimento de atualizações por proprietários de ações

a) Interface web: Vista global de atualizações de ação A maneira mais flexível e eficiente de obter feedback pelos proprietários de ações é a interface web. Seguindo um link enviado por notificação por email, os proprietários da ação são enviados para uma visão global de todas as atualizações de ações (**action updates**). Os proprietários de ação têm flexibilidade para providenciar de feedback a essas atualizações de ações como for conveniente. Desta maneira, não é preciso ter o software instalado.

Imagen 39 — Vista global de ações (Interface web)

b) Interface web: Submeter atualizações de ações Pela visão geral apresentada na imagem acima, os proprietários de ação podem escolher a atualização de ação e rever as suas propriedades, notas, anexos e informações contextualizadas. Especificamente, os proprietários de ações podem providenciar feedback como uma nova resolução (*resolution/status*), data de implementação (*implementation date*), fazer upload de anexos, entre outros, antes de submeter o seu feedback.

Imagen 40 — Submissão de ações (Interface web)

3) Rastreamento e relatório

a) Rastrear atualizações e revisão de feedback
Até este ponto, a auditoria ou o departamento **GRC** não teve de fazer nada manualmente, mas agora o feedback recebido dos proprietários de ação necessita de ser revisto.

O ecrã de rastreamento de ação (*action tracking*) providencia uma das maneiras mais convenientes de analisar e rever atualizações de ação (*action updates*), em que é possível filtrar as mesmas. Baseando-se na informação dada pelo proprietário da ação, o revisor decide se aceita ou rejeita o input.

Imagen 41 — Rastreamento de atualizações e revisão de feedback

b) Visão global de relatório de atualizações de ação

Existem várias maneiras de providenciar uma visão geral de atualizações de ação (*action updates*) graficamente durante o ciclo de seguimento de ações.

Imagen 42 — Visão global do relatório de atualizações de ação

Na imagem acima pode-se observar de maneira simples e interativa de visualização geral. Neste caso, a maioria das atualizações estão em estado pendente (*pending*). Como estes gráficos, todas as secções são sensíveis ao contexto o que significa que é fácil chegar-se a um registo individual ou contexto.

4) Dashboards de auditoria e análise de funcionalidades

a) Cobertura de auditoria

O ecrã de cobertura de auditoria (*audit coverage*) apresenta as auditorias existentes no universo bidimensional. O ecrã pode dar zoom em combinações de entidades-processos (*entity-process*) de baixo nível, ou desdobradas ao nível agregado mostrando percentagens de 0% a 100%. Um ou mais anos podem

ser selecionados para análise, enquanto que critérios adicionais podem ser adicionados ao pré-filtro. Clickando na célula no topo do ecrã irá apresentar as auditorias correspondentes e os detalhes no fundo do ecrã.

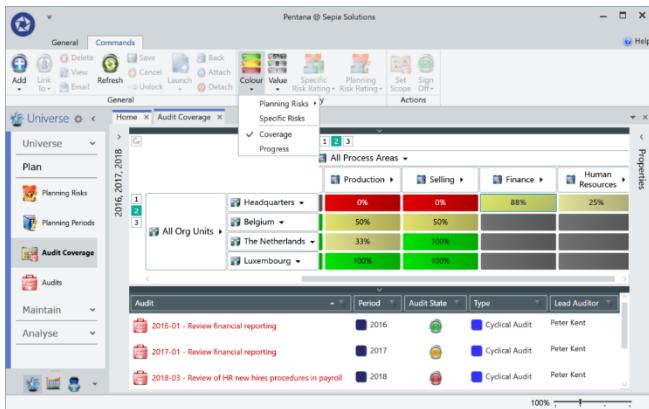


Imagen 43 — Dashboard de cobertura de uma auditoria

5) Exposição ao risco e heat map

a) Heat map de risco

O **heat map** é gerado baseando-se na matriz de risco configurável em que o número de riscos ao nível de entidades (**entity-level risks**), correspondentes a cada célula, são contados. Escolhas de análise adicionais incluem a pontuação inherente/residual, ou avaliações de risco (**risk assessments**) internas/externas. Como todos os ecrãs de análise, clickar em qualquer parte do gráfico irá apresentar os registos correspondentes no fundo do ecrã. Selecionar qualquer registo irá apresentar as propriedades à direita e permite ao utilizador ver tudo sobre o registo ou contexto selecionado.

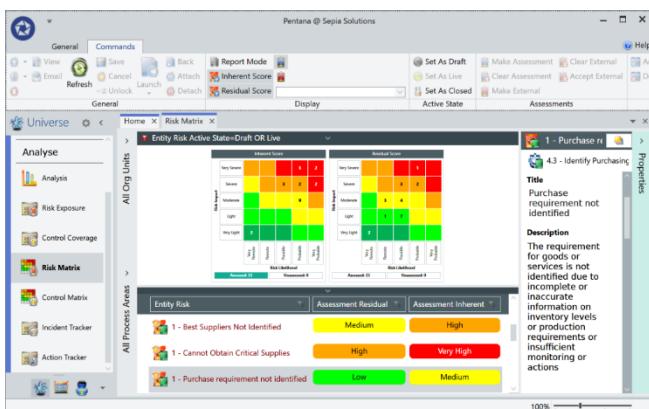


Imagen 44 — Mapa de exposição ao risco

b) Exposição de risco

O ecrã de exposição de risco (**risk exposure**) usa novamente o universo bidimensional como base para apresentar as pontuações agregadas (**aggregated scores**) dos riscos de entidade (**entity risks**). A pontuação influencia a cor da célula. Opcionalmente o movimento ou tendência da pontuação de risco é apresentada na visão geral gráfica.

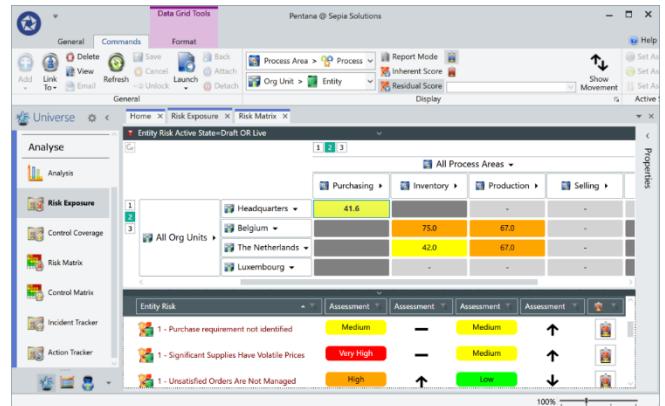


Imagen 45 — Ecrã de exposição ao risco

Na imagem acima, o movimento é apresentado no fundo do ecrã como parte dos detalhes correspondentes à célula selecionada (**Purchasing**) na matriz.

6) Matriz de controlo e cobertura

a) Matrix de controlo

O oposto ao **heat map** de risco é o ecrã de matriz de controlo (**control matrix**) onde todos os controlos de nível de entidade (**entity-level controls**) são traçados na matriz configurada baseada no controlo de avaliações (**control assessments**) interno/externo. Esta visão geral torna fácil localizar os controlos deficientes. Clickando numa célula irá apresentar uma lista de todos os controlos nessa célula.

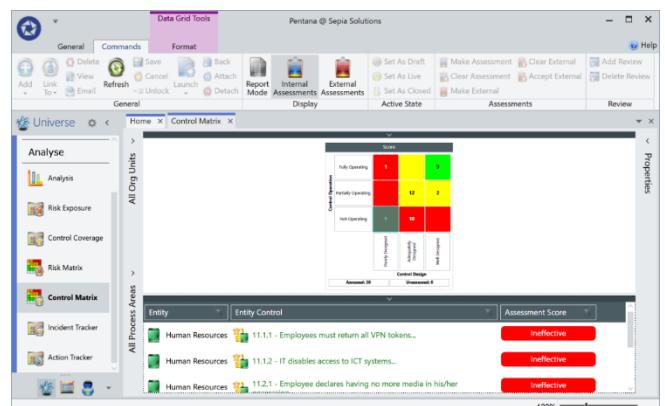


Imagen 46 — Matrix de controlo

b) Controlo de cobertura

O ecrã de controlo de cobertura (**control coverage**) usa o universo bidimensional como base e apresenta as pontuações agregadas (aggregated scores) de controlo de entidades (**entity controls**). Opcionalmente o movimento ou tendência da pontuação de risco é apresenta na visão geral gráfica.

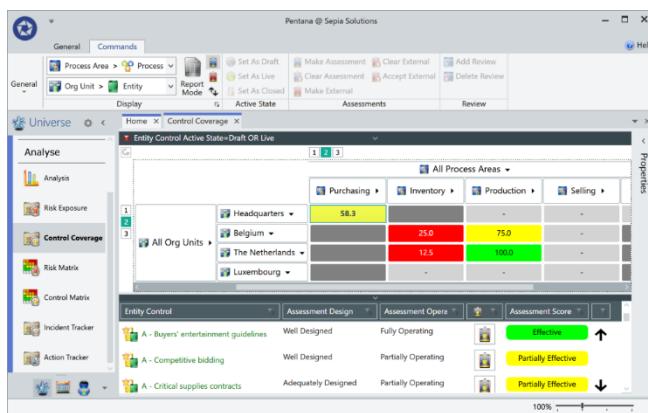


Imagen 47 — Matrix de cobertura

Na imagem acima, o movimento é apresentado no fundo do ecrã como parte dos detalhes correspondentes à célula selecionada (**Purchasing**) na matriz. Esta informação mostra onde a organização está realmente em controlo ou não.

7) Rastreamento de incidentes e ações

a) Rastreamento de incidentes

O ecrã do rastreador de incidentes (**incident tracker**) usa novamente o universo para tracejar os incidentes (**incidentes**). As células podem apresentar o número de incidentes (**number of incidents**) correspondentes ao pré-filtro ou o valor total monetário dos incidentes. Este módulo de análise providencia uma visão geral dos incidentes ou “quase incidentes” de toda a organização.

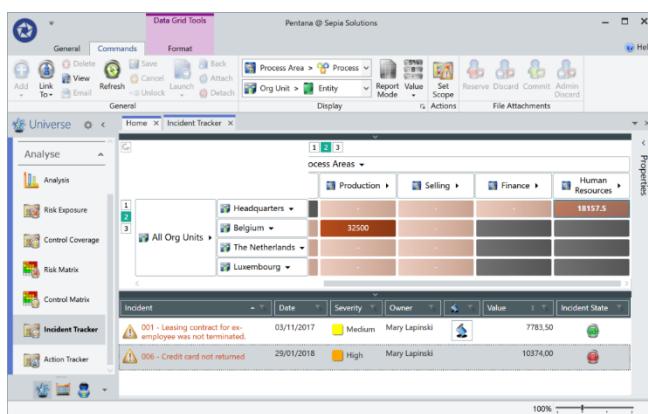


Imagen 48 — Rastreamento de incidentes

b) Rastreamento de ações

A maneira mais eficiente de rever e relatar seguimentos de ação (**action follow-up**) será a utilização do ecrã do rastreador de ações (**action tracker**). Neste ecrã as colunas/linhas do universo podem ser expandidas e colapsadas para dar zoom in ou agrregar. O número de ações apresentadas é influenciado pelos pré-filtros usados pelo utilizador.

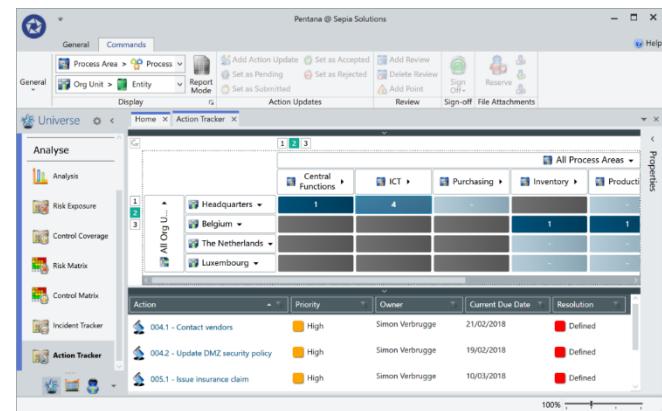


Imagen 49 — Rastreamento de ações

Este ecrã pode também ser usado para construir uma visão geral de “amadurecimento de ações” (**action aging**) como apresentado na imagem abaixo:

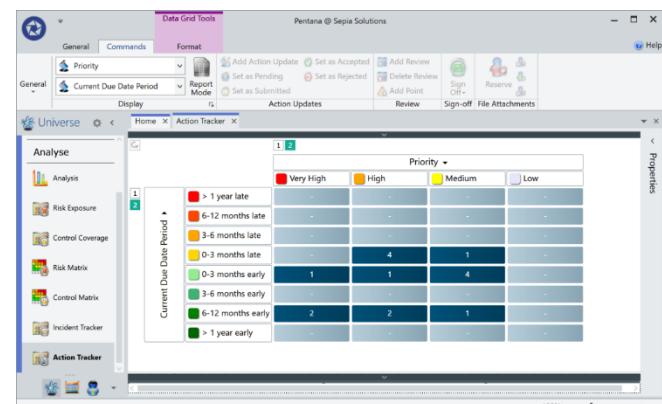


Imagen 50 — Visão geral de ‘amadurecimento de ações’

A análise na imagem acima parece-se muito com uma tabela pivot tracejando o número de ações baseado na sua prioridade e data-limite.

8) Análise on-the-fly

Questões de natureza estatística que não conseguem ser respondidas nas vistas normais ou ecrãs de propósito especial muito provavelmente podem ser respondidas no ecrã genérico de análise (**analysis screen**). Neste ecrã de análise de propósito geral, o

utilizador seleciona a componente (por exemplo incidentes, riscos, achados, auditorias, entre outros). Posteriormente seleciona o tipo de valor a usar e o tipo de gráfico e subsequentemente o campo a ser analisado. Certos tipos de gráfico podem funcionar com dois campos simultaneamente.

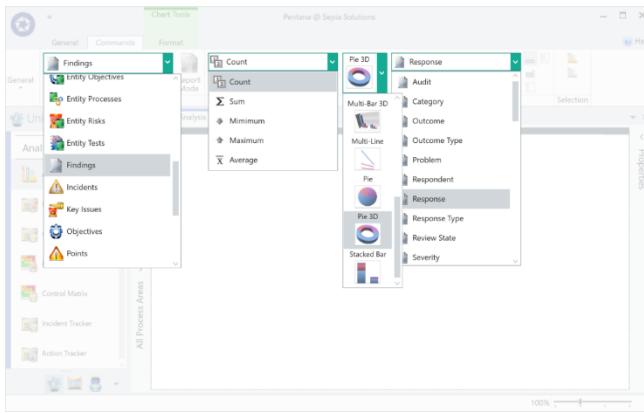


Imagen 51 — Dashboard de análise on-the-fly

Estes menus existem no módulo de análise, e podem ser interagidos na parte superior no software (**ribbon**).

H. Configuração e setup do Pentana software

1) Terminologia

O módulo de terminologia (**terminology**) permite aos utilizadores modificar o nome de todos itens, como componentes, campos individuais e mesmo botões de navegação. Uma auditoria pode ser rotulada de “investigação” (**investigation**) ou “projeto” (**project**), enquanto que um achado (**finding**) pode ser modificado para “problema” (**problem**) ou “observação” (**observation**). Campos individuais podem ser renomeados e dados orientações de estilo de tooltip.

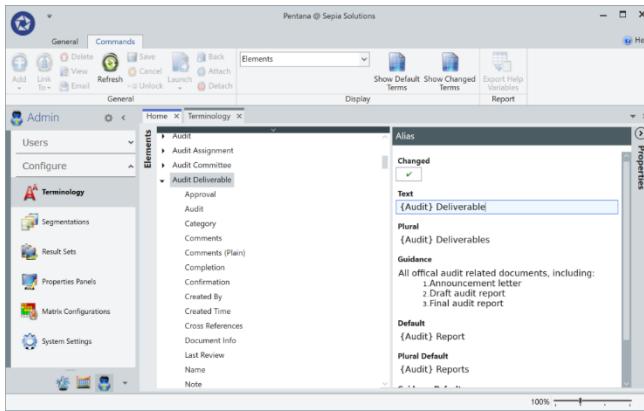


Imagen 52 — Configuração e setup de terminologia

2) Segmentação

As segmentações (**segmentations**) podem ser geridas no ecrã de segmentação. A maior parte das segmentações incluem campos adicionais como nome, descrição e cor. O nome é o valor chave para agrupar dados, descrição é apresentada quando o utilizador considera um valor a definir e a cor pode ser usada para relatórios gráficos.

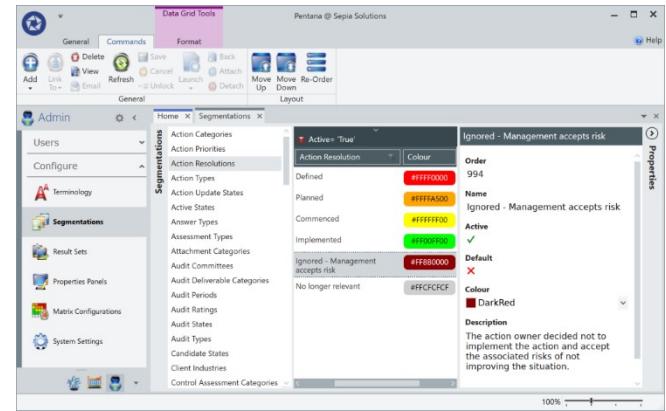


Imagen 53 — Configuração e setup da segmentação

3) Painel de propriedades

O layout do painel de propriedades (**properties panel**) pode ser modificado na sua totalidade. Utilizadores chave (**key users**) podem esconder campos do painel de propriedades, mover campos, reordenar as secções e colapsar secções menos utilizadas. Desta maneira a interface pode ser ajustada para mostrar campos de verdadeiro interesse para a organização.

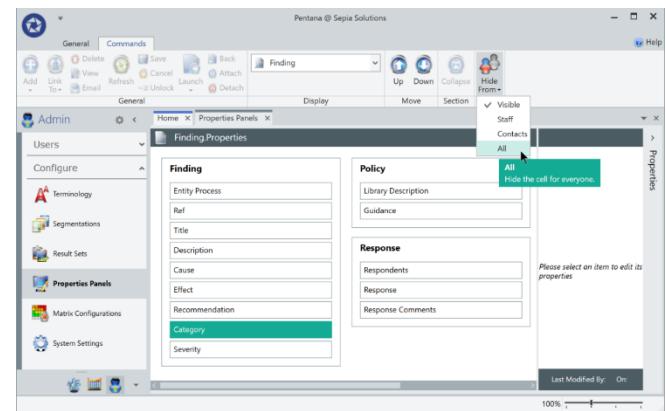


Imagen 54 — Painel de propriedades

4) Permissões

Pentana inclui cinco a seis papéis (**roles**) para cada um dos quatro níveis (**universo, cliente, entidade,**

auditoria). Utilizadores staff bem como utilizadores de negócio (**contact users**) são ligados a estes papéis. Estes papéis podem ser modificados pelos utilizadores chave (**key users**), modificando centenas de opções detalhadas que definem que acesso de um papel particular tem a certos elementos.

Permission	2.1 Universe Manager	2.2 Universe Departmental User	2.3 Universe User	2.4 Third Line
Delete Candidate Audits	Grant	Grant	Deny	Deny
Launch Candidate Audits	Grant	Grant	Grant	Grant
Launch Weightings	Grant	Grant	Grant	Grant
Launch Attachments	Grant	Grant	Grant	Grant
Launch Audit Coverage	Grant	Grant	Grant	Deny
Launch Audits	Grant	Grant	Grant	Grant
Read Standard Audits	All	Assigned	Assigned	Department
Read Confidential Audits	All	Assigned	Assigned	Department
Define Audits	Grant	Deny	Deny	None
Scope Audits	Grant	Deny	Deny	Assigned
Manage Audits	Grant	Deny	Deny	All
Confirm Audits	Grant	Deny	Deny	Deny
Undo Confirm Audits	Grant	Deny	Deny	Deny

Imagen 55 — Dashboard de permissões

Neste ecrã de permissões (**permissions**), pode-se não só modificar acesso a dados, mas também a acesso a módulos funcionais. Cada um dos módulos pode ser ligado ou desligado pela modificação de permissões. Esta é uma boa maneira de simplificar a interface de utilizador, escondendo funcionalidades não utilizadas.

I. Planeamento de auditorias baseado em risco

1) Períodos de planeamento

Para se começar a planear, o utilizador tem de definir um período de planeamento (**planning period**) que representa um timeframe para onde o planeamento é aplicável. Pentana permite a sobreposição de períodos, ou duplicados de períodos para que as atualizações possam ser bem processadas e documentadas. Pentana providencia meios de trabalho numa base estável durante o exercício de planeamento ou revisão do mesmo.

Planning Period	Active State	Start Date	End Date
Audit Planning 2017 Q1	Active	01/01/2017	31/12/2017
Audit Planning 2017 Q3 (revised)	Active	01/01/2017	31/12/2017
Audit Planning 2018 Q1	Active	01/01/2018	31/12/2018
Audit Planning 2018 Q3 (revised)	In Progress	01/01/2018	31/12/2018
Audit Planning 2019 Q1	In Progress	01/01/2019	31/12/2019
Audit Planning 2019 Q3 (revised)	In Progress	01/01/2019	31/12/2019

Imagen 56 — Dashboard de períodos de planeamento

2) Risco de planeamento

Riscos de planeamento (**planning risks**) são usados para representar riscos, tópicos ou temas de alto nível. Estes riscos são copiados para todos os processos-entidade (**entity-processes**) apropriados de um período de planeamento (**planning period**). Estão disponíveis vários campos para riscos de planeamento.

Planning Risk	Weight	Active	Process Type	Entity Type
Data loss	3,00	✓	Human Resources	ICT
Business Continuity	1,00	✓	ICT	Production Selling
Theft	4,00	✓	Inventory Production	
Industrial accidents	1,00	✓	Production	
White-collar crime	4,00	✓	HQ	
Fraud	4,00	✓	Finance Purchasing Selling	

Imagen 57 — Menu de risco de planeamento

3) Avaliação de riscos de planeamento

Após os riscos de planeamento (**planning risks**) sejam replicados em todos os processos-entidade (**entity-processes**), o utilizador pode começar a avaliá-los no âmbito da entidade e processo relacionados. Ao contrário dos riscos ao nível de entidade (**entity-level**) ou auditoria (**audit-level**), os riscos de planeamento não são acedidos usando probabilidade (**likelihood**) e impacto (**impact**), mas são baseados numa simples segmentação (**segmentation**). É de notar que as avaliações podem ser atribuídas a diferentes utilizadores.

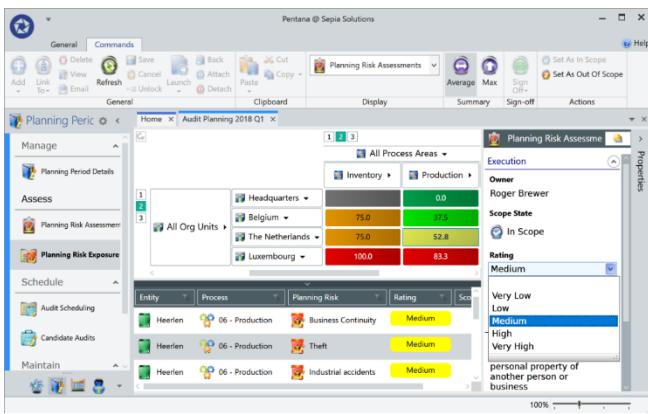


Imagem 58 — Menu de avaliação de riscos de planeamento

4) Fatores de agendamento

a) Aplicação de fatores de agendamento

Para assistir na criação do plano de auditoria, Pentana usa os seguintes fatores em consideração:

- Frequência de auditoria fixa;
- Classificação da última auditoria;
- Classificação de riscos de planeamento;
- Classificação de risco de entidade.

Ligar ou desligar estes fatores faz com o Pentana considere esse fator ou não na sugestão de onde planear uma auditoria durante o período de planeamento.

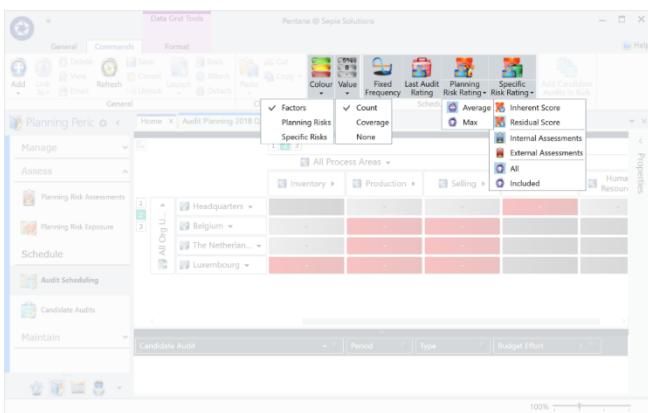


Imagem 59 — Aplicação de fatores de agendamento

b) Áreas sugeridas para o plano de auditoria e candidatos

Pentana não cria o plano de auditoria. Em vez disso, Pentana destaca áreas (**entity-processes**) no universo que, de acordo com os fatores implementados, devem ser auditados durante o período de planeamento (**planning period**) definido. O utilizador pode criar candidatos de auditoria (**candidate audits**). Quando o

utilizador coloca o cursor por cima de uma célula da matriz, um pop-up mostra a última data de auditoria e os diferentes fatores e pontuações (**factors and scores**). Neste ecrã as cores significam o seguinte:

- **Vermelho:** Uma auditoria deve ser planeada;
- **Amarelo:** Uma auditoria não deve ser planeada, mas um candidato foi criado;
- **Verde:** Uma auditoria não é necessária e nenhum candidato foi criado.

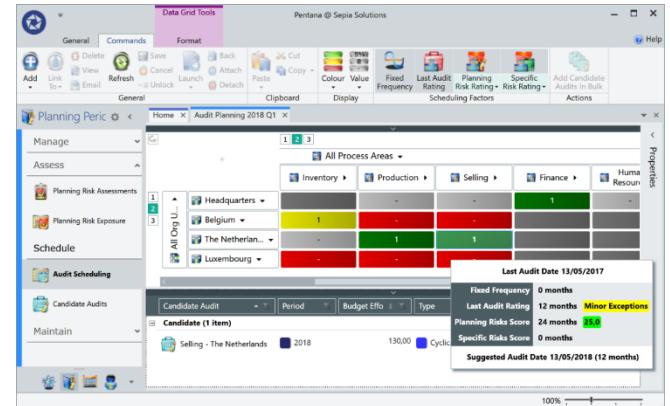


Imagem 60 — Áreas sugeridas para o plano de auditoria e candidatos

Os registos criados no ecrã da imagem 60 não são auditorias, são candidatos a auditoria. O gestor de auditoria pode estimar o orçamento para cada candidato e comparar este total com os recursos e tempo disponíveis da auditoria para esse período. O ecrã que será apresentado na imagem 61 é onde se pode decidir confirmar (**confirm**) ou não as potenciais auditorias, bem como observar todos os candidatos:

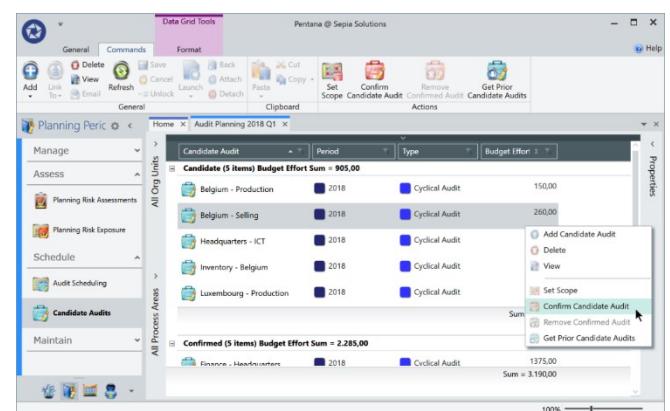


Imagem 61 — Gestão de potenciais candidatos

J. Timesheets

Membros da equipa de auditoria podem documentar quanto tempo é perdido no trabalho de auditoria e outras tarefas como reuniões, formação ou mesmo férias. Utilizadores chave (key users) podem configurar o sistema especificando que as timesheets são semanais, mensais, se os fins de semana são incluídos e se cada valor introduzido deve corresponder ao comprimento de um dia de trabalho normal.

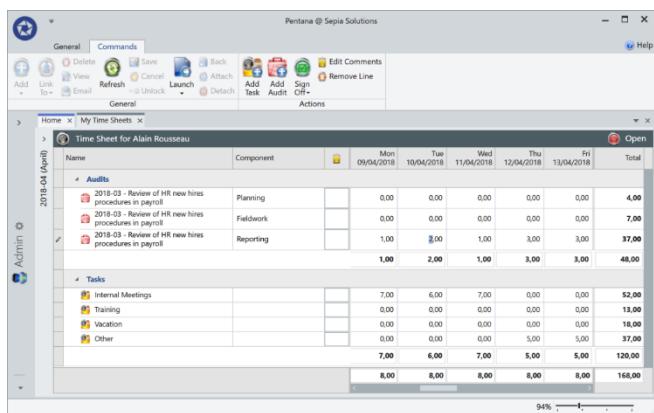


Imagen 62 — Timesheets

III. CONCLUSÃO

Antes de mais, é importante referir que até ao momento de desenvolvimento deste documento, o pedido para obter a demonstração do Pentana Audit não foi respondido, pelo que foi necessário o uso de outros recursos disponíveis online.

Concluindo, este documento deixa uma ideia geral da norma aplicável e como que um “tutorial” e explicação de como o software Pentana Audit funciona. É de referir que conforme visto no documento, este software é mais dirigido a organizações e à sua gestão no que toca a segurança de informação. É possível concluir que, apesar de ser uma norma e software em constante evolução, é de importante implementação para respeitar a privacidade dos dados e informação, especialmente quando se trata de um negócio.

Futuramente espera-se que cada vez mais negócios e organizações se certifiquem e implementem a norma descrita neste documento, seja em conjunto com outras normas ou não e apesar de ter sido apenas incluído o Pentana Audit é de lembrar que existe um vasto leque de outros softwares disponíveis, com vários tipos de monetização, implementação e até mesmo diferentes períodos de demonstração ou funcionalidades incluídas na demonstração.

IV. REFERÊNCIAS

- [1] How does Pentana audit software support Internal Audit? - Sepia Solutions
- [2] The Information Audit: Principles and Guidelines
- [3] <https://www.degruyter.com/document/doi/10.1515/LIBR.2003.23/html>
- [4] The information audit: Role and scope - ScienceDirect
- [5] <https://www.sciencedirect.com/science/article/abs/pii/S0268401207000059>
- [6] The information audit: An integrated strategic approach - ScienceDirect
- [7] <https://www.sciencedirect.com/science/article/abs/pii/S0268401297000388>
- [8] Appraisal of the Effectiveness and Efficiency of an Information Security Management System Based on ISO 27001 | IEEE Conference Publication | IEEE Xplore
- [9] <https://ieeexplore.ieee.org/abstract/document/4622587/keywords#keywords>
- [10] A structured approach to integrating audits to create organisational efficiencies: ISO 9001 and ISO 27001 audits: Total Quality Management & Business Excellence: Vol 26, No 5-6
- [11] <https://www.tandfonline.com/doi/abs/10.1080/14783363.2013.876181>
- [12] Achieving ISO 27001 certification and GDPR assessment | by Every Media blockchain Platform | Medium
- [13] https://medium.com/@emp_official/achieving-iso-27001-certification-and-gdpr-assessment-675971fbd105
- [14] Optimizing ISO 27001 compliance: integrating cybersecurity frameworks | by Trulioo | The RegTech Hub | Medium
- [15] <https://medium.com/the-regtech-hub/optimizing-iso-27001-compliance-integrating-cybersecurity-frameworks-2610661c48a7>
- [16] Benefits of ISO/IEC 27001 Information Security Management System | by CFE CERTIFICATION | Medium
- [17] <https://cfecertification.medium.com/benefits-of-iso-iec-27001-information-security-management-system-f4883edbcc23>
- [18] M. Marques da Silva, Multimedia Communications and Networking. CRC Press, 1st edition, ISBN: 9781439874844, FL,
- [19] USA, March 2012 by CRC Press. <http://www.crcpress.com/product/isbn/9781498746816>.
- [20] Fernando Boavida, Mário Bernardes, Pedro Vapi, Administração de Redes Informáticas, FCA – Editora de Informática Lda., Março 2009