ISACA®
Trust in, and value from, information systems

CLOUD COMPUTING LESSONS LEARNED

Marc Vael, Chief Audit Executive Smals / President ISACA Belgium, November 2015

Information is emerging as the
most important business asset
of the 21st century.

What Happens in an Internet Minute?

1,572,877 GB of global IP data transferred[1]

10 Million ads displayed[2]

347,222 Tweets[3]

3.3 Million pieces of content shared[4]

6.9 Million messages sent[4]

Netflix + Youtube = **more than ½ of all traffic**[5]

$400 Million during Alibaba peak day sales[6]

438,801 Wiki page views[7]

10 Million WeChat messages at its peak[9]

34.7 Million instant messages (MIM) sent[8]

194,064 app downloads[10]

$133,436 in sales[11]

31,773 hours of music played[12]

38,194 photos uploaded[13]

57,870 page views[14]

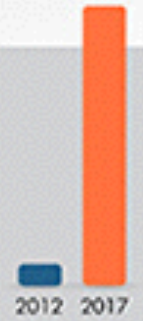
4.1 Million searches[15]

100 hours of video uploaded[16]

138,889 hours of video watched[16]

23,148 hours of video watched[17]

And Future Growth is Staggering



By 2017, mobile traffic will have grown **13X** in just 5 years[1]

In 2017, there will be **3X** more connected devices than people on Earth[1]

All digital data created reached **4 zettabytes** in 2013[18]

WHEN WAS THE TERM USED FOR THE FIRST TIME?

Intermediaries in Electronic Markets

Session: MD19
Date/Time: Monday 14:45-16:15
Type: Invited
Sponsor:
Track:
Cluster: Electronic Commerce
Room: Duncan A
Chair: Sulin Ba
Chair Address: Univ. of Southern CA, Marshall Sch. of Bus. Admin., Dept. of IOM, Los Angeles, CA 90089-1421,
Chair E-mail:

MD19.1 The Importance of Intermediation in Electronic Markets *Charles Steinfield --- MI State Univ., Dept. of Telecomm., E Lansing, MI 48824-1212,*
Contrary to expectations of electronic commerce enthusiasts, electronic markets will generally require as much intermediation than traditional markets. Anecdotal evidence for this abounds in the form of the emergence of a range of new intermediaries. A theoretical framework and propositions regarding the role of intermediaries in electronic markets are discussed.

MD19.2 Intermediaries in Cloud-Computing: A New Computing Paradigm *Ramnath Chellappa --- Univ. of TX, Ctr. for Res. on Elect. Comm., MSIS Dept., Grad. Sch. of Bus., Austin, TX 78712 , (ram@cism.bus.utexas.edu)*
Computing has evolved from a main-frame-based structure to a network-based architecture. While many terms have appeared to describe these new forms, the advent of electronic commerce has led to the emergence of 'cloud computing.' This work aims at analyzing the role of agents and intermediaries enabling this framework.

MD19.3 Comparison Agents on the Web *Dave King --- Comshare, Inc., , , (dave@comshare.com)*
Business-to-consumer commerce on the WWW offers buyers an unprecedented opportunity to 'comparison' shop. To save buyers the pain of searching across the Web, software agents provide the means to automate the process. We review the technology's underlying 'comparison' agents and examine commercial and research products that provide this functionality.

MD19.4 Profit-Oriented Knowledge Brokering *Sulin Ba --- Univ. of Southern CA, Marshall Sch. of Bus. Admin., Dept. of IOM, Los Angeles, CA 90089-1421, (sulin@rcf.usc.edu)*
A new organizational construct, the knowledge broker, motivated by organizational goals of profit maximization and enabled by the technological development in electronic commerce, is introduced as a profit-oriented intermediary to manage organizations' knowledge resources. It will enable organizations to carry out value-added 'knowledge-rich' transactions in the electronic marketplace.

Return to INFORMS home page
Return to Conference home page

26th of October 1997

ISACA
Trust in, and value from, information systems

WHO HYPED ALL THIS?

"What's interesting [now] is that there is an emergent new model, and you all are here because you are part of that new model. I don't think people have really understood how big this opportunity really is. It starts with the premise that the data services and architecture should be on servers. **We call it cloud computing – they should be in a "cloud" somewhere**. And that if you have the right kind of browser or the right kind of access, it doesn't matter whether you have a PC or a Mac or a mobile phone or a BlackBerry or what have you – or new devices still to be developed – you can get access to the cloud."

Mr. Eric Schmidt, Chairman & CEO Google
Search Engine Strategies Conference, 9th of August 2006
http://www.google.com/press/podium/ses2006.html

ISACA
Trust in, and value from, information systems

DEFINITION OF CLOUD COMPUTING

A model for enabling convenient, on-demand broad network access to a shared pool of configurable computing resources that can be rapidly provisioned & released with minimal management effort or service provider interaction and with automatic measuring, controlling & optimization.

5 characteristics

3 service models

4 deployment models

NIST, Definition of Cloud Computing, October 2009

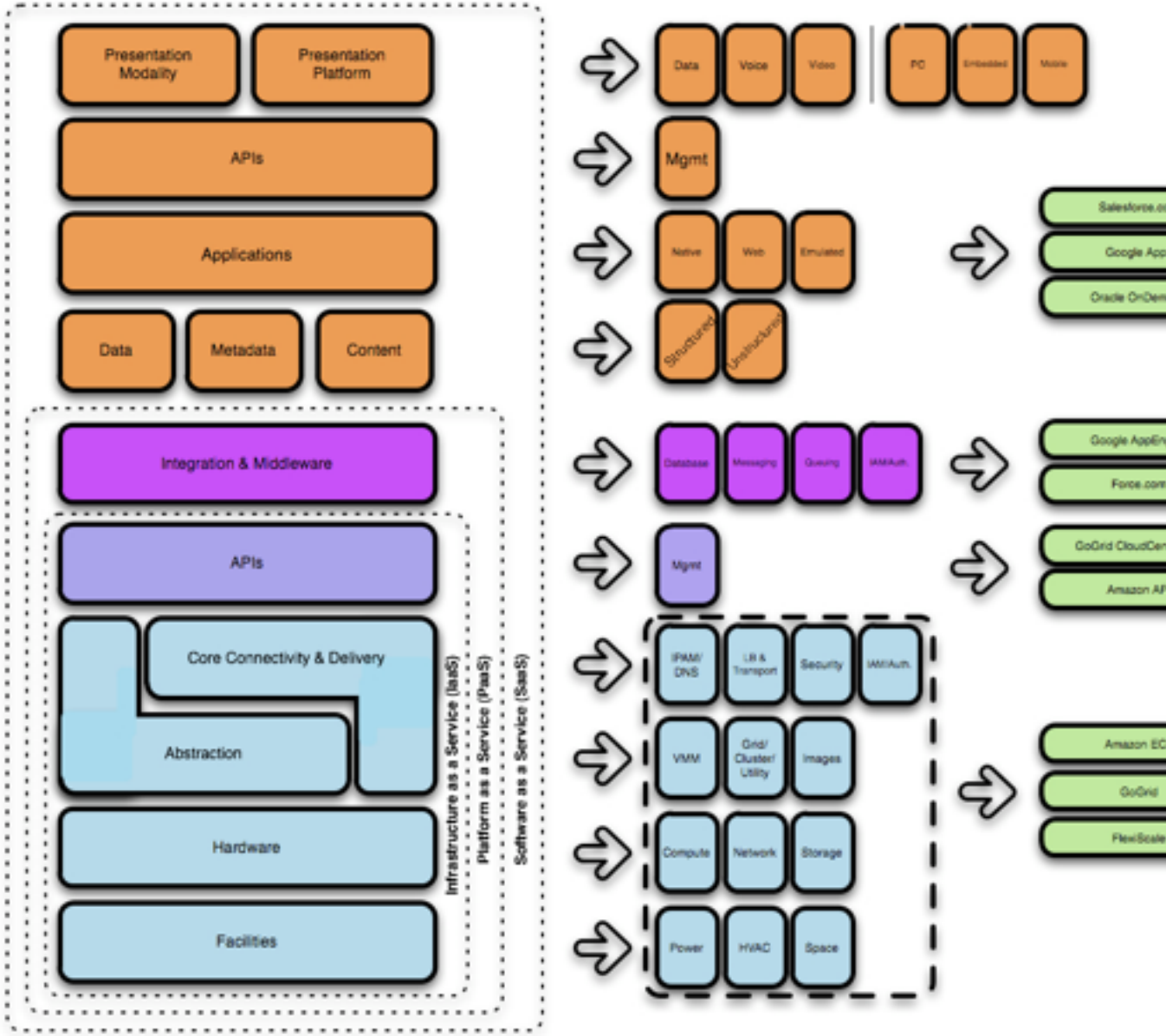
DEFINITION

1. *On-demand self-service.*
2. *Broad network access.*
3. *Resource pooling.*
4. *Rapid & elastic provisioning (add & withdraw).*
5. *Automatically measured, controlled, optimized service.*

NIST, Definition of Cloud Computing, October 2009
ISACA, Cloud Computing: Business Benefits With Security, Governance and Assurance Perspectives, 2010

ISACA
Trust in, and value from, information systems

Cloud Model



Security Control Model

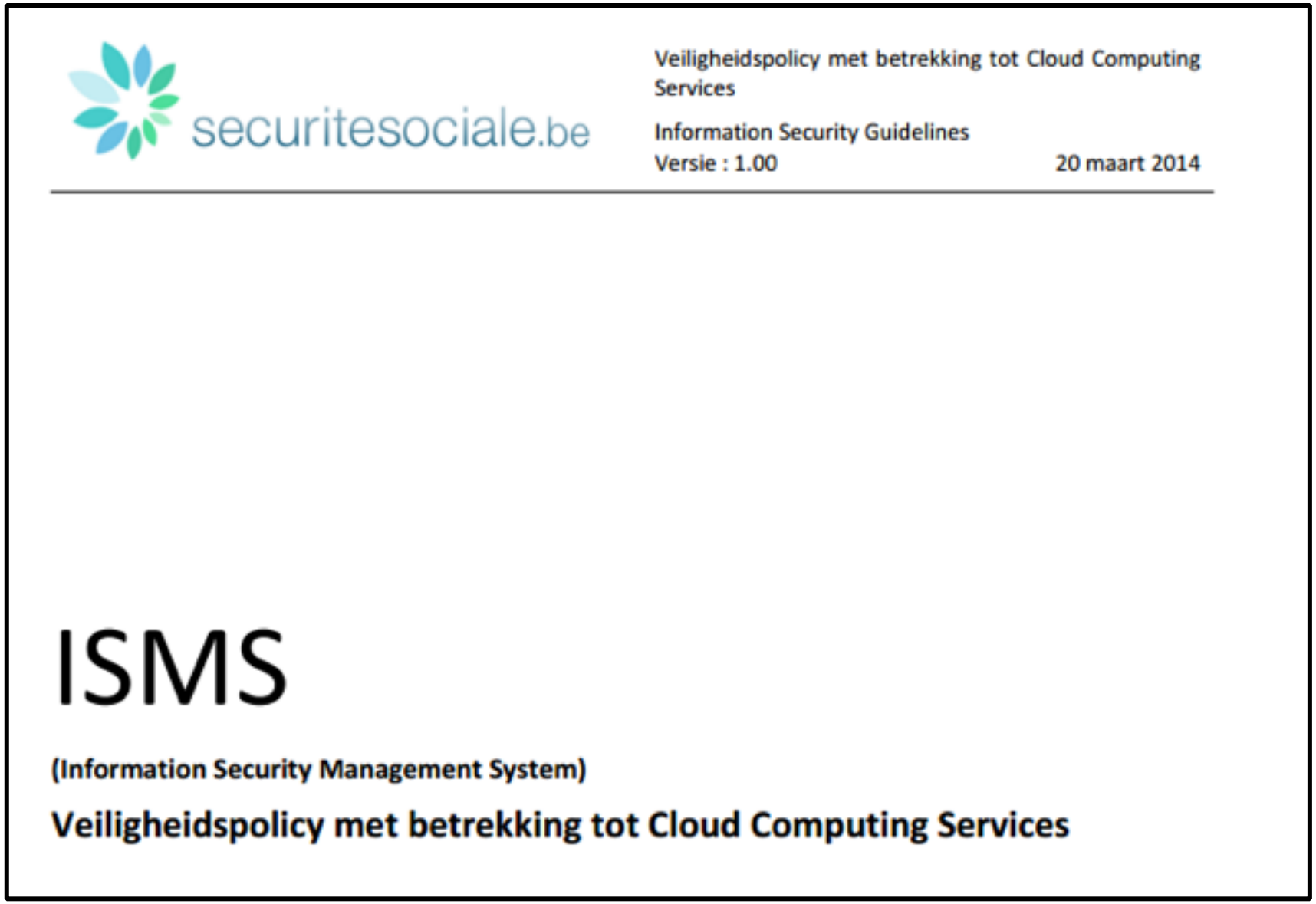
Applications	SDLC, Binary Analysis, Scanners, WebApp Firewalls, Transactional Sec.
Information	DLP, CMF, Database Activity Monitoring, Encryption
Management	GRC, IAM, VA/VM, Patch Management, Configuration Management, Monitoring
Network	NIDS/NIPS, Firewalls, DPI, Anti-DDoS, QoS, DNSSEC, OAuth
Trusted Computing	Hardware & Software RoT & API's
Compute & Storage	Host-based Firewalls, HIDS/HIPS, Integrity & File/log Management, Encryption, Masking
Physical	Physical Plant Security, CCTV, Guards

Cloud Computing Taxonomy & Ontology v1.5 Chris Hoff +

ISACA
Trust in, and value from, information systems

MAIN CLOUD DRIVERS

1. Optimized resource utilization (pay-as-you-go = near to perfect alignment with actual demand).
2. Cost savings (from capital expenditure (CAPEX) to operational expenditure (OPEX) significant up-front & total cost savings + transparency of usage charges driving behavioral change in organization).
3. Better responsiveness (on-demand, agile, scalable, flexible services to respond to changing requirements & peak periods).
4. Faster cycle of innovation (flexible patching & upgrading).
5. Reduced time for implementation (processing power & data storage as needed + at capacity needed in near-real time).
6. Resilience (reduced potential for system failure & risk of downtime).



https://www.ksz-bcss.fgov.be/binaries/documentation/nl/securite/policies/isms_050_cloud_computing_policy_nl.pdf

ISACA
Trust in, and value from, information systems

4. Risico's verbonden aan de "Cloud"

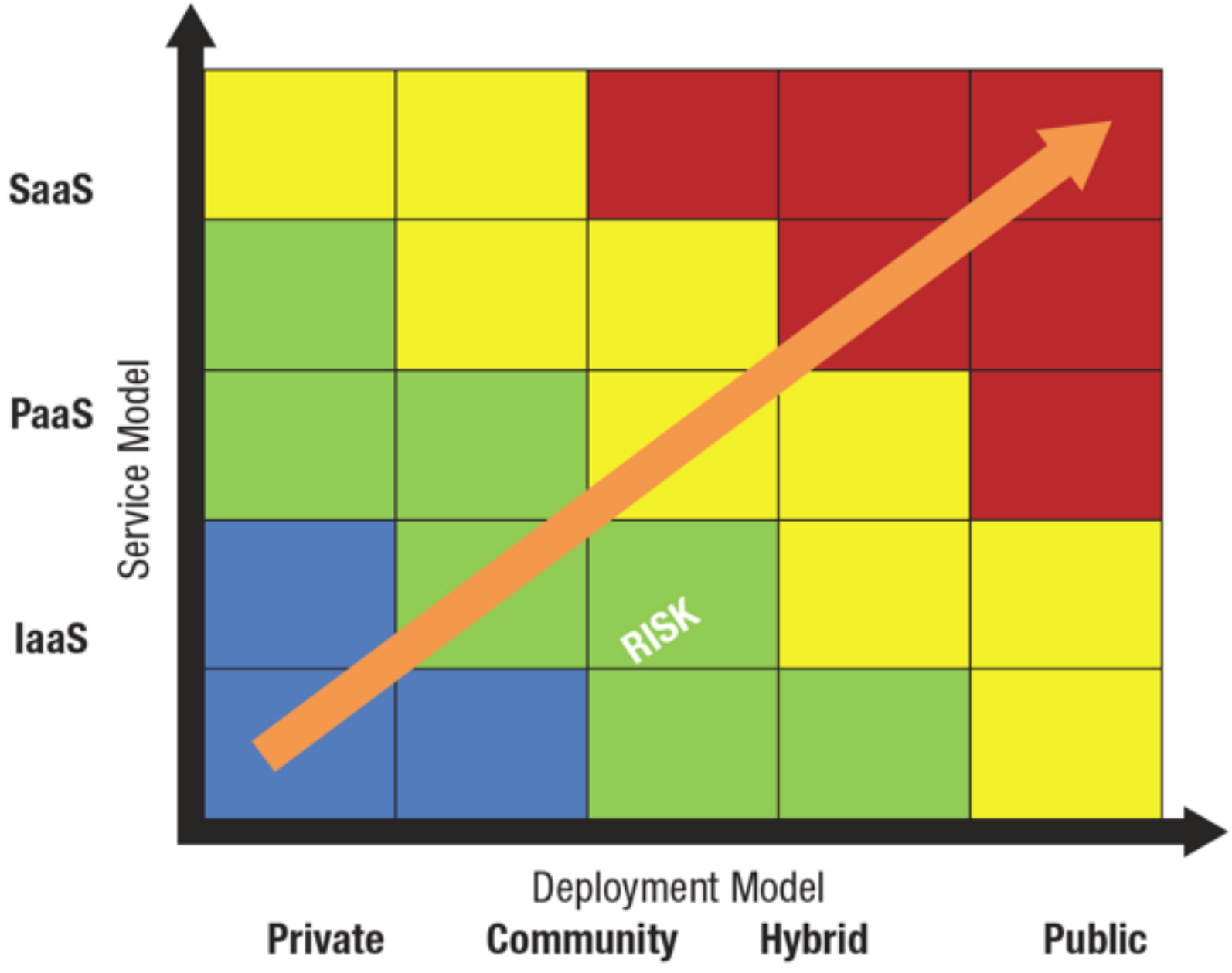
De overgang naar Cloud Computing vereist een strenge aanpak op het vlak van het beheer van de veiligheidstechnische, contractuele en juridische risico's. De instelling die een beroep wenst te doen op een "Cloud"-provider moet zich ervan vergewissen dat die provider de geschikte veiligheidsmaatregelen kan toepassen, om zich te beschermen tegen de risico's van de Cloud en in verband met de traditionele informaticaverwerkingen en in het bijzonder tegen de risico's die relevant zijn voor de bescherming van de persoonsgegevens. De belangrijkste risico's die op dat vlak werden geïdentificeerd, zijn de volgende:

- een verminderde governance met betrekking tot de verwerking;
- de risico's verbonden aan de onderaannemers van de leverancier, bijvoorbeeld een fout in de onderaannemingsketen wanneer de leverancier zelf een beroep doet op derden om een dienst te leveren;
- de technische afhankelijkheid ten opzichte van de provider van de Cloud Computing-oplossing, bijvoorbeeld het risico dat er gegevens verloren gaan bij migratie naar een andere provider of een interne oplossing;
- een gegevenslek, met andere woorden het risico dat gegevens die op een (virtueel) systeem zijn gehost, gewijzigd kunnen worden of toegankelijk zijn voor niet-gemachtigde derden naar aanleiding van een tekortkoming of een slecht beheer van de provider;
- de uitvoering van juridische vorderingen op basis van een buitenlands recht zonder overleg met de nationale instanties;
- het niet-naleven van de regels die door de instelling werden uitgevaardigd met betrekking tot de bewaring en de vernietiging van gegevens, o.a. bij een ondoeltreffende of onbeveiligde vernietiging van de gegevens of een te lange bewaarduur;
- problemen bij het beheren van de toegangsrechten;
- de onbeschikbaarheid van de dienst geleverd door de provider;
- de stopzetting van de dienst door de provider (bv. als gevolg van een gerechtelijke beslissing of de overname van de provider door een derde of bij een faillissement);
- de niet-overeenstemming met de regelgeving, in het bijzonder met betrekking tot internationale transfers.

Een uitgebreide, niet-exhaustieve lijst van 35 risico's die door het ENISA[3] werd meegedeeld, kan in overweging worden genomen bij de risicoanalyse zodra het kader van het project is vastgelegd.

www.ksz-bcss.fgov.be/binaries/documentation/nl/securite/policies/isms_050_cloud_computing_policy_nl.pdf

Cloud Computing Risk Map



ISACA
Trust in, and value from, information systems

3. Risks

Policy and organizational risks

- R.1 Lock-in
- R.2 Loss of governance
- R.3 Compliance challenges
- R.4 Loss of business reputation due to co-tenant activities
- R.5 Cloud service termination or failure
- R.6 Cloud provider acquisition
- R.7 Supply chain failure

Technical risks

- R.8 Resource exhaustion (under or over provisioning)
- R.9 Isolation failure
- R.10 Cloud provider malicious insider - abuse of high privilege roles
- R.11 Management interface compromise (manipulation, availability of infrastructure)
- R.12 Intercepting data in transit
- R.13 Data leakage on up/download, intra-cloud
- R.14 Insecure or ineffective deletion of data
- R.15 Distributed denial of service (DDoS)
- R.16 Economic denial of service (EDOS)
- R.17 Loss of encryption keys
- R.18 Undertaking malicious probes or scans
- R.19 Compromise service engine
- R.20 Conflicts between customer hardening procedures and cloud environment

Legal risks

- R.21 Subpoena and e-discovery
- R.22 Risk from changes of jurisdiction
- R.23 Data protection risks
- R.24 Licensing risks

Risks not specific to the cloud

- R.25 Network breaks
- R.26 Network management (ie, network congestion / mis-connection / non-optimal use)
- R.27 Modifying network traffic
- R.28 Privilege escalation
- R.29 Social engineering attacks (ie, impersonation)
- R.30 Loss or compromise of operational logs
- R.31 Loss or compromise of security logs (manipulation of forensic investigation)
- R.32 Backups lost, stolen
- R.33 Unauthorized access to premises (including physical access to machines and other facilities)
- R.34 Theft of computer equipment
- R.35 Natural disasters

ISACA
Trust in, and value from, information systems

http://www.enisa.europa.eu/activities/risk-management/files/deliverables/cloud-computing-risk-assessment

R.10 Cloud provider malicious insider - abuse of high privilege roles

Probability	MEDIUM (Lower than traditional)	Comparative: Lower
Impact	VERY HIGH (Higher than traditional)	Comparative: Higher (aggregate) Comparative: Same (for a single customer)
Vulnerabilities	V34. Unclear roles and responsibilities V35. Poor enforcement of role definitions V36. Need-to-know principle not applied V1. AAA vulnerabilities V39. System or OS vulnerabilities V37. Inadequate physical security procedures V10. Impossibility of processing data in encrypted form V48. Application vulnerabilities or poor patch management	
Affected assets	A1. Company reputation A2. Customer trust A3. Employee loyalty and experience A4. Intellectual property A5. Personal sensitive data A6. Personal data A7. Personal data - critical A8. HR data A9. Service delivery – real time services A10. Service delivery	
Risk	**HIGH**	

http://www.enisa.europa.eu/activities/risk-management/files/deliverables/cloud-computing-risk-assessment

5.2. Uitvoeringswaarborg door de provider

1. Clausule met betrekking tot de mogelijkheid voor een "cloud"-provider om een deel van zijn activiteiten uit te besteden.
2. Clausule met betrekking tot de integriteit, continuïteit en kwaliteit van de dienstverlening
3. Clausule met betrekking tot de teruggave van de gegevens
4. Clausule met betrekking tot de overdraagbaarheid van de gegevens en de interoperabiliteit van de systemen
5. Clausule met betrekking tot de auditregeling
6. Clausule met betrekking tot de verplichtingen van de provider inzake vertrouwelijkheid van de gegevens
7. Clausule met betrekking tot de soevereiniteit
8. Clausule met betrekking tot de verplichtingen van de provider inzake gegevensbeveiliging

5.3. Naleving van de goede praktijken door de provider

1. Gegevensbescherming
2. Beveiliging van de rekencentra
3. Logische toegangsbeveiliging
4. Beveiliging van de systemen
5. Beveiliging van de netwerktoegangen

www.ksz-bcss.fgov.be/binaries/documentation/nl/securite/policies/isms_050_cloud_computing_policy_nl.pdf

5.4. Naleving van de wettelijke en technische verplichtingen bij de verwerking van persoonsgegevens[6]

Alvorens "Cloud computing" in te voeren, moet elke instelling de impact hiervan evalueren op de veiligheid en de vertrouwelijkheid van de verwerking en de opslag van persoonsgegevens in de Cloud. In functie van de gevoeligheid van de gegevens zoals vastgelegd door de instelling en de impactanalyse zal de instelling al dan niet een beroep kunnen doen op de diensten van een "Cloud computing"-provider.

De volgende regels zijn van toepassing bij gebruik van deze Cloud-diensten:

- In functie van haar activiteiten moet elke instelling niet alleen de Belgische en Europese wetgeving naleven maar ook de specifieke wetgeving eigen aan een sector;
- de instelling moet steeds waken over de naleving van de reglementering met betrekking tot de bescherming van de persoonsgegevens (privacywet[7]) bij de verwerking van dergelijke gegevens in een Cloud. In dat geval is de instelling die de gegevens bezit steeds verantwoordelijk voor de correcte naleving van de reglementering met betrekking tot de bescherming van de persoonsgegevens;
- in geval van outsourcing van persoonsgegevens moet de instelling zich bij de keuze van de "Cloud computing"-provider steeds beperken tot providers die enkel cloud-diensten van het type "gemeenschappelijke Cloud (of private)" aanbieden;
- Behoudens een toegelaten afwijking, is voor elke outsourcing van persoonsgegevens een vercijfering van de gegevens noodzakelijk tijdens het transport en voor de bewaring ervan. De vercijferingsmiddelen moeten bovendien steeds onder controle van de instelling worden beheerd en mogen niet worden uitbesteed.

---

[6] Persoonsgegevens omvatten tevens medische, sociale of privé-gegevens volgens de classificatie van gegevens die binnen de sociale zekerheid geldt

[7] http://www.privacycommission.be/nl/privacywet-en-uitvoeringsbesluiten

Never outsource what you do not manage properly today!

You always remain accountable!

ISACA
Trust in, and value from, information systems

CLOUD CHALLENGES

1. Principles, Policies and Frameworks:
- *Cloud security policy/procedure transparency*
- *Compliance requirements*

2. Processes:
- *Adequate security controls*

3. Organisational Structures:
- *Public cloud server owners' due diligence*

4. Culture, Ethics and Behaviour:
- *CSP business viability*
- *Screening of other cloud computing clients*

5. Information:
- *Cloud data ownership*
- *Record protection for forensic audits*
- *Data disposal for current SaaS or PaaS applications*

6. Services, Infrastructure and Applications:
- *Data location*
- *Commingled data*
- *Identity and access management*
- *Disaster recovery*

7. People, Skills and Competencies:
- *Lock in with CSP proprietary application program interfaces*

ISACA

ISACA
Trust in, and value from, information systems

Cloud Computing Management Audit/Assurance Program

Download (Member Only, 1.5M)

Purchase the Book

The audit/assurance program is a tool and template to be used as a road map for the completion of a specific assurance process. ISACA has commissioned audit/assurance programs to be developed for use by IT audit and assurance professionals with the requisite knowledge of the subject matter under review, as described in ITAF section 2200—General Standards. The audit/assurance programs are part of ITAF section 4000—IT Assurance Tools and Techniques.

Objective—The cloud computing audit/assurance review will:

- Provide stakeholders with an assessment of the effectiveness of the cloud computing service provider's internal controls and security
- Identify internal control deficiencies within the customer organization and its interface with the service provider
- Provide audit stakeholders with an assessment of the quality of and their ability to rely upon the service provider's attestations regarding internal controls.

It is not designed to replace or focus upon audits that provide assurance of specific application processes and excludes assurance of an application's functionality and suitability.

Scope—The review will focus on:

- The governance affecting cloud computing
- The contractual compliance between the service provider and customer
- Control issues specific to cloud computing

IT audit and assurance professionals are expected to customize this document to the environment in which they are performing an assurance process. This document is to be used as a review tool and starting point. It may be modified by the IT audit and assurance professional; it is *not* intended to be a checklist or questionnaire. It is assumed that the IT audit and assurance professional holds the Certified Information Systems Auditor (CISA) designation, or has the necessary subject matter expertise required to conduct the work and is supervised by a professional with the CISA designation and/or necessary subject matter expertise to adequately review the work performed.

Quick Links

I want to... | My Bookmarks | Saved Searches

- COBIT - use it effectively
- Explore certification opportunities
- Explore licensing and promotion opportunities
- Go to COBIT online
- View COBIT training opportunities

CLOUD COMPUTING AUDIT PROGRAM

- **Planning & Scoping the Audit**
  - Define audit/assurance objectives.
  - Define boundaries of review
  - Identify & document risks
  - Define change process
  - Define assignment success
  - Define audit/assurance resources required
  - Define deliverables
  - Communications
- **Governing the Cloud**
  - Governance & Enterprise Risk Management
  - Legal & Electronic Discovery
  - Compliance & Audit
  - Portability & Interoperability
- **Operating in the Cloud**
  - Incident Response, Notification & Remediation
  - Application Security
  - Data Security & Integrity
  - Identity & Access Management
  - Virtualization

ISACA®
Trust in, and value from, information systems

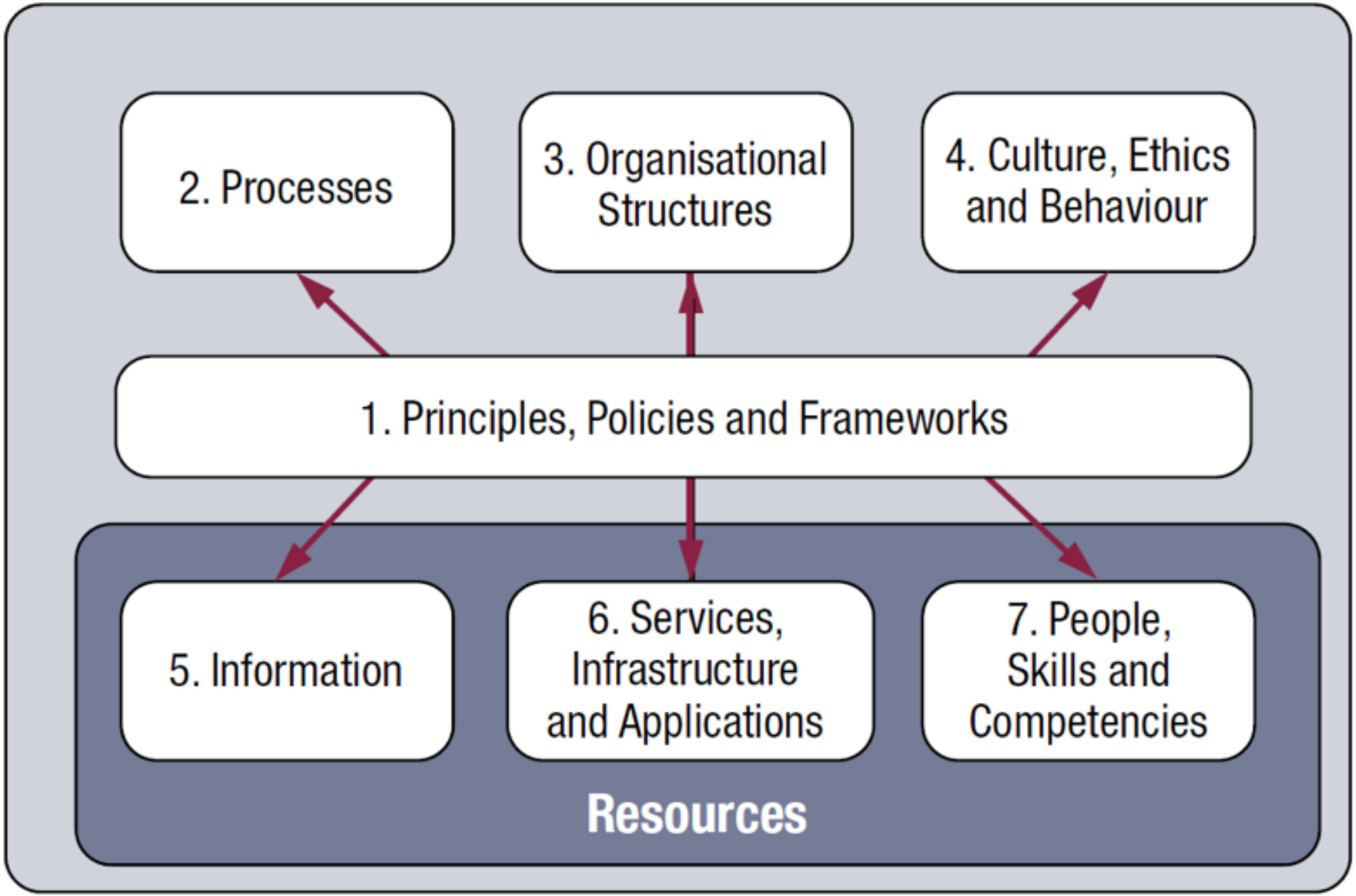
Enabling Processes

COBIT® 5

AN ISACA® FRAMEWORK

ISACA®

Trust in, and value from, information systems


2. Processes
3. Organisational Structures
4. Culture, Ethics and Behaviour
1. Principles, Policies and Frameworks
5. Information
6. Services, Infrastructure and Applications
7. People, Skills and Competencies
Resources

Cloud security evaluatiemodel

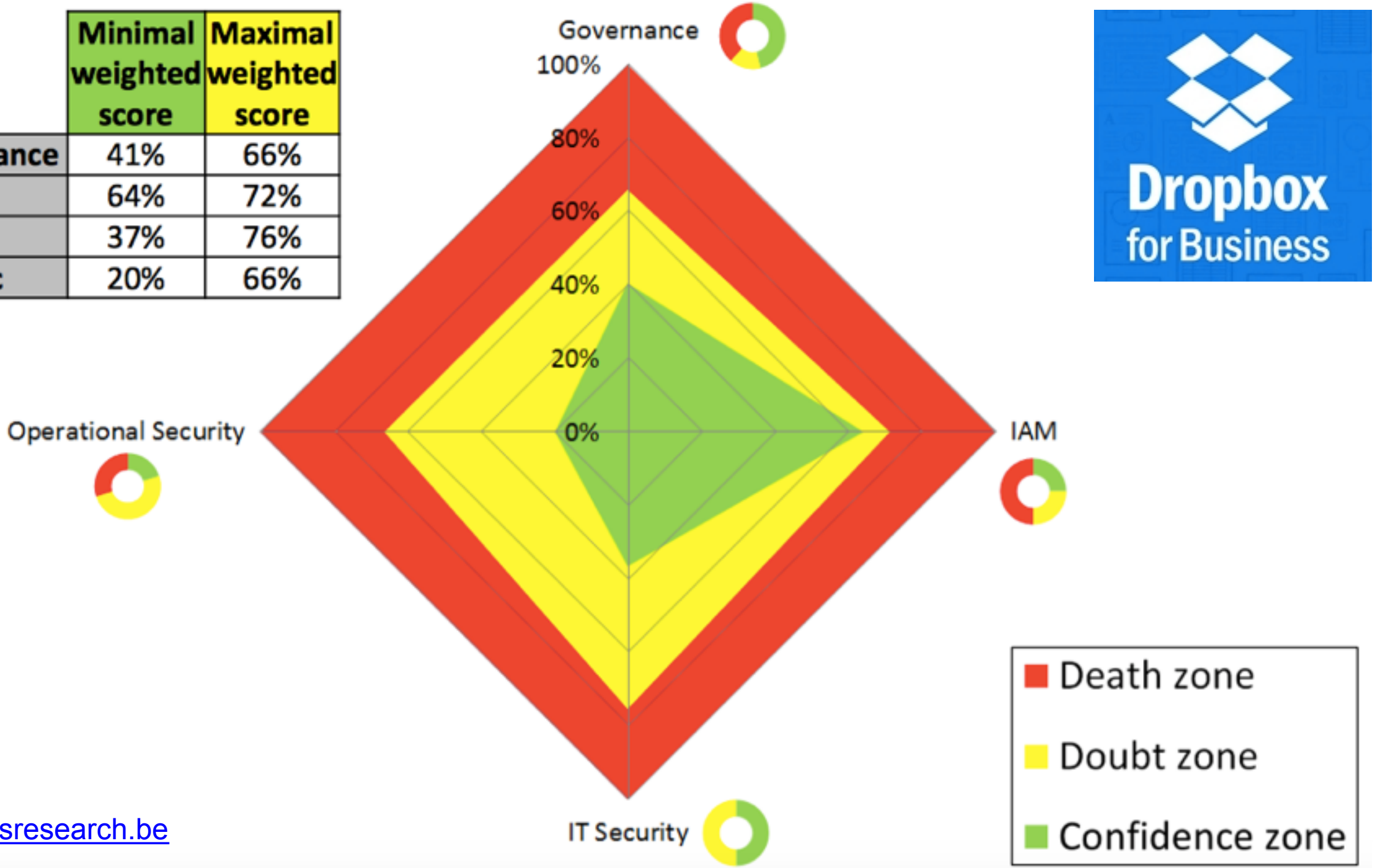
version FR

Context

De cloud is de laatste jaren een onontkoombaar en populair begrip geworden dat uitgegroeid is van een vaag en risicovol concept tot de ICT-strategie "van de toekomst" die elke organisatie vroeg of laat zal toepassen. Naast de kostenbesparingen is de hoofdreden van deze hype de vlotte toegankelijkheid tot tal van informaticaresources met bijna oneindig veel mogelijkheden, en dit alles met een minimaal beheer. Een organisatie kan op die manier de resources die gedeeld worden op een clouddienst huren waardoor hij dus de huurder ("tenant") wordt van de infrastructuur in plaats van de eigenaar. Het delen van zo'n infrastructuur is spijtig genoeg de achilleshiel van de clouddiensten. Cyberaanvallen hebben immers aangetoond dat het delen van eenzelfde clouddienst door tenants misbruikt kan worden. De beveiligingsproblemen, in het bijzonder vertrouwelijkheid en integriteit van gegevens, baren de gebruikers van de cloud dus veel kopzorgen omdat ze het volledige beheer van hun gegevens niet meer in eigen handen hebben. In de context van de overheid, sociale zekerheid en gezondheidszorg zijn deze problemen eens zo groot omdat ze mogelijk gevoelige gegevens betreffen van de burgers en ondernemingen.

Het model: gids voor cloud security

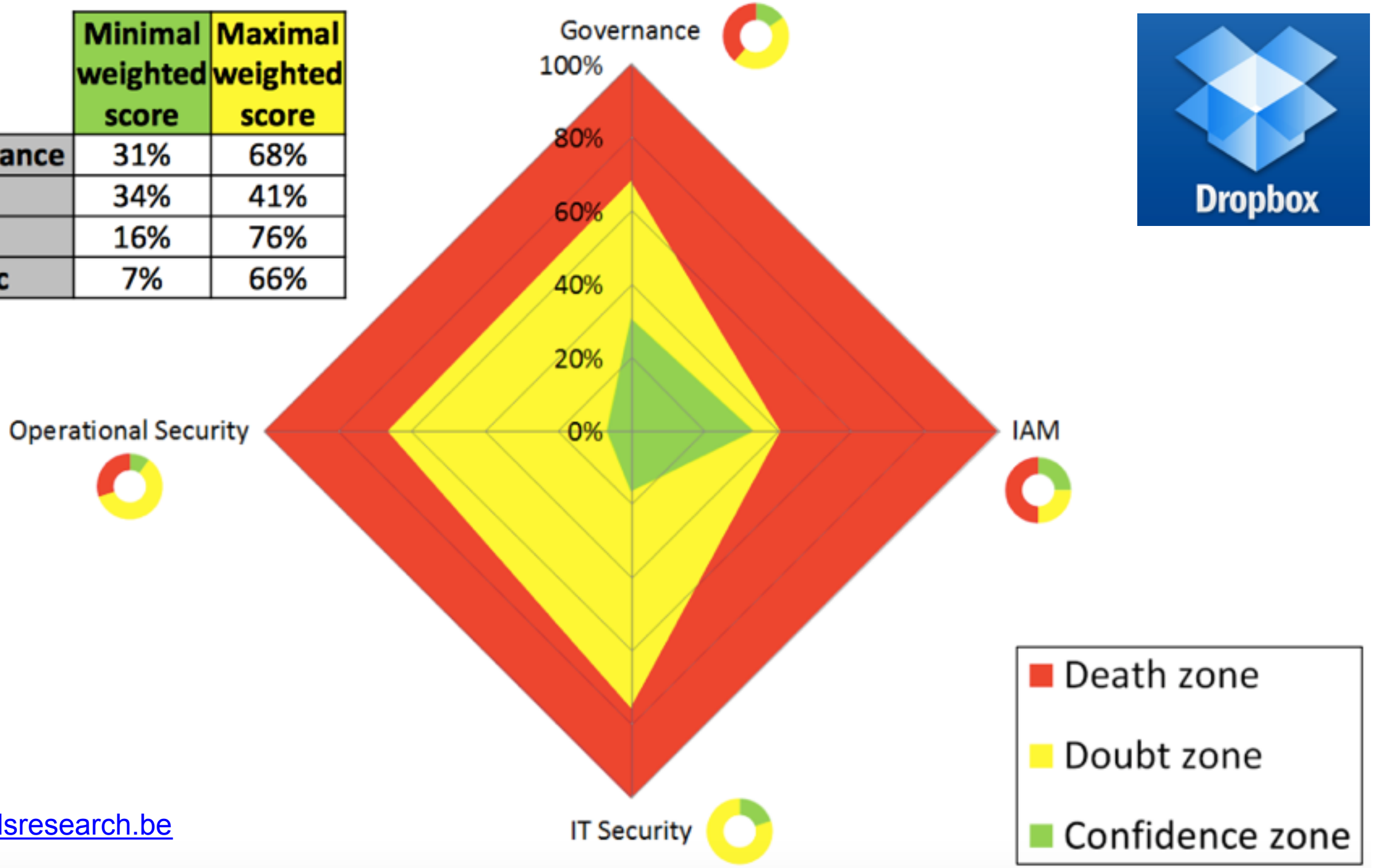
	Minimal weighted score	Maximal weighted score
Governance	41%	66%
IAM	64%	72%
IT Sec	37%	76%
Ope Sec	20%	66%



Dropbox for Business

www.smalsresearch.be

	Minimal weighted score	Maximal weighted score
Governance	31%	68%
IAM	34%	41%
IT Sec	16%	76%
Ope Sec	7%	66%



Dropbox

www.smalsresearch.be

Public

Internal

Confidential

Personal

Social

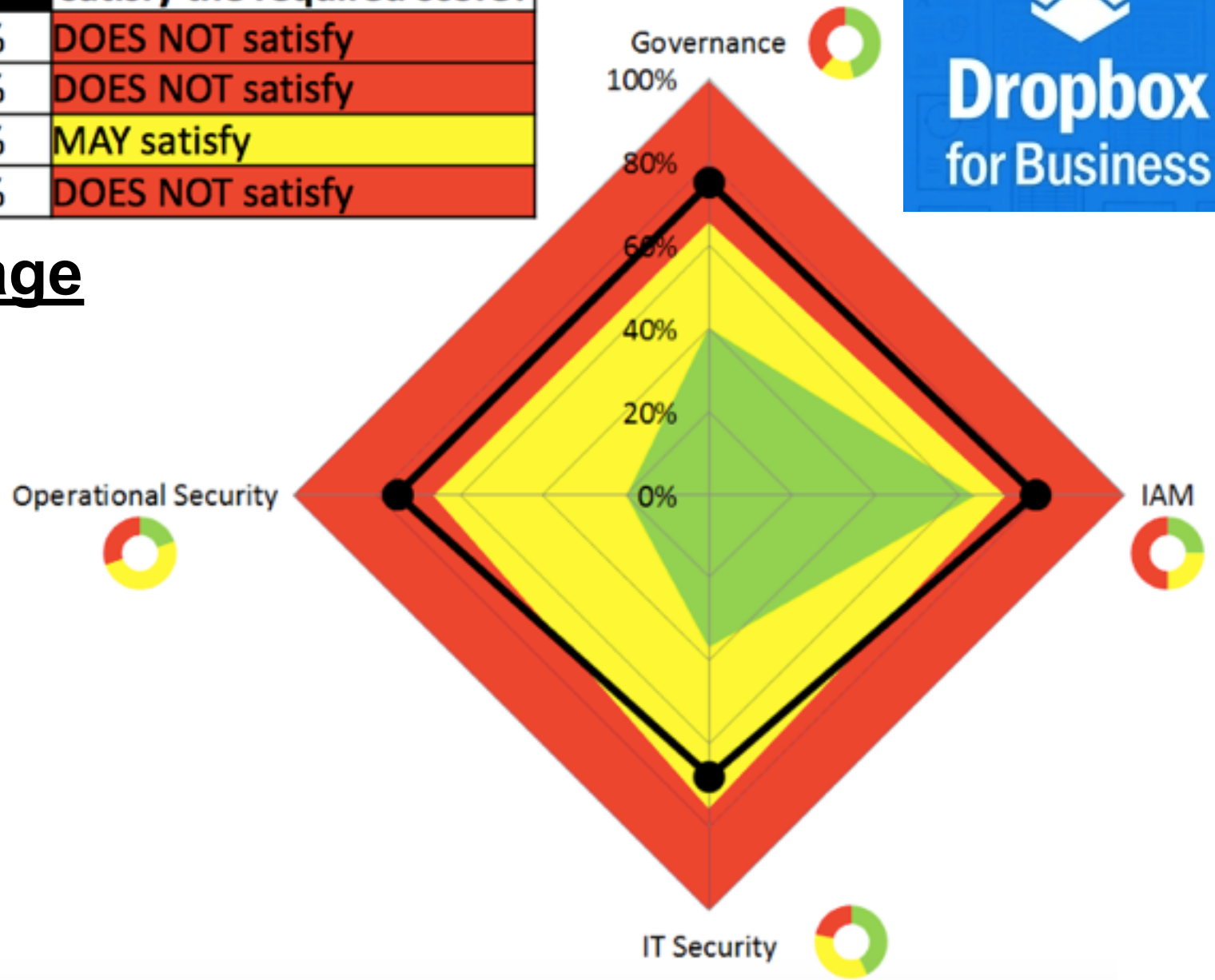
Medical

Ref: Data classification policy of the Belgian social security

REF

	Minimal weighted score	Maximal weighted score	Required score	Does Dropbox for Business satisfy the required score?
Governance	41%	66%	75%	DOES NOT satisfy
IAM	64%	72%	78%	DOES NOT satisfy
IT Sec	37%	76%	68%	MAY satisfy
Ope Sec	20%	66%	75%	DOES NOT satisfy

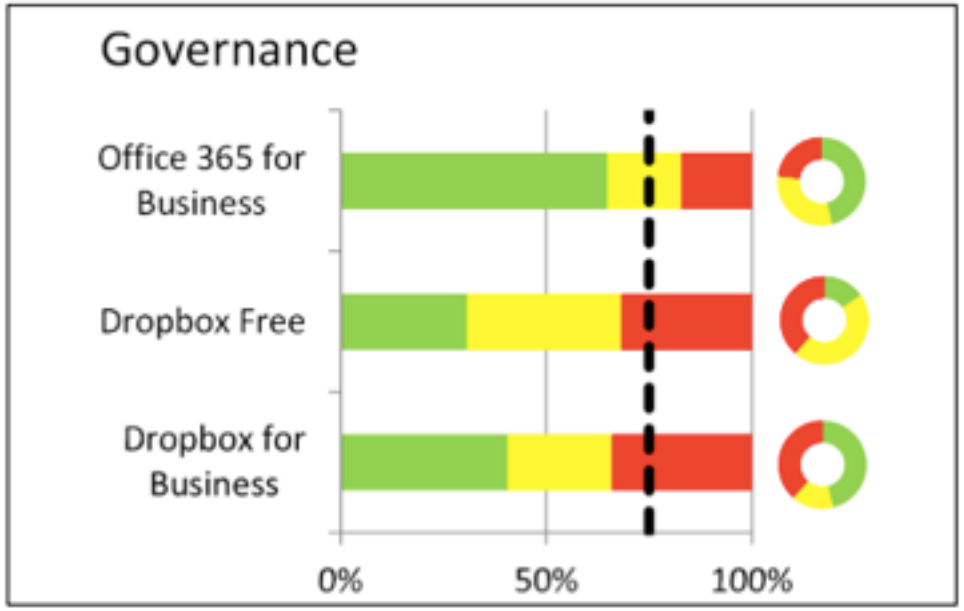
Example pay slip storage

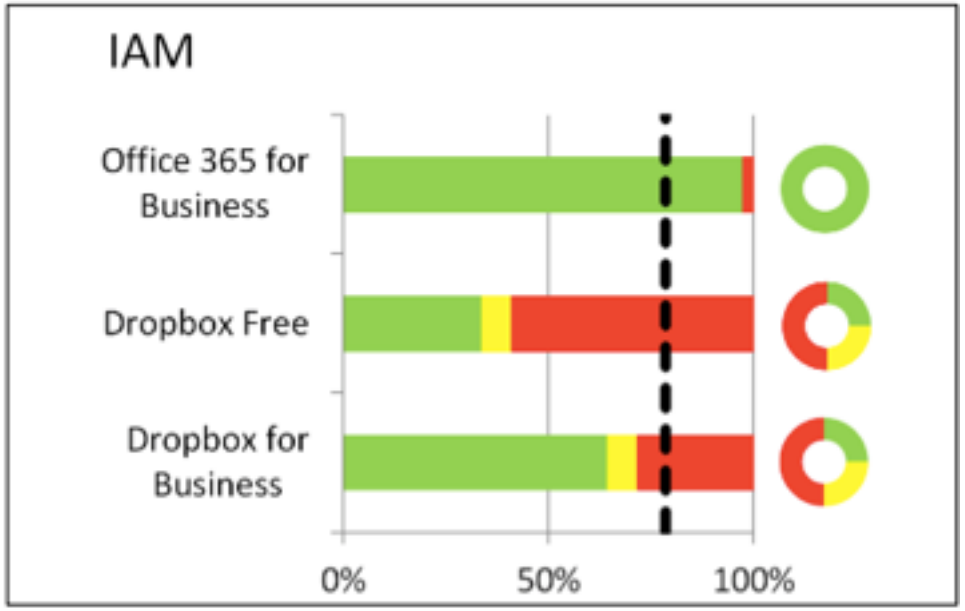


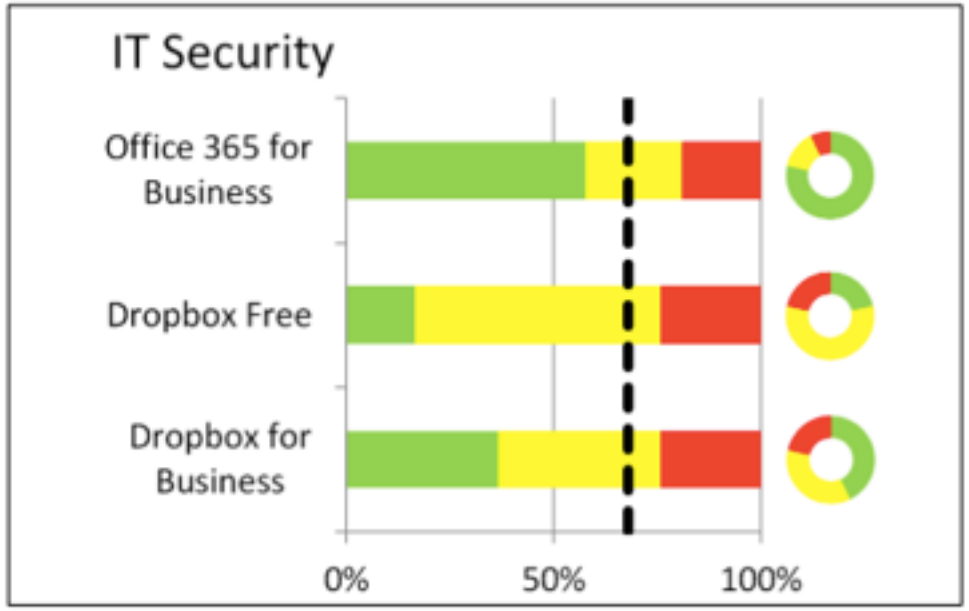
Dropbox for Business

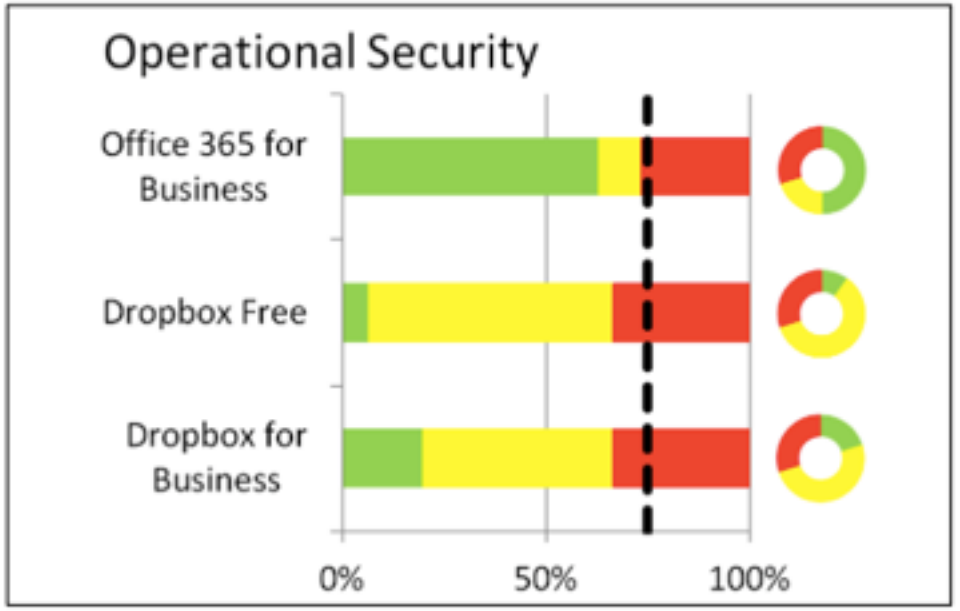
www.smalsresearch.be

Example pay slip storage









www.smalsresearch.be

ENISA's security guide and online tool for SMEs when going Cloud

Press Release
2015-04-10
http://enisa.europa.eu

ENISA publishes a security guide and an online tool for Cloud security for SMEs to help them assess the risks and opportunities when deploying Cloud services.

The security guide on SMEs

The guide highlights the most important **eleven (11) security risks** and **eleven (11) security opportunities for SMEs** to take into account when procuring a cloud service. A selection of **twelve (12) targeted security questions** linked to the security risks and opportunities are presented as a 'procurement cheat sheet' to provide SMEs with a clear view of the cloud service they procure. These features are enhanced by two exemplary cases of the use of cloud services by SMEs: as a customer and as a vendor offering services. The report indicates the challenges and opportunities in each case, and the security questions the SMEs should address to the provider in order to have a clear understanding of the current security state.

The SME security tool

The SME security tool is an implementation support for the security guide: using the tool, SMEs can rate the risks and opportunities according to their requirements and generate a customised list of security questions which can be used during procurement to collect information on the security measures adopted. The tool helps calculate and visualize risks and opportunities. The results of the tool are

SME Cloud Security Tool

SME Cloud Security Tool offers the functionality to rate the risks and opportunities and to generate a list of security questions to understand the main features of the cloud service under deployment. The tool can also calculate and visualise risks and opportunities, and consult the results into a customised set of security questions. Rate the security opportunities and the security risks below according to your organisation requirements.

Opportunities

As every SME is different, not all of these security opportunities to cloud services are as important for all of you. This tool enables you to select the rating or ranking of the opportunities most relevant to you as an SME using the following scale:

- Small opportunity: As an SME you could exploit this opportunity, but benefits would be limited.
- Medium opportunity: As an SME you should exploit this opportunity, because benefits would be significant.
- Large opportunity: As an SME you must exploit this opportunity, as there would be crucial benefits.

ID	Title / Description	Opportunity
O1	**Geographic spread** *Geographic spread can provide resiliency against regional issues and local disasters such as storms, earthquakes, or cable cuts. It can also be used to mitigate certain Denial of Service (DoS) attacks, allowing customers to get access at other locations.*	Small (Could Have) Medium (Should Have) High (Must Have)
O2	**Elasticity** *Cloud computing providers can use large data centers with large amounts of spare resources, to be able to respond to rapid changes in resource usage, peak usage, and Denial of Service (DDoS) attacks.*	Small (Could Have) Medium (Should Have) High (Must Have)

ISACA

AN ISACA CLOUD VISION SERIES WHITE PAPER

CLOUD GOVERNANCE:

Questions Boards of Directors Need to Ask

Cloud computing is gaining momentum. As cloud offerings gain maturity, cloud service providers are becoming more competitive. Some providers are reducing prices as they realize investments and leverage economies of scale. Others are differentiating based on quality, for example, providing better availability, improved security or enhanced ability to manage services. While the benefits of cloud computing are real in economic, strategic and operational terms, realizing those benefits is not a simple process. To achieve the benefits of cloud computing, adoption drivers must be aligned with enterprise goals and objectives, and business and cultural factors must be favorable for adoption. Like any investment, cloud projects should be guided by the board of directors to ensure value creation and optimization of risk. When evaluating cloud initiatives, board members should ask their management teams specific questions, the answers to which will determine whether cloud services will have a positive and sustainable impact on enterprise goals and whether risk remains within enterprise tolerances.

ISACA
Trust in, and value from, information systems

GOVERNANCE QUESTIONS THE BOARD OF DIRECTORS SHOULD ASK ABOUT CLOUD

1. Do management teams have a plan for cloud computing? Have they weighed value and opportunity costs?

2. How do current cloud plans support the enterprise's mission?

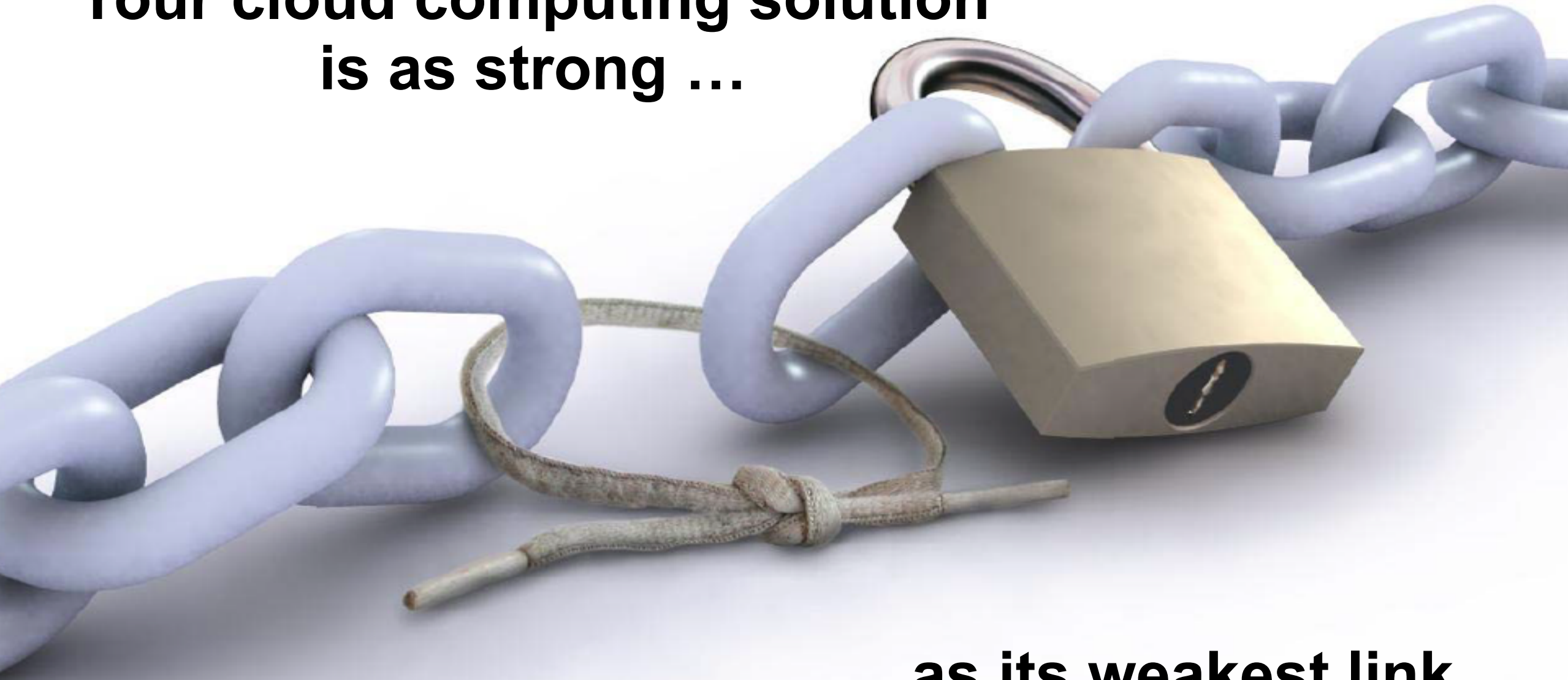
3. Have executive teams systematically evaluated organizational readiness?

4. Have management teams considered what existing investments might be lost in their cloud planning?

5. Do management teams have strategies to measure and track the value of cloud return versus risk?

ISACA®
Trust in, and value from, information systems

Your cloud computing solution is as strong …



… as its weakest link

CLOUD REFERENTIES

NIST Special Publication 800-145: The NIST Definition of Cloud Computing. NIST, 2011 http://csrc.nist.gov/publications/nistpubs/800- 145/SP800-145.pdf

ISACA Cloud Computing Guidance.
http://www.isaca.org/cloud

European Union Agency for Network and Information Security
ENISA
http://www.enisa.europa.eu/

Cloud Security Alliance
CSA
https://cloudsecurityalliance.org/

ISACA
Trust in, and value from, information systems

LATEST CLOUD TRENDS : NEW SERVICE OFFERINGS

- **Security as a Service (SecaaS)**

– CSP provides standalone MSS ranging from antivirus scanning and mail security to full deployments of end-point security.

– CSP offloads appliance utilization for client, and CPU- & memory-intensive activities are moved to cloud services : minimized risk when applying patches/updates (no longer directly linked to the device).

- **Disaster Recovery as a Service (DRaaS)**

CSP offers cloud infrastructure to provide enterprise with DR solution: back-up equipment & storage & BCP services.

– Reducing cost for in-house DR infrastructure (ROI in DR services).

– Offsite storage=DR environment is less likely to fail in case of major disaster.

- **Identity as a Service (IDaaS)**

– Management of identities in the cloud that is separated from users & applications that use identities: managed identity services (including provisioning) or management for both onsite/offsite services. Delivering SSO solution can also be part of the cloud service offering.

– Deliver IAM solution: access & roles are configured by CSP and users are authorized by enterprise internal solutions (federated model).

LATEST CLOUD TRENDS : NEW SERVICE OFFERINGS

- **Data Storage/Analytics as a Service (Big Data)**

analyze all types of data by taking away constraints on volume, variety, velocity and veracity removed through synergy between new technologies & extended capabilities provided by cloud computing. Enterprises receive decision-making support from info that results from big data analysis, such as real-time reporting and predictive analysis.

- **Information as a Service (InfoaaS)**

provides required information: query result is more important than query.

- **Integration Platform as a Service (IPaaS) (“cloud integrator”)**

“a suite of cloud services enabling development, execution and governance of integration flows connecting any combination of on premises and cloud-based processes, services, applications and data within individual or across multiple organizations.” Cloud integrators help cope with complexity + facilitate integration without need to constantly modify & maintain diverse incompatible applications. IPaaS enables efficient & cost-saving methods to ensure IT integration throughout enterprise + provides more robust solution in areas of data confidentiality, integrity and availability + data GRC.

- **Forensics as a Service (FRaaS)**

“establishes cloud forensic investigative process, which can be implemented within cloud, integrated with tolls that should endure relevant information gathered, verified and stored in a manner that is forensically sound & legally defensible.”

LATEST CLOUD TRENDS : CLOUD SERVICE BROKER (CSB)

Third-party provider with access to multiple data centers & cloud service offerings.

CSB integrates & tailors those various services into 1 service that can be intertwined with enterprise in-house applications and systems.

Advantages:

- helps enterprise to determine best possible framework for integration with cloud services.
- can guarantee interoperability between various cloud services needed. Additional support for in-house applications ensures cloud adventure integrates seamlessly within enterprise environment.
- because of integration with various CSPs, going cloud becomes cost-effective.

important prerequisites:

- cloud computing standards to increase benefits & reduce risk.
- cloud standardization will help CSPs & users build more robust portable solutions.

ISACA
Trust in, and value from, information systems

LATEST CLOUD TRENDS : CLOUD STANDARDIZATION

Moving to the cloud still provides many challenges : Portability, interoperability, certifications, correct service level agreements (SLAs) and knowing what to expect.

Governments are encouraging cloud standardization and are working on developing legislation concerning cloud. EU has Cloud Select Industry Groups (C-SIGs) currently working on cloud code of conduct, voluntary datacenter certification, standardized SLAs and data protection.

Certifications in cloud operations, security or code development are important for enterprises & individuals.

ISACA

LATEST CLOUD TRENDS : G-CLOUD

Public-sector IT investments are increasingly influenced by

- financial constraints,
- rapidly aging technology
- higher standard of service delivery that is demanded by the community.

G-Cloud = government's answer to new approach of IT sourcing & management and is considered critical to

- achieve value,
- decrease cost of its IT infrastructure,
- drive innovation
- support sustainable investments

A second evolution in G-Cloud is its deployment to citizens = cloud broker service to supply various cloud solutions to citizens

Guidance

How to use CloudStore

Organisation: Cabinet Office
Page history: Published 1 November 2013
Topic: Government efficiency, transparency and accountability
Primary category: Government funding programmes

Information about buying and supplying cloud-based services using the G-Cloud framework.

Contents

Overview

CloudStore is an online marketplace where suppliers offer their services to the public sector via the G-Cloud framework. Public sector bodies can review and buy these services on CloudStore.

Cloud computing lets you access internet-based computing, reducing the need to invest in your own hardware and software. Therefore, by using CloudStore you can:

- avoid long contracts
- buy the exact amount of computing resources you need

ISACA®

Trust in, and value from, information systems