www.pwc.com

Cloud Computing

O papel da auditoria interna no equilíbrio entre o risco e a oportunidade

16 novembro 2017

ipai instituto português de auditoria interna

pwc

Agenda

Cloud Computing

Tipos de *Cloud* e exemplos de utilização

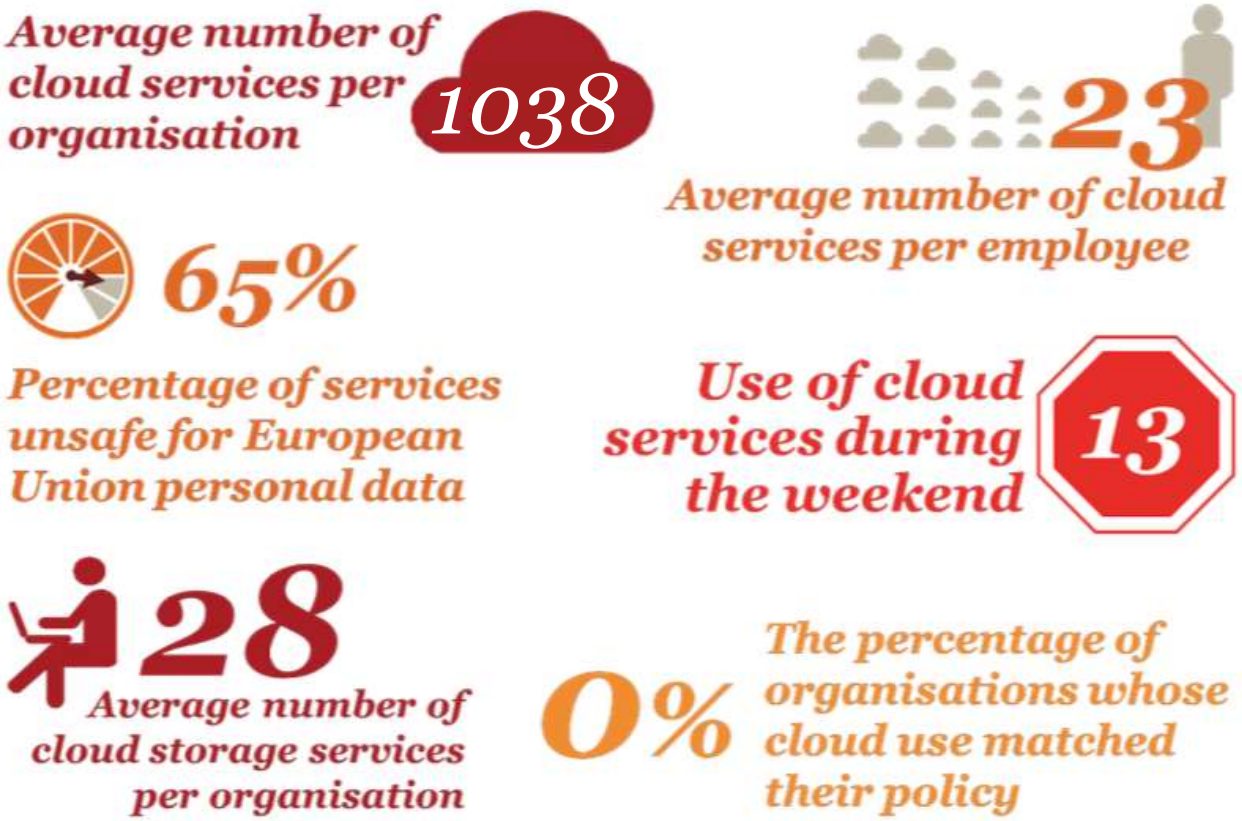
Principais benefícios e desafios

Drivers de risco

Principais Riscos

O papel do auditor interno

Números e riscos



Skyhigh Cloud Adoption & Risk Report in Europe
Q1 2016

Cloud Computing
Tema actual

Departamentos de TIs:

- Complexos
- Elevados custos
  - Capital humano
  - Operações
  - Investimento
- Resistência ao dinamismo

Cloud Computing

Tendência que visa responder a estes desafios

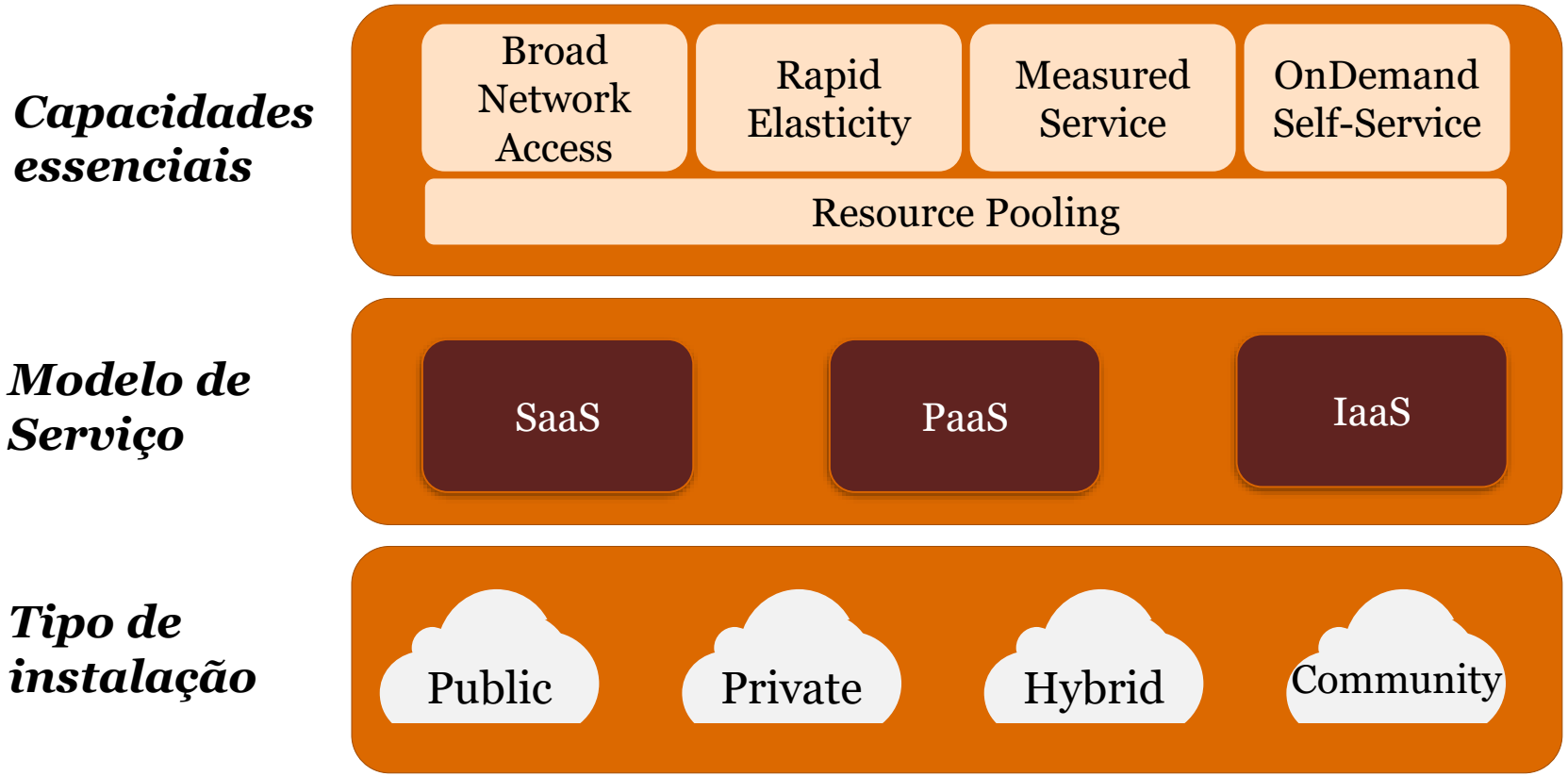
Cloud Computing
Tema actual

O próximo passo evolutivo na maturidade dos Sistemas de Informação!

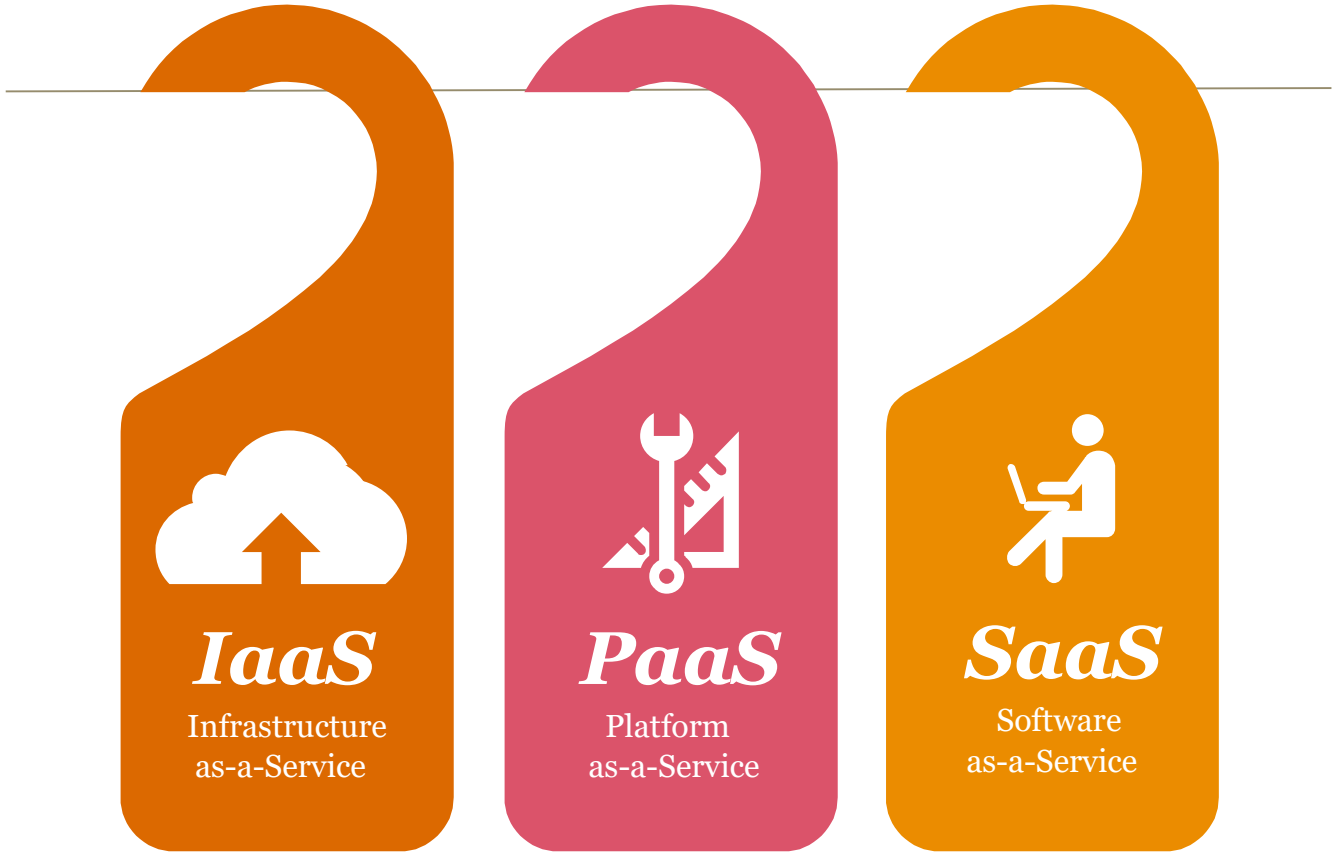
- Recursos de computação centralizados de forma a suportar processos de negócio
- Transformação dos recursos necessários em serviços escaláveis com base na necessidade
- Contraste com o modelo tradicional *on-premise* e com a aquisição de hardware e software

Cloud Computing
Modelo NIST

Modelo Visual da definição de Cloud Computing



Cloud Computing
Modelos de serviço



Cloud Computing
Modelos de serviços Cloud

	Âmbito de prestação de serviços	Tipo de utilização
 ***IaaS***	Recursos de hardware, rede e armazenamento são prestados na *cloud*, enquando o cliente mantém o controlo e a operação das suas aplicações.	Servidores / Armazenamento
 ***PaaS***	Recursos de hardware, rede e sistemas operativos são prestados na *cloud* enquanto o cliente desenvolve as aplicações para execução de forma remota.	Desenvolvimento de aplicações
 ***SaaS***	O prestador oferece as aplicações e toda a infraestrutura adjacente, acessível via web.	Aplicações

Cloud Computing
Modelos de serviços Cloud

 ***IaaS***	*Host*
 ***PaaS***	*Build*
 ***SaaS***	*Consume*

Cloud Computing
Modelos de serviços Cloud - Exemplos

	Exemplos de prestadores
IaaS	hp, IBM, altice, amazon web services, vmware
PaaS	Windows Azure, force.com cloud platform, appfog, Google Cloud Platform
SaaS	SAP, Dropbox, Office 365, Gmail, EVERNOTE

Cloud Computing
Tipos de Cloud

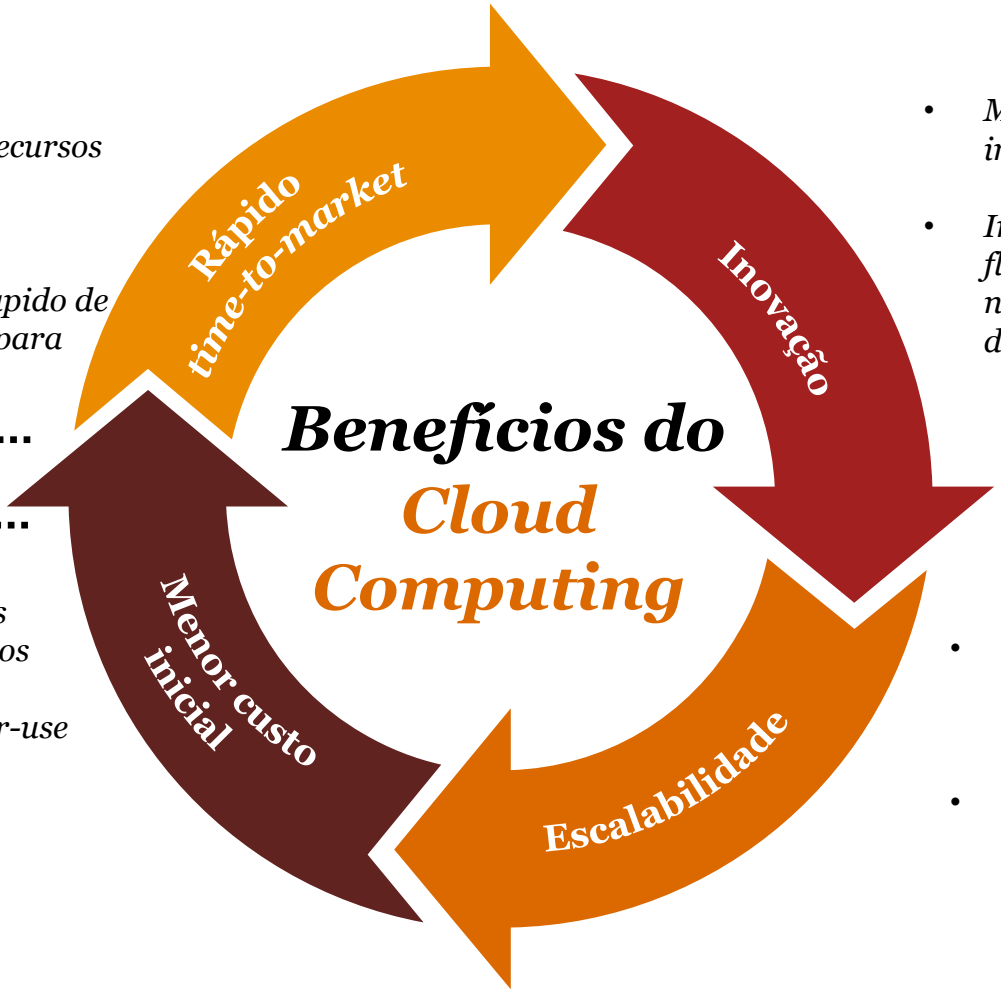
	Descrição
 ***Public***	Serviço de acesso generalizado. Existem também *Community Clouds* acessíveis por comunidades específicas.
 ***Private***	Serviço exclusivo para uma organização.
 ***Hybrid***	Combinação de duas ou mais clouds interconectadas.

Cloud Computing
Major Players

Cloud Computing
Benefícios

- *Acesso imediato a recursos de processamento e armazenamento*
- *Provisionamento rápido de servidores virtuais para cargas variáveis*

- *Recursos agrupados para optimizar custos*
- *Baseado em pay-per-use ou ciclos de carga*

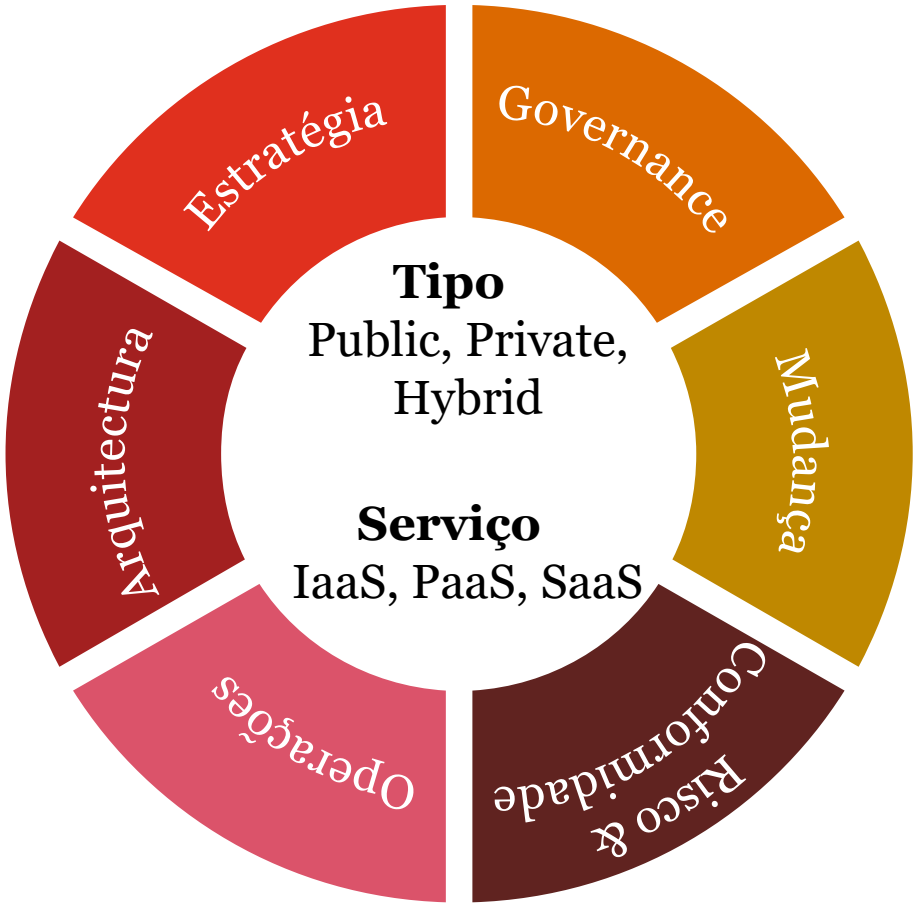


- *Menores barreiras para inovação em TI*
- *Infraestrutura de TI flexível alinhada com as necessidades variáveis do negócio*

- *Aumentar ou diminuir serviços alinhados com a carga*
- *Escalabilidade automática comandada por níveis de serviço pré-definidos*

Cloud Computing
Aspectos a ter em consideração

Conforme o modelo de serviço e tipo de cloud, devemos ter preocupações diferentes



Cloud Computing
Principais desafios

Cloud Computing
Principais desafios

Quanto custa a adopção dos serviços cloud ad-hoc?

Cloud Computing
Principais desafios

Investimento em cloud falhado por falta de adopção?

Cloud Computing
Principais desafios

Utilizadores estão a **violar políticas de TI** com utilização de **serviços não autorizados**?

Cloud Computing
Principais desafios

Os serviços utilizados ad-hoc cumprem as nossas **políticas e níveis de serviço**?

Cloud Computing
Principais desafios

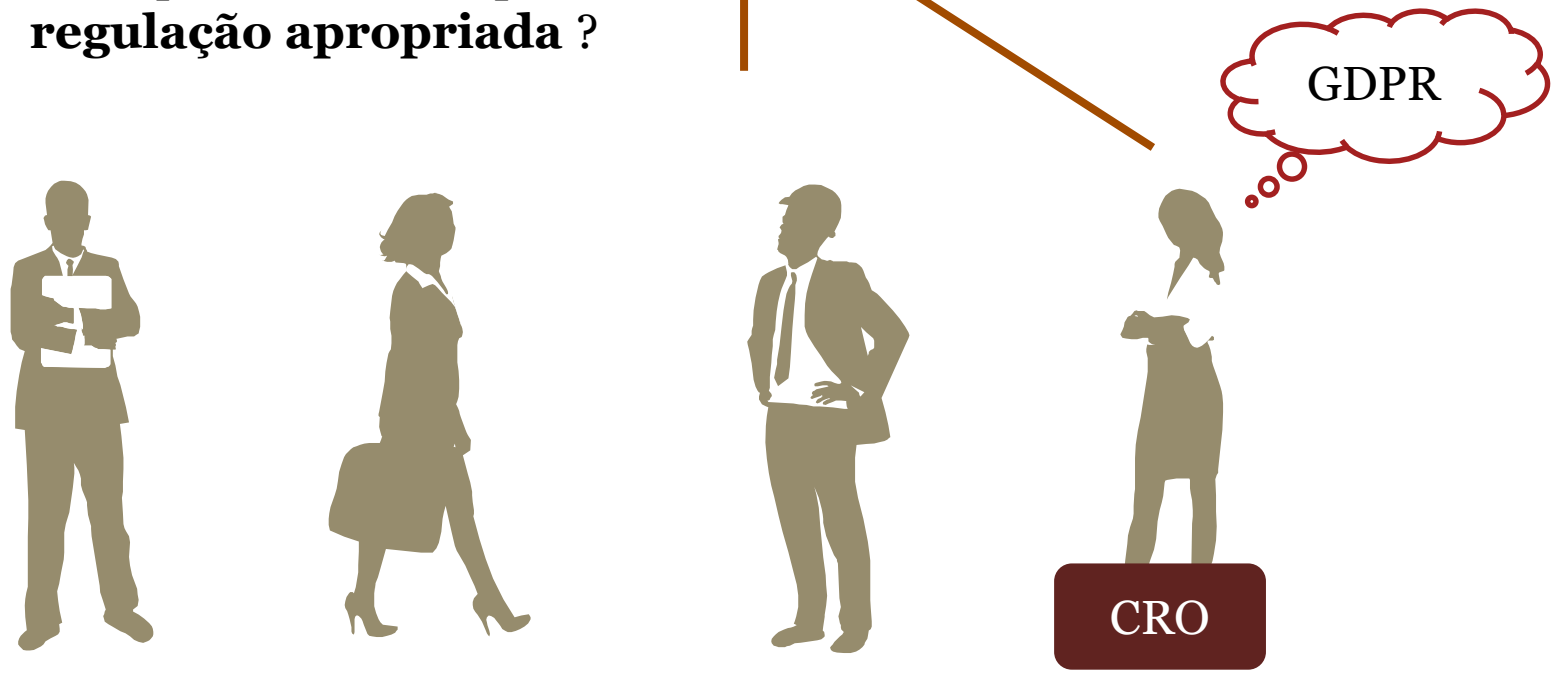
Qual a **percepção** dos nossos clientes na utilização da *cloud*?

Cloud Computing
Principais desafios

A utilização de cloud afecta a **consistência** da experiência de clientes?

Cloud Computing
Principais desafios

Onde estão fisicamente os dados e em que medida cumprimos a **regulação apropriada** ?



Cloud Computing
Principais desafios

Qual o **risco** da utilização dos serviços não autorizados?

Cloud Computing
Principais desafios

A adopção de serviços cloud torna-me **mais ágil**, mas **conseguimos gerir** o serviço prestado?

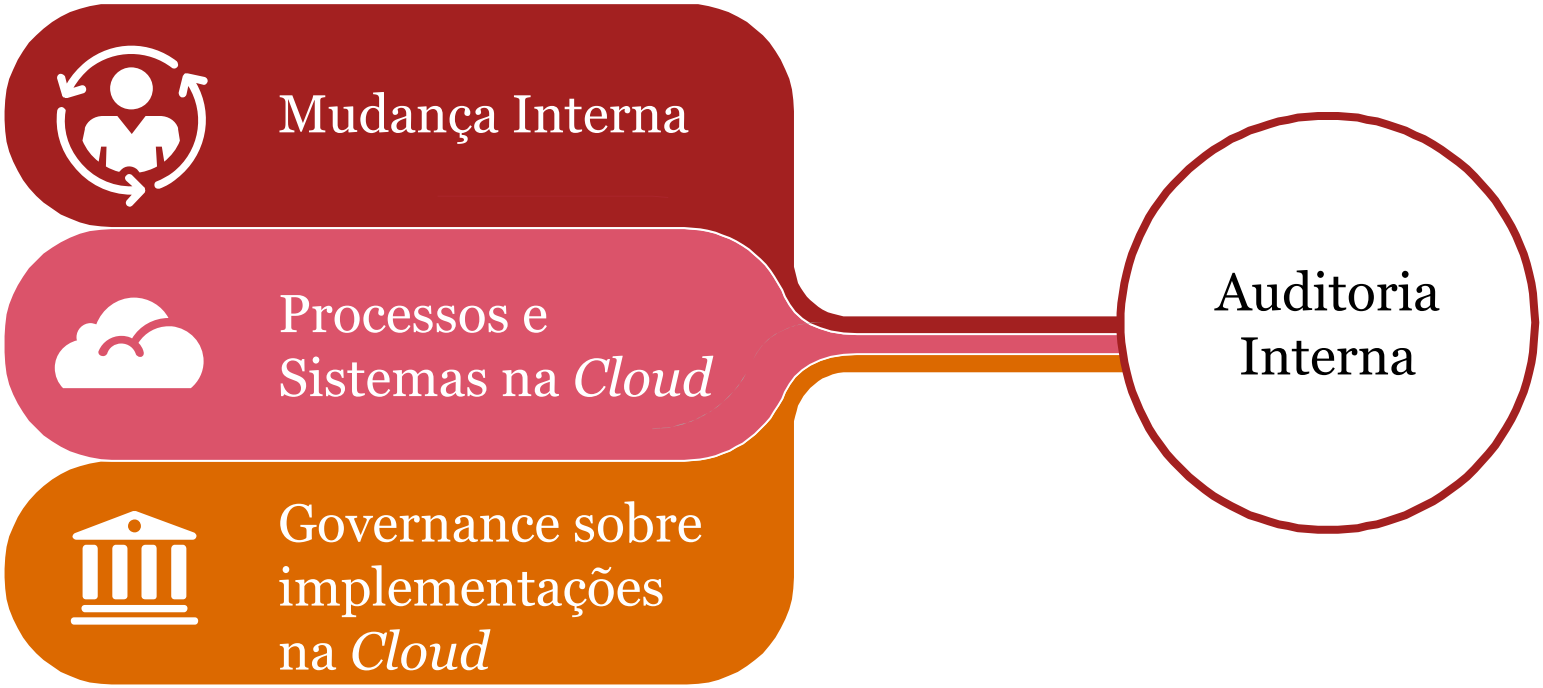
Cloud Computing
E os auditores internos?

Qual o papel do auditor interno?

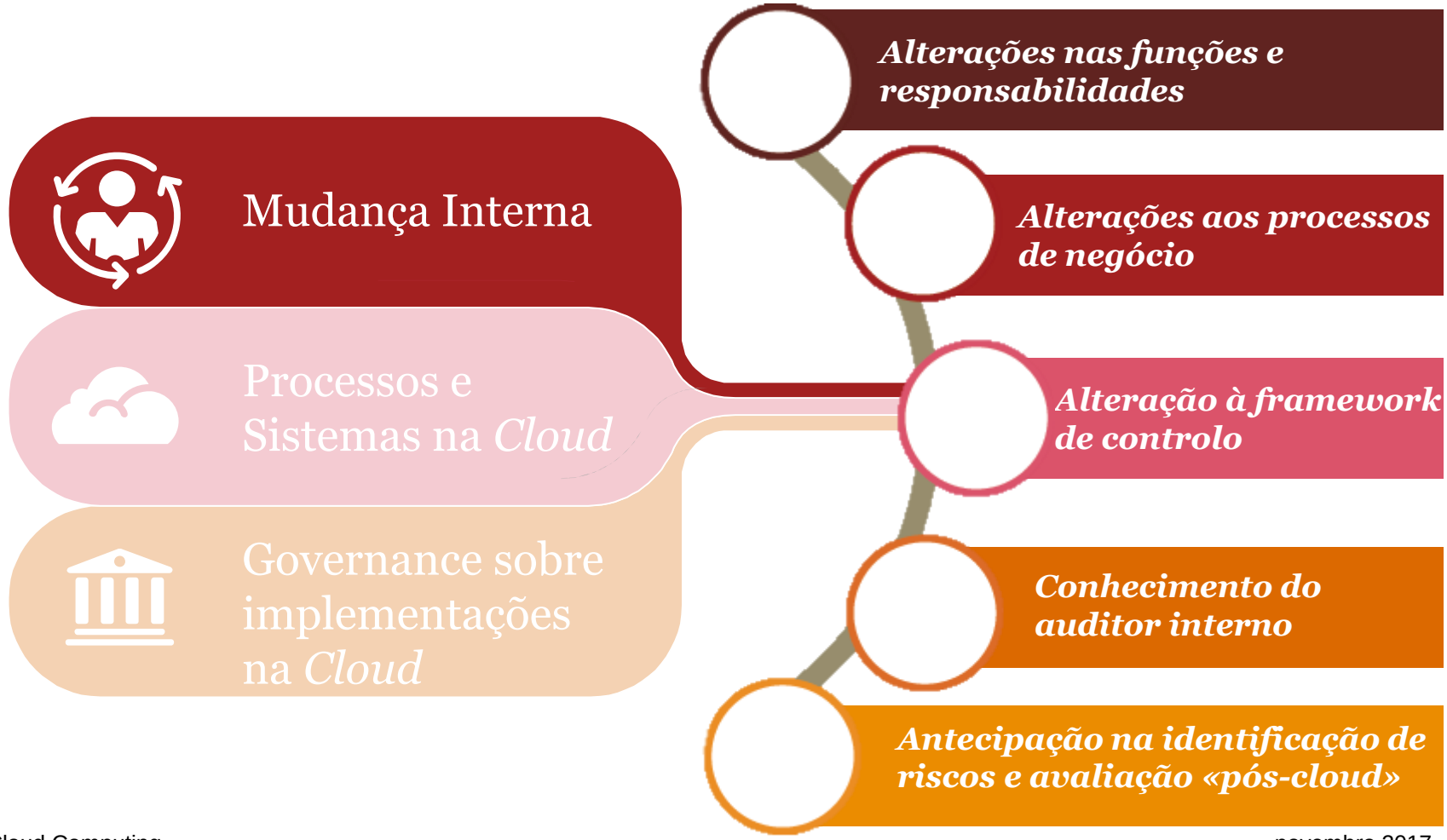
A adopção generalizada de soluções *cloud* pode alterar todas as funções de negócio e o auditor interno assume um papel fundamental através do Governance.

Governance vs. Assurance?

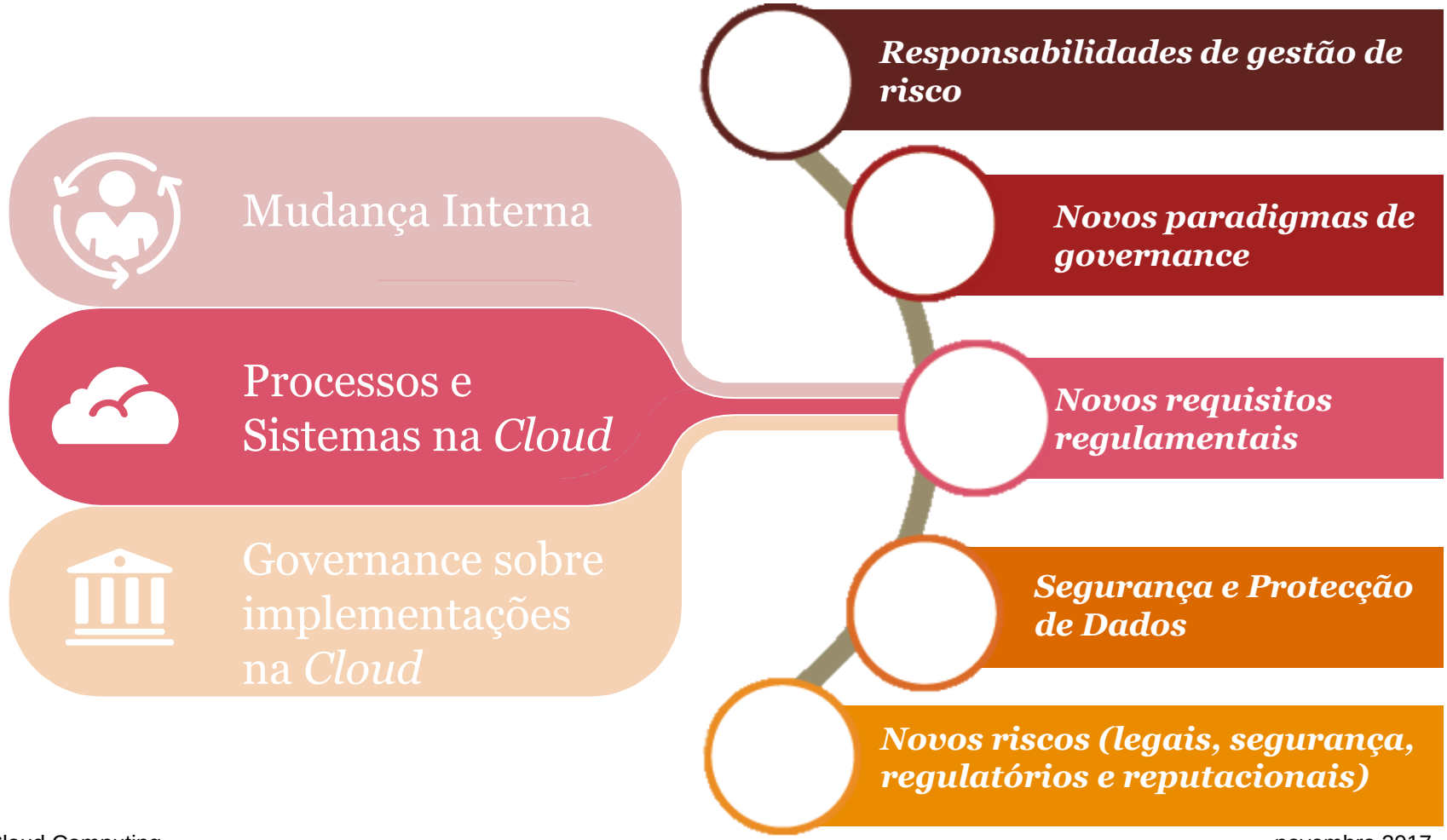
Cloud Computing
Drivers de risco para o auditor interno



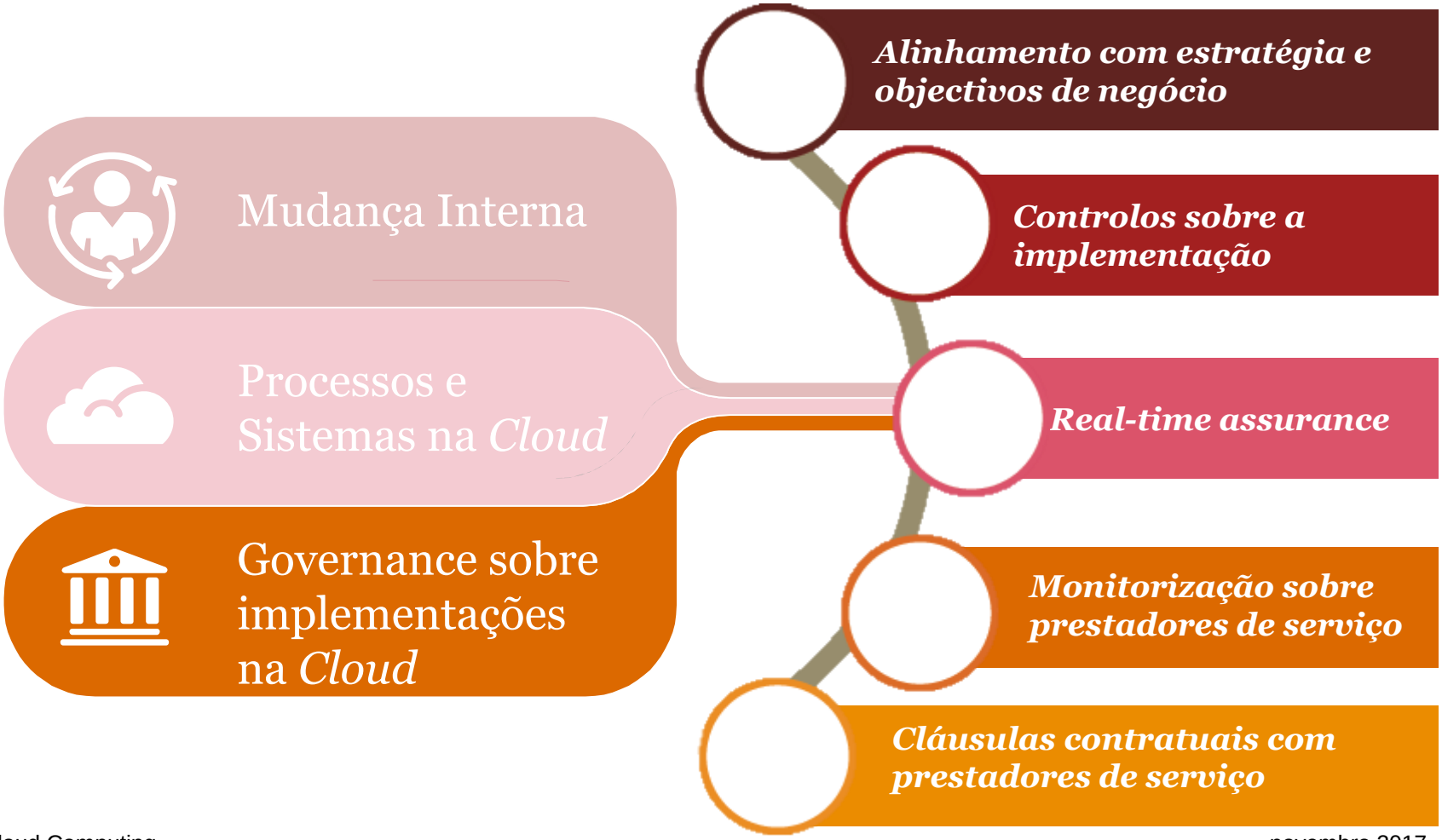
Cloud Computing
Drivers de risco para o auditor interno



Cloud Computing
Drivers de risco para o auditor interno



Cloud Computing
Drivers de risco para o auditor interno



Cloud Computing
O papel do auditor interno

A transição para a Cloud requer preparação, planeamento, gestão e supervisão.

A **nossa** responsabilidade mantém-se!

Cloud Computing
Objectivos do Auditor Interno

01 Entender, avaliar e comunicar a eficácia dos controlos e segurança do CSP

Identificar fraquezas ou deficiências de controlo de forma proactiva **02**

03 Obter um nível de conforto na capacidade de prestação de serviço

Cloud Computing
Como atingir os objectivos

Acompanhar a mudança desde o início!

- Qual é o business case?
- Em que medida está alinhado com a estratégia do negócio?
- O que vamos transferir para a *cloud*?

Cloud Computing
Como atingir os objectivos

- Como vão ser protegidos os meus dados?
- De quem é essa responsabilidade?
- Onde serão guardados os dados? Legislação aplicável?
- Como é que se alinha com os outros controlos?

Cloud Computing
Como atingir os objectivos

- Quais são os níveis de serviço?
- Como gerir a conformidade?
- Como gerir incidentes e problemas?

Cloud Computing
Como atingir os objectivos

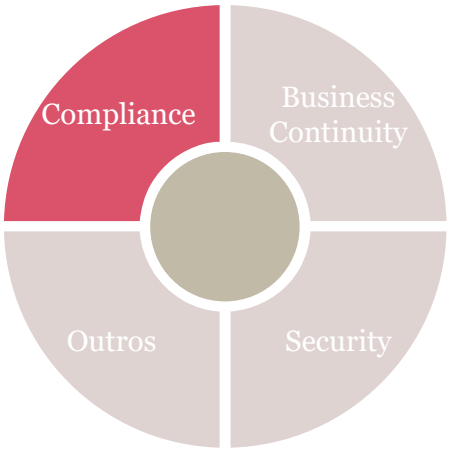
- Atingimos os benefícios esperados?
- Projecto concluído com sucesso?

Cloud Computing
Como atingir os objectivos

- Quem monitoriza o serviço prestado?
- As obrigações contratuais são monitorizadas?
- A facturação é correcta?

Cloud Computing
Principais Riscos

Cloud Computing
Principais Riscos



Compliance:

- Legislativos
- Regulatórios
- Corporativos
- Contratação (*right to audit*)

Cloud Computing
Principais Riscos

Business Continuity:

- Business Continuity
- Disaster Recovery
- Disponibilidade do serviço
- Gestão de performance

Cloud Computing
Principais Riscos

Security:

- Perda de *governance*
- Ambiguidade sobre responsabilidades / *ownership*
- *Lock-in*
- *Isolation failure*
- Localização dos dados
- Protecção dos dados
- Gestão de incidentes de segurança
- Eliminação de dados insegura ou incompleta
- Ataques internos do prestador de serviço

Cloud Computing
Principais Riscos

Security:

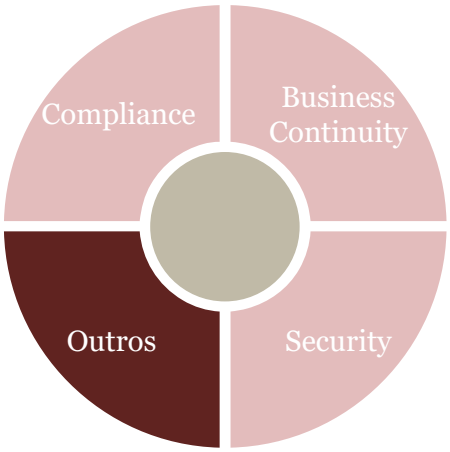
enisa
European Network and Information Security Agency

Cloud Computing

Benefits, risks and recommendations for information security

2009 (Rev. 2012)

Cloud Computing
Principais Riscos



Outros:

- Interoperabilidade com sistemas actuais
- Regressão da adopção do serviço
- Capacidades de customização
- Conformidade e direitos de auditabilidade
- Soberania sobre dados – jurisdição legal sobre dados
- Direitos sobre propriedade intelectual
- Obrigações contratuais

Cloud Computing
Principais Riscos

Exemplos de riscos específicos:

- **Business case** – Os benefícios e redução de custos podem estar sobre-estimados e não consideram riscos e custos de operação.
- **Data ownership** – Ambiguidade em relação à propriedade dos dados na *cloud* (e.g. informação confidencial, propriedade intelectual, informação de clientes).
- **Data security** – Impossibilidade de aplicar políticas de segurança corporativas no ambiente cloud e confiar apenas nos mecanismos de segurança implementados pelo CSP.
- **Sovereignty** – Falta de clareza sobre localização dos dados e respective legislação aplicável.
- **Assurance** – Impossibilidade de obter conforto suficiente sobre os controlos implementados pelo CSP.

Cloud Computing
Factores de sucesso (1/2)

Capacidades técnicas:

- Conhecimento sobre serviços cloud transversal aos responsáveis pela gestão de risco, legal, compras, TI e auditoria interna.

Framework de avaliação robusta:

- Critérios robustos e transversais de avaliação.
- Inclusão de principais áreas (propriedade de dados, encriptação, acessos e transparência da tecnologia utilizada).

Governance:

- Responsáveis legais, de risco, de compras e TI estão alinhados no processo de *governance*. Quem é responsável pelo quê?

Cloud Computing
Factores de sucesso (2/2)

Portabilidade:

- Facilidade de migração para/da *cloud*

Relações com CSP's:

- Limitar a relação com alguns CSP's e evitar a contratação de serviços a vários prestadores (fragmentação do mercado).
- Inclusão de principais áreas (propriedade de dados, encriptação, acessos e transparência da tecnologia utilizada).

Pontos de vista TI vs Negócio:

- Garantir que a adopção de soluções cloud é vantajosa para a organização como um todo

Cloud Computing
Mitos

Ouvi dizer que…

- A *Cloud* é menos segura que a alternativa de ter todos os dados dentro da organização.
- O *Cloud Computing* só é aplicável para consumidores finais e pequenas organizações.
- Cloud Computing não é uma opção para actividades críticas da organização.
- As *clouds* privadas oferecem todos os benefícios do Cloud Computing sem os riscos associados.

Cloud Computing
Saber mais

pwc.com/cloud

pwc.pt/ras

Outros:

Cloud Security Alliance (CSA)

- Cloud Controls Matrix (CCM)
- Common Assessment Initiative Questionnaire (CAIQ)
- ENISA – Cloud Computing: Benefits, risks and recommendations for information security

- **National Institute of Standards and Technology's (NIST)**
  - The NIST Definition of Cloud Computing
  - NIST SP 500-322 “Evaluation of Cloud Computing Services Based on NIST 800-145”

Questões?

… que podem fazer aos vossos CEO / CIO:

- Como é que a estratégia de adopção de soluções cloud vai reduzir os custos das TI e como vai ajudar a explorer novas oportunidades de negócio?
- Como é comparável a estrutura de TI da nossa organização com a utilização de uma *cloud* pública? Comparámos as duas abordagens?
- Como é que a nossa política de segurança aborda a actual utilização de serviços *cloud*?
- Se já estão a implementar…
  - Quais são os planos de implementação e migração?
  - **Contam com o envolvimento dos Auditores Internos?**

Outras questões?

Pedro Santinhos
Manager
pedro.miguel.santinhos@pt.pwc.com