KPMG

Hacking the Cloud – June 2011

Security in the 'cloud'
Myth versus Reality

drs. Mike Chung RE

AUDIT ▪ TAX ▪ ADVISORY

Tabloid Science: Attack of the Maneating Catfish

October 31, 2008

If London's *SUN* newspaper is to be believed, a giant Asian catfish known as the Goonch has mutated into a maneater, after developing a taste for the human remnants dumped from riverside funeral pyres. Based on a new documentary being aired on Britain's Channel 5 television, the behemoth catfish tale has just enough plausibility to focus new interest on a species that occasionally makes its way into home aquariums.

The recently published tabloid article by Emma Cox leads off proclaiming: "A FEARSOME mutant fish has started killing people after feeding on human corpses, scientists fear," under a headline of "Humans scoffed by mutant fish." (Scoff being British/Canadian slang for gobble.)

Tracking the Goonch for the show "Nature Shock," biologist Jeremy Wade presents ichthyological scare story, complete with needle-toothed monsters from the deep that may have risen from bottom scavengers to apex predators.

Folk Theory

Along the Great Kali River, flowing between India and Nepal, some villagers told Wade that they believe a "monster" dwells in their midst. Their theory is that it has evolved from eating prawns to a killer with an acquired taste for humans.

Hypothesis

- Cloud computing is a neologism
- Off-premise cloud services are generally far better secured compared to on-premises IT at enterprises
- In god* we trust

* No specific religion

I. Neologism of the cloud

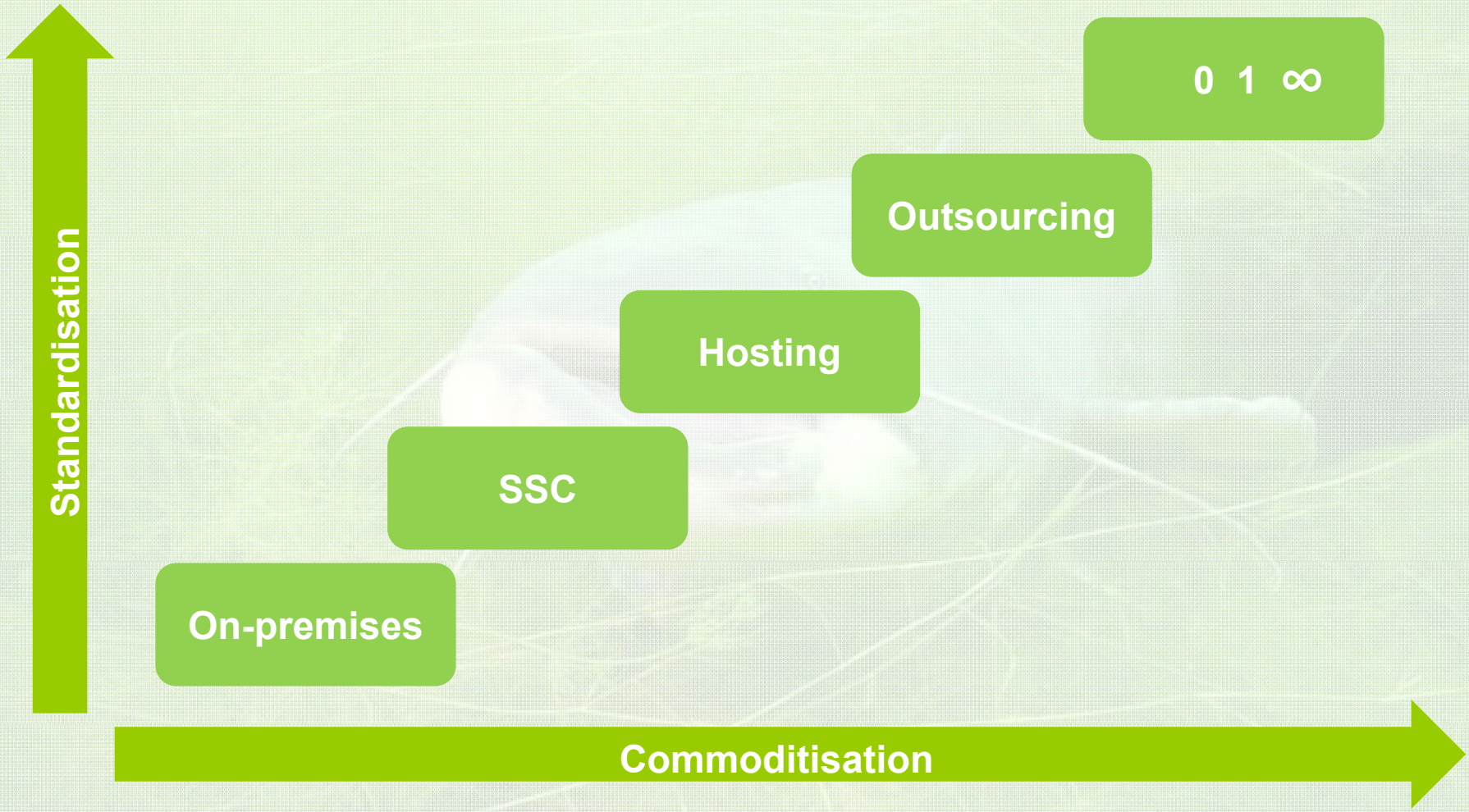
"The interesting thing about cloud computing is that we've redefined cloud computing to include everything that we already do. I can't think of anything that isn't cloud computing with all of these announcements. When is this idiocy going to stop?" Larry Ellison

Cloud means everything and nothing

- Cloud computing is an all-embracing, therefore a meaningless term

- We are witnessing a paradigm shift from on-premise IT towards external delivery of services
  - Commoditization – portfolio management, standardization of IT resources
  - Centralization – SSC, hosting, (out)sourcing, external cloud
  - Massive investments by the IT industry in various types of external cloud services

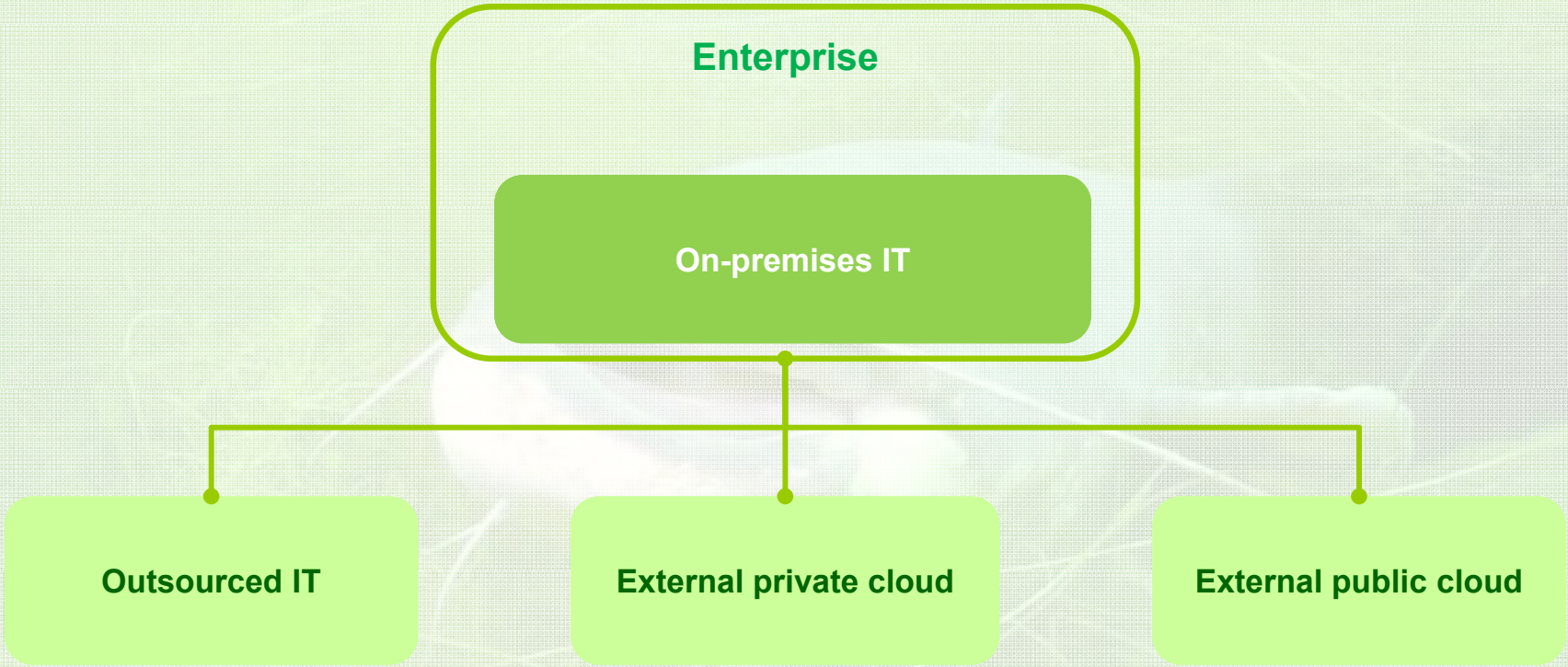
Paradigm shift



Future mode is a hybrid IT

- The IT environment for the years to come is a hybrid IT environment
  - External cloud market is marginal
  - Growth of external cloud services cannot be ignored
  - Future mode of IT is a hybrid environment with growing significance of external cloud services

Hybrid IT environment



II. Security of the cloud

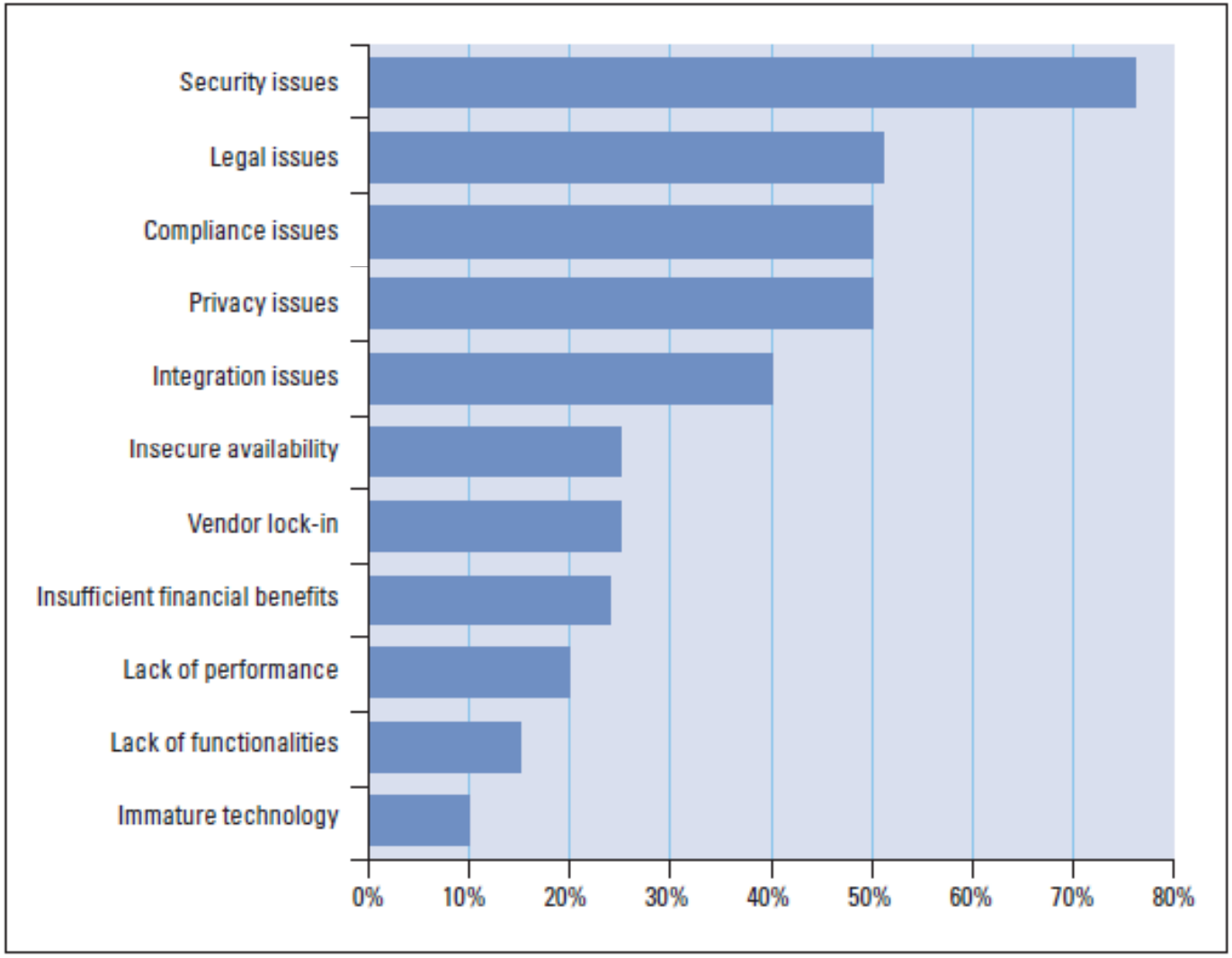
"The biggest issue for me when it comes to cloud computing is obscurity. It is not exactly about the lack of security measures, but the total lack of transparency." CISO of a firm in the industrial markets sector

Information security

- **Definition**
  - Information security means protecting information and information systems from unauthorized access, use, disruption, or destruction
  - The terms information security, computer security and information assurance are frequently used interchangeably
- **Quality aspects**
  - Confidentiality
  - Integrity
  - Availability
- **Scope**
  - Digital data
  - Corporate environment

What the CIOs think

What are your main concerns regarding the use of cloud computing?



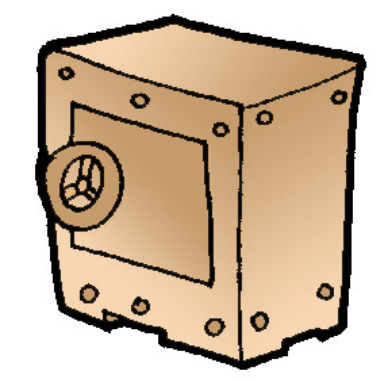
Source: KPMG the Netherlands, 2010

Cloud incidents in practice

- Thousands of customers lost their data in the cloud due to the ‘Sidekick disaster’ of Microsoft/T-Mobile (2009)
- Botnet incident at Amazon EC2 infected customer’s computers and compromised their privacy (2009)
- Gmail was unavailable for several hours due to unspecified reasons (2010)
- Gmail was (apparently) hacked by ‘Aurora’ (2010)
- GoGrid’s network problems had major impact on service availability (2011)
- Hotmail lost e-mail for two days (2011)
- Salesforce.com was partly unavailable for 30 minutes due to unspecified reasons (2011)
- Amazon EC2 services crash compromised customer’s data (2011)

A comparison

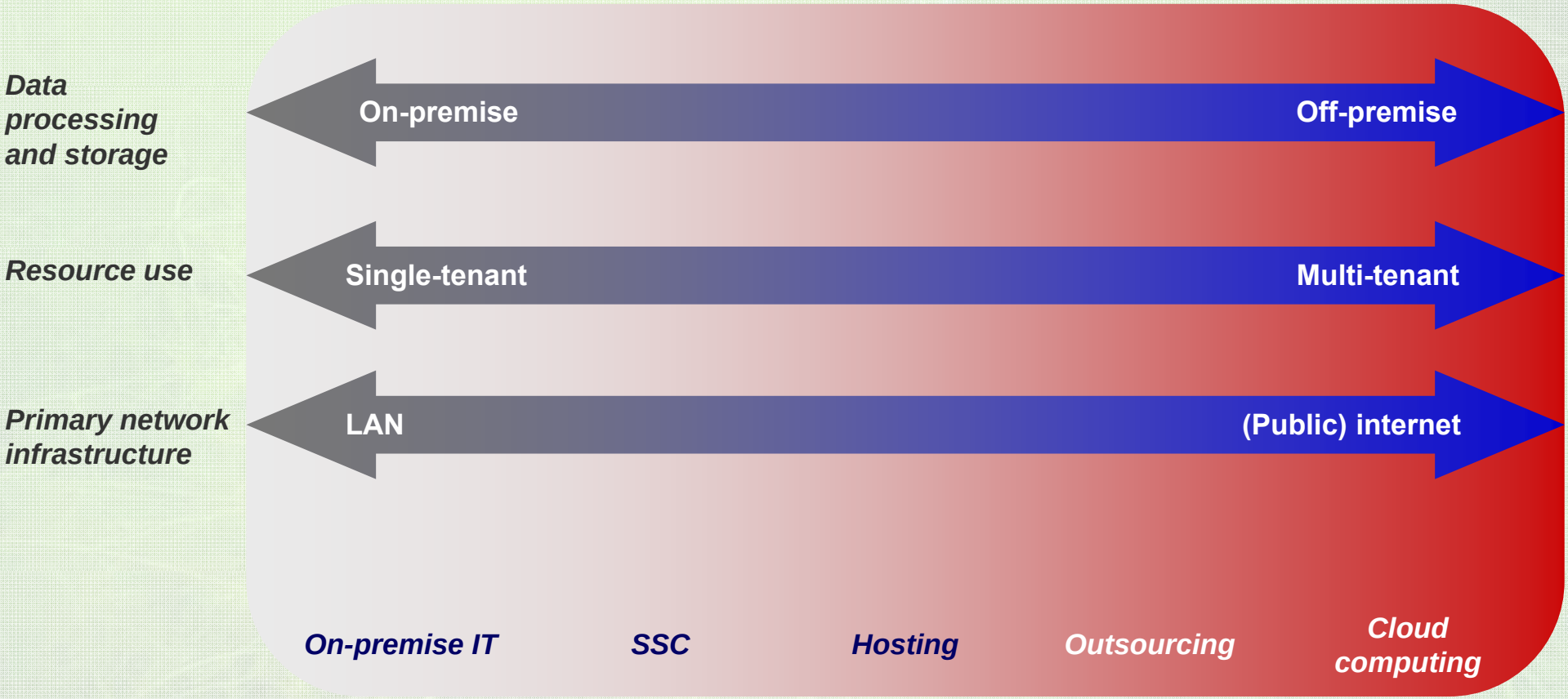
Towards



Risk profile of the cloud

- **Location of data storage and IT assets**
  - Traditional IT: on-premise; within the internal security domain of customer
  - Cloud computing: off-premise; outside the internal security domain of customer; hosted/located at cloud service provider or distributed/scattered over a multitude of (third party) providers
- **Usage of (IT) resources**
  - Traditional IT: exclusive for the customer
  - Cloud computing: varying degrees of multi-tenancy
- **Principal infrastructure**
  - Traditional IT: LAN, leased lines
  - Cloud computing: public internet

Risk profile of the cloud



Specifice challenges

- Loss of governance: no control over critical security areas like vulnerability management, infrastructure hardening, physical security etc.
- Data storage: data may be stored in the cloud without proper customer segregation allowing possible accidental or malicious disclosure to third parties
- Data deletion: customer data that was required to be deleted may still be retained on backup servers or storage located in the cloud without customers' knowledge
- Identity and Access Management: weak logical access controls due to immature technology and poor integration
- e-Investigations: the ability for cloud customers to invoke their own electronic investigations procedures within the cloud can be limited by the delivery model in use, and the access and complexity of the cloud architecture

Specifice challenges

- Breach/disclosure: timely discovery and reporting of a breach by the cloud provider may be challenging
- Security monitoring: customers cannot effectively deploy monitoring systems on infrastructure they do not own; they must rely on the systems in use by the cloud service provider for security monitoring
- Frequently changing technology and virtualization: skills and knowledge enhancement required for staff to work with virtualization and other new cloud technologies
- Confidentiality: the cloud facilitates the ability to use/share data across organizations and therefore increases the potential for secondary uses of data that require additional consent or authorization

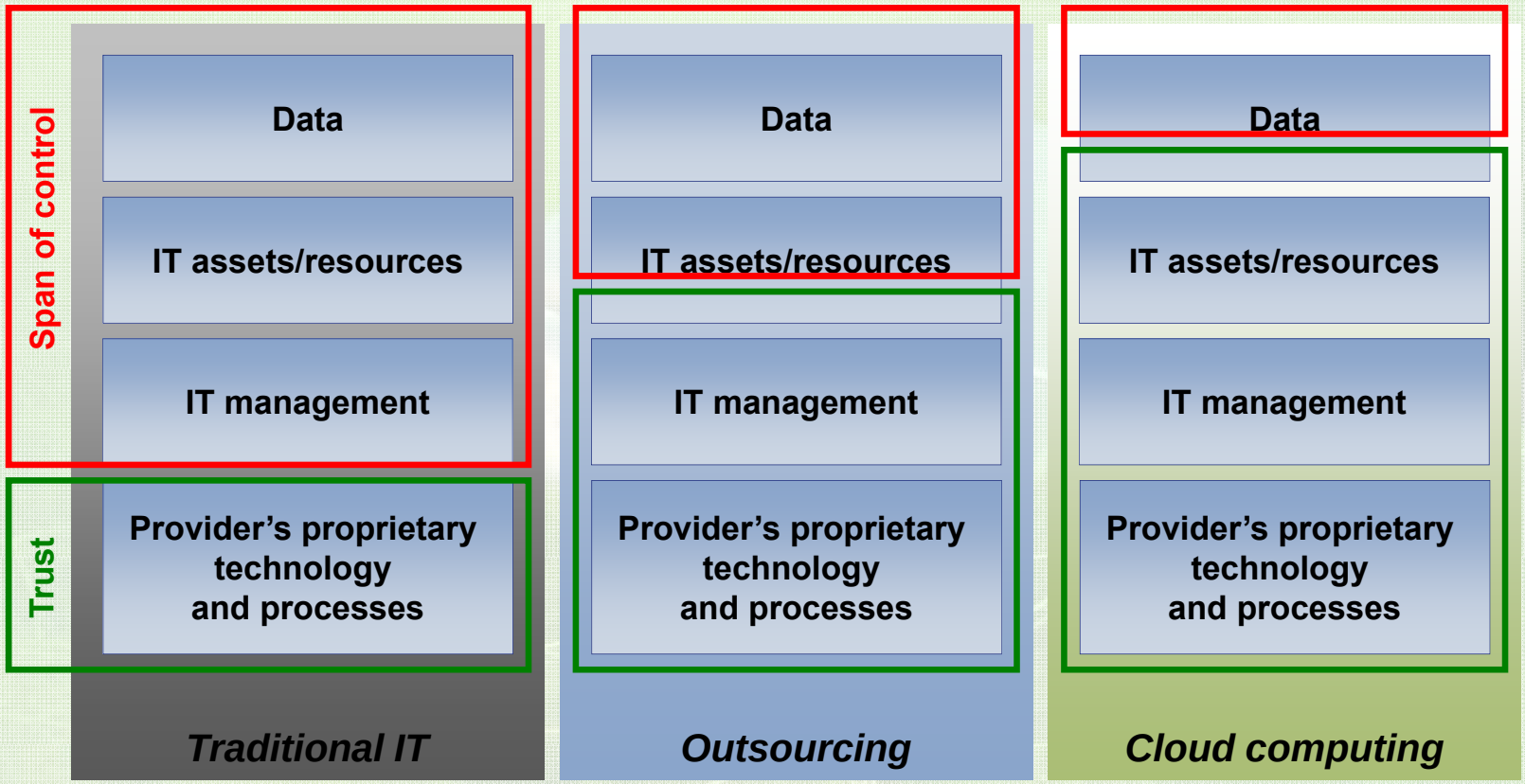
III. How to trust?

"While he was speaking, a cloud appeared and enveloped them, and they were afraid as they entered the cloud." Luke 9:43

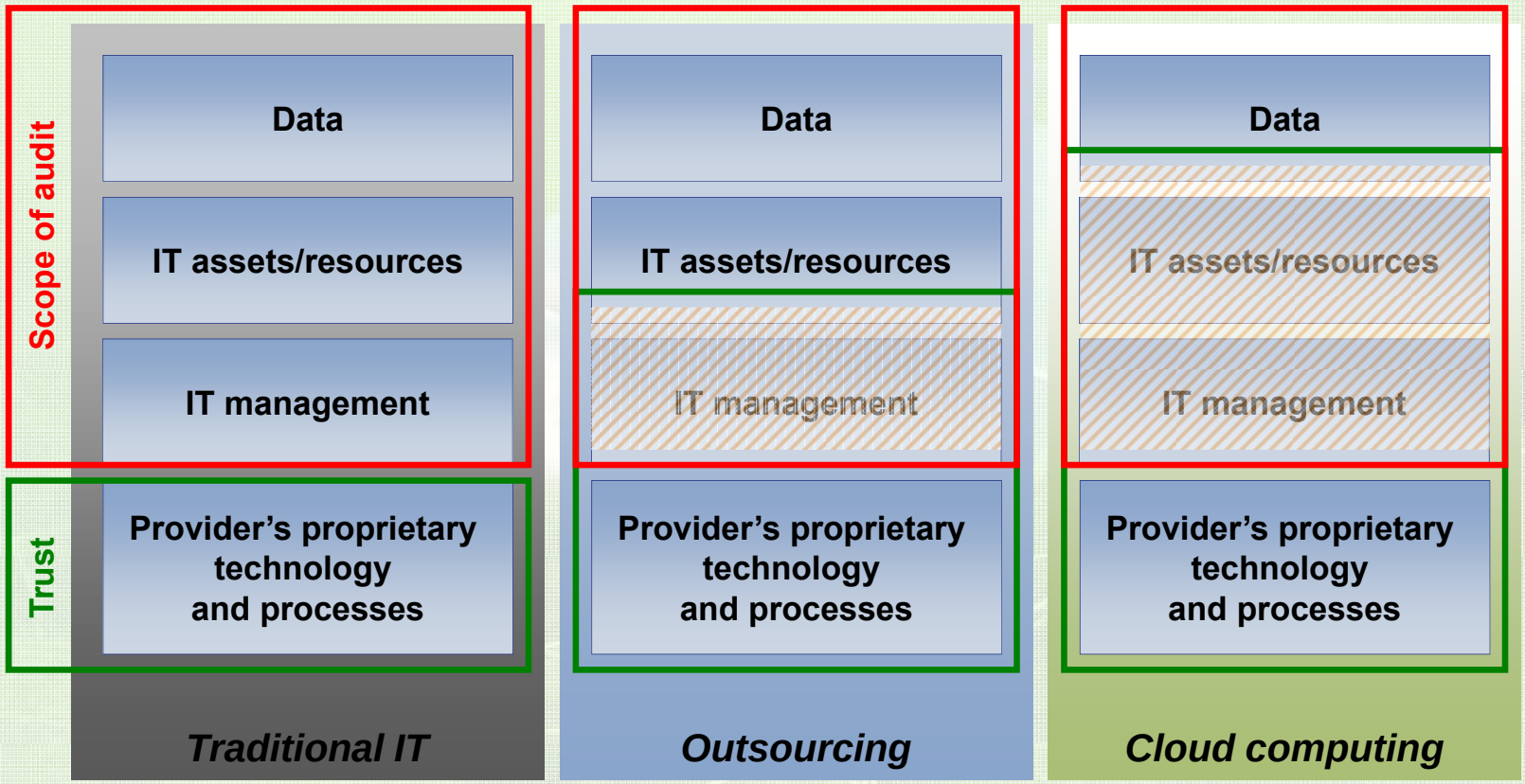
Basis of trust

- Reputation
- Guarantee
- Assurance

Control & trust



Area of difficulty



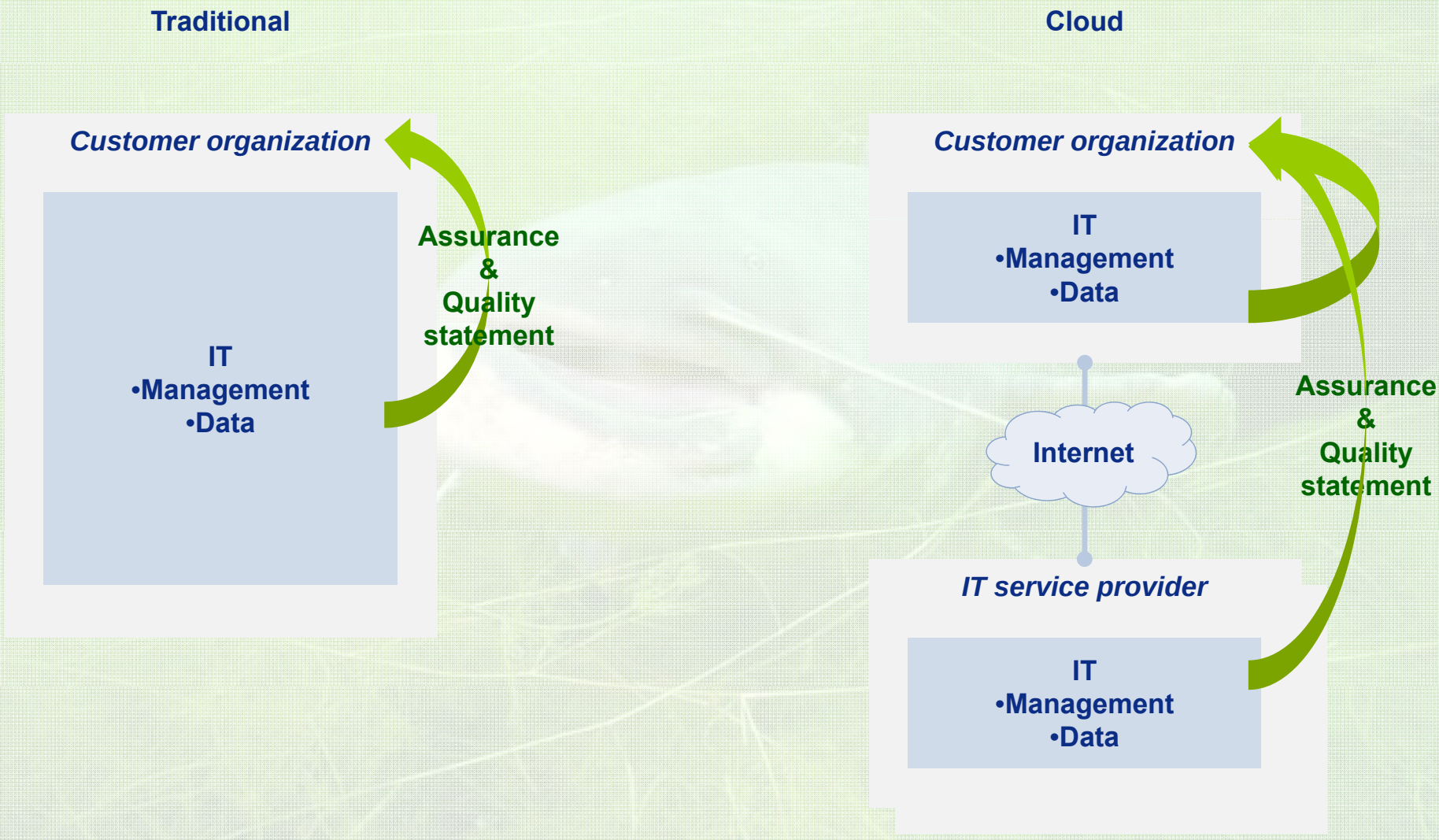
Current audit standards

- Localized IT as starting point (ITIL)
- Strong focus on ‘traditional’, on-premise IT (ISO27001/2, PCI DSS)
- Static (Cobit)
- Strong focus on processes (SOx)

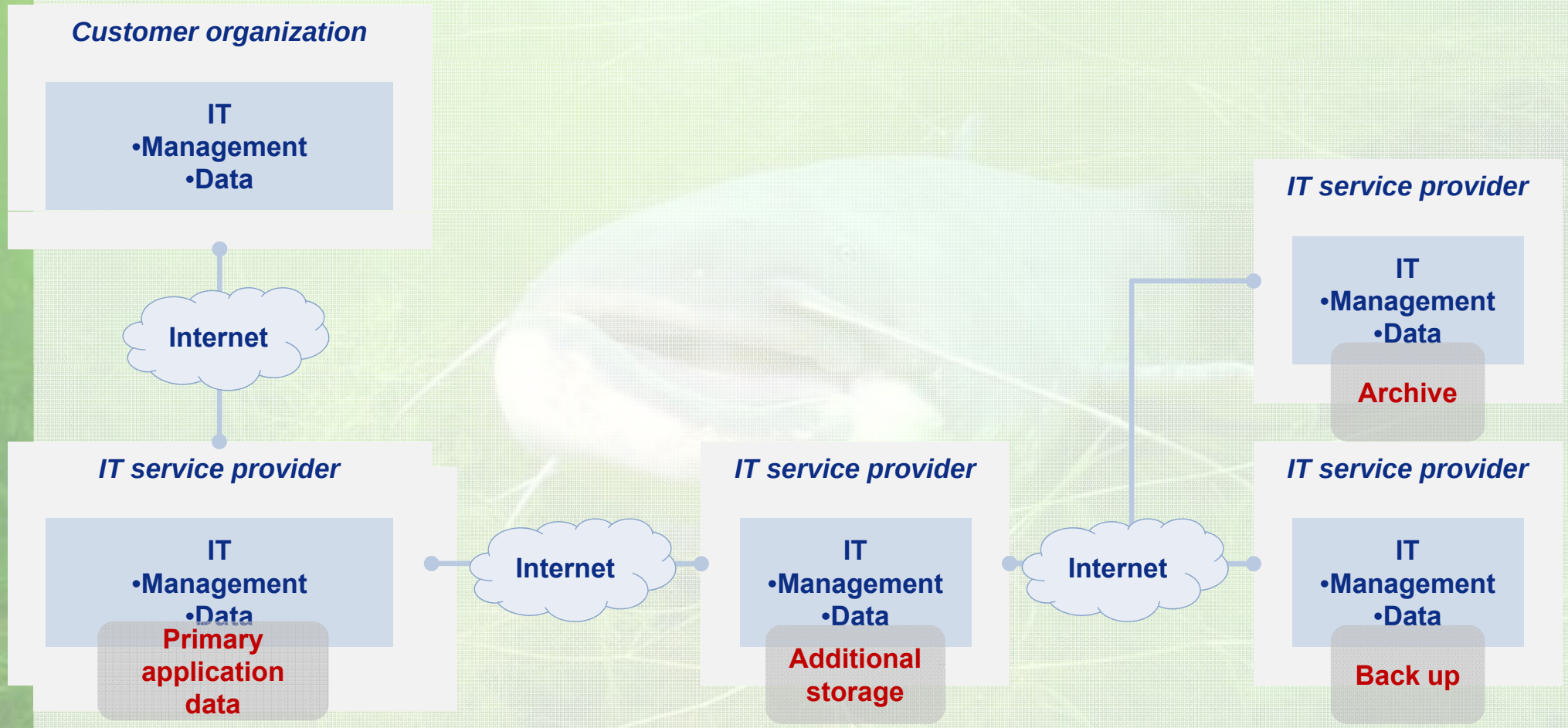
New audit standards

- Abundance of ‘standards’
  - ENISA, Cloud Computing Benefits, risks and recommendations for information security
  - ENISA, Cloud Computing Information Assurance Framework
  - Cloud Security Alliance (CSA)
  - ISACA
  - ISF
  - OWASP, Application Security Verification Standard 2009 – Web Application Standard, 2009
  - KPMG, Beveiligingraamwerk SaaS
- Limited scope, mainly focused on security
- Scarcely used, barely accepted by the market

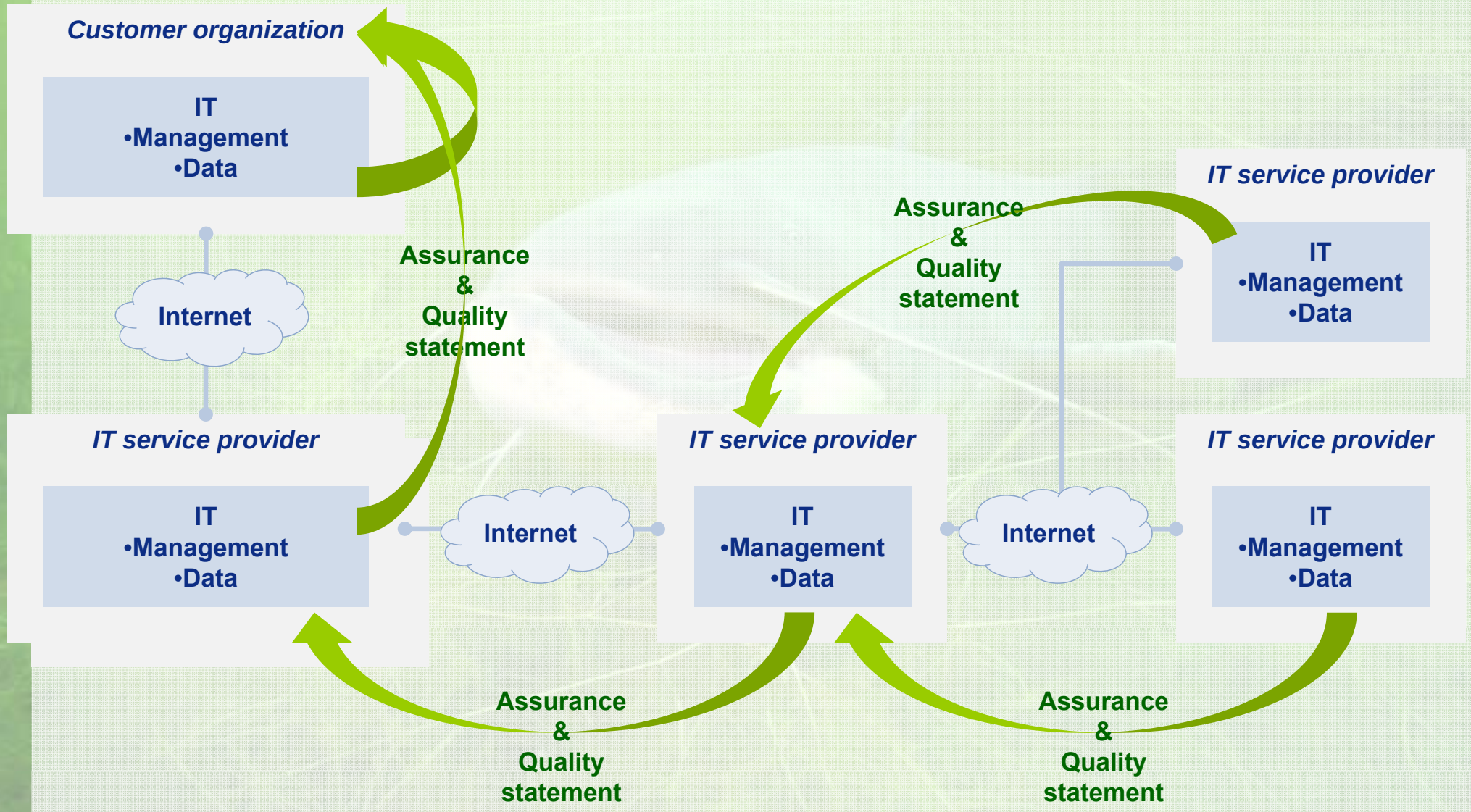
Assurance: an example



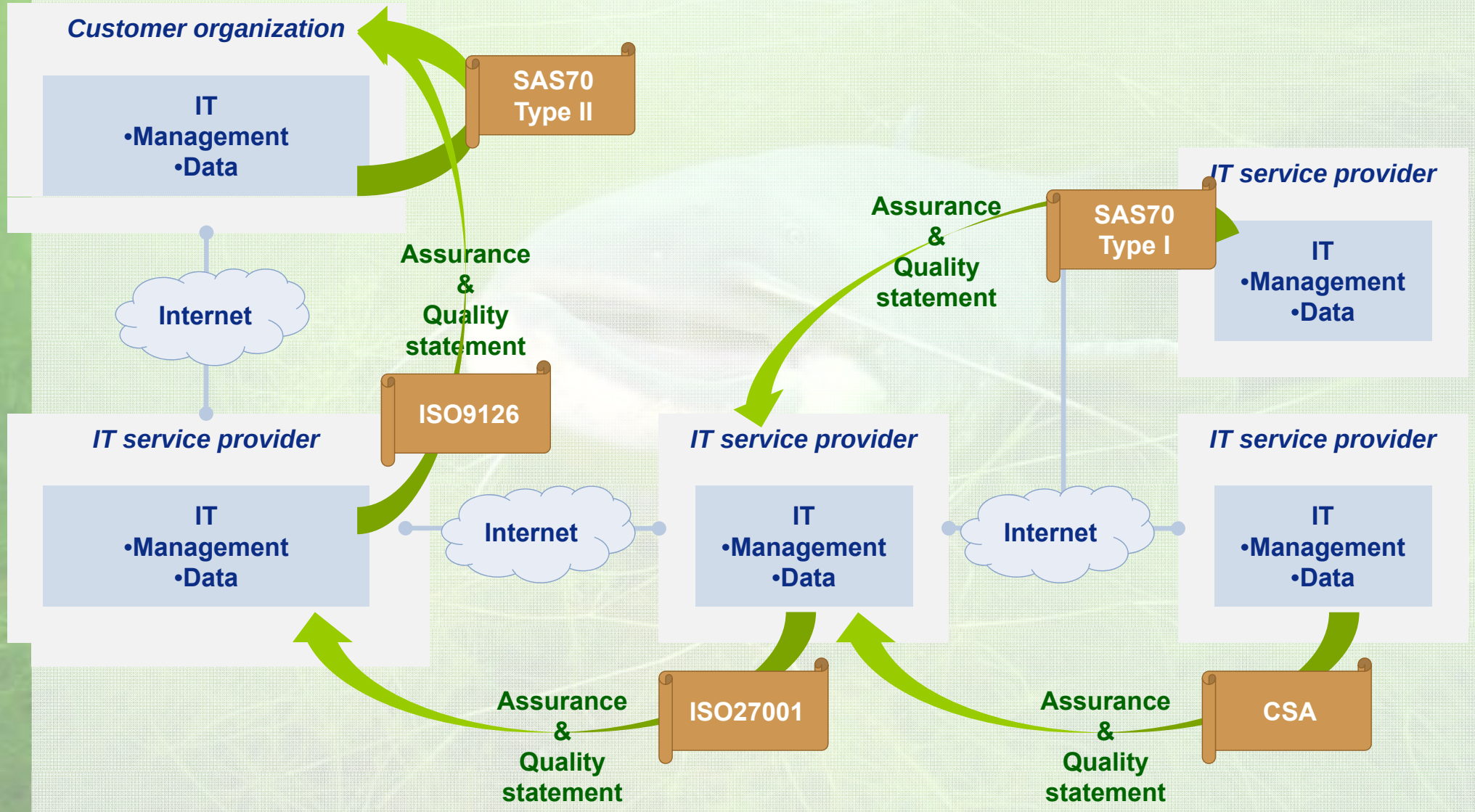
Assurance: an example



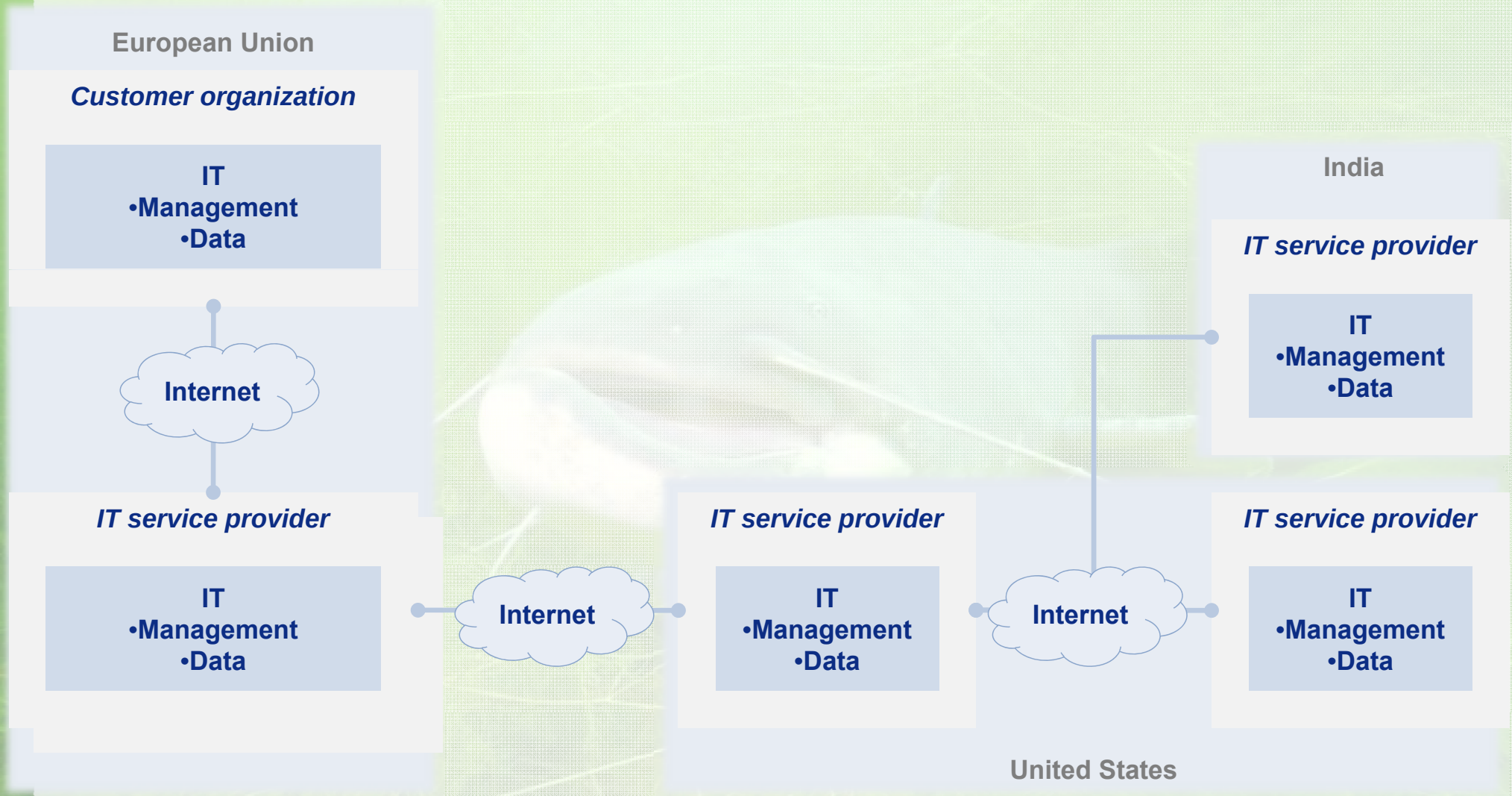
Assurance: an example



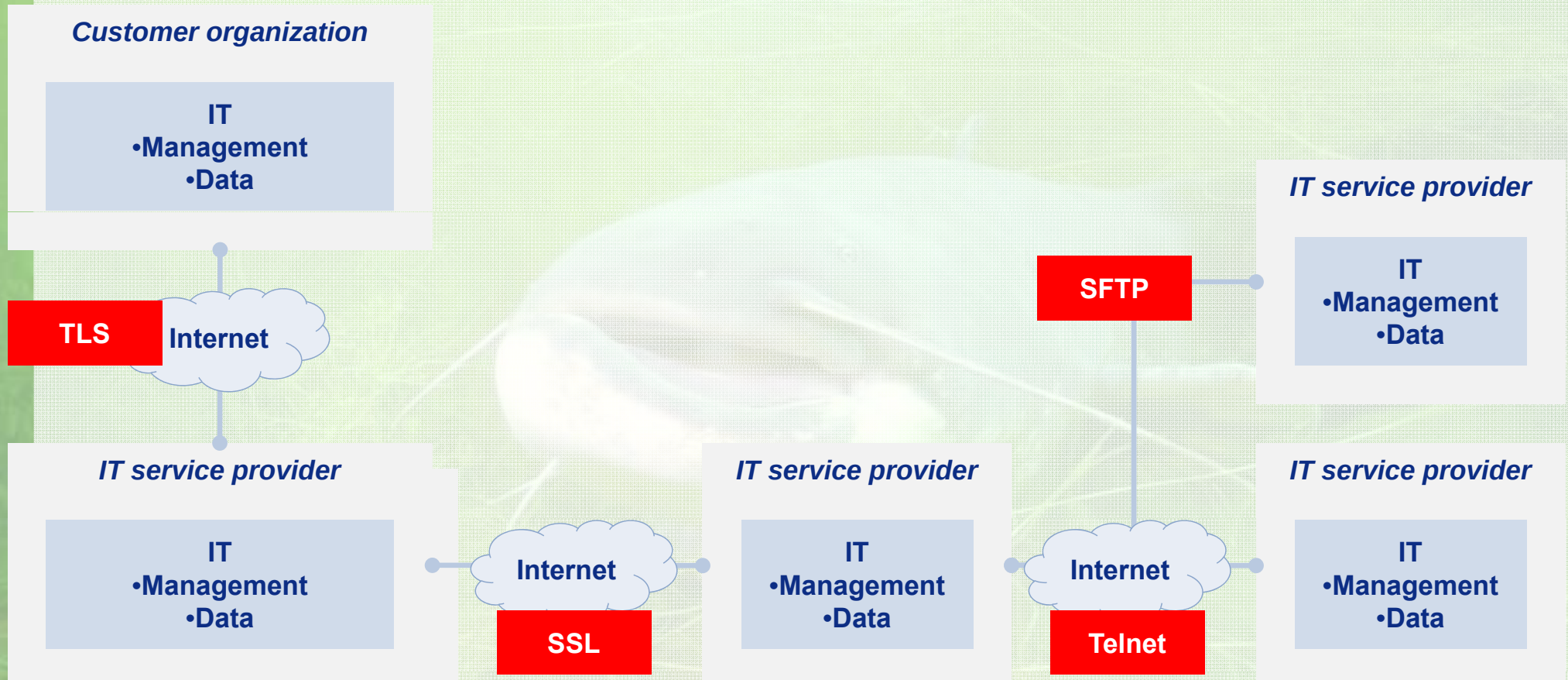
Assurance: an example



Assurance: an example



Assurance: an example



Audits

- Audits are partly limited
  - Limited to processes relevant to financial statements
  - Wide intervals between audits
  - Same standards used as for on-premise IT environments - hardly any attention on multi-tenancy, service integration and external data storage
- Quality of audits is difficult to judge
  - Free to choose the controls
  - Dependent on the expertise and view point of the auditor
  - Many variations on audit approach, set-out and level of (technical) detail
- Audit reports are superficially reviewed by (potential) customers and auditors - lacunas are rarely raised

Conclusions

- Cloud computing is a neologism
- Off-premise cloud services are generally far better secured compared to on-premises IT at enterprises
- In god* we trust

* No specific religion

WELS CATFISH

Silurus glanis

Maximum Length: Up to 10 feet
Maximum Weight: Up to 330 pounds

Vicious and Voracious: The wels catfish is defined by a long, scaleless body; a broad, flat head; and an extremely wide mouth containing rows of small, sandpaper-like teeth — hundreds of them. It also has two sets of barbels (whisker-like organs) on the upper and lower jaw, which help the fish hunt its prey in the murky waters of large lakes and slow-flowing rivers across Europe. The wels catfish is an adept hunter, first using its pectoral fins to create a disorienting eddy and then taking advantage of its vast, vacuum-like mouth to suck prey in and swallow it whole.

More Wels Catfish

Wels Catfish Photos | Monster Wels Catfish (video) | Wels Catfish Attacks (video) | Wels: Built to Kill (video)

Maneater or Misunderstood? Tales of man-eating wels catfish date back as far as the 15th century, but 2008 saw a spate of attacks in Lake Schlachtensee outside of Berlin. Many believe the attacker to be a 5-foot wels catfish. These fish have been caught in Russia with human remains in their stomachs, but most experts suspect the victims were already drowned before being swallowed. Still, the wels catfish can exhibit aggressive behavior during its mating season, making it plausible that this monster fish could be responsible for attacks against humans that venture into its territory.

Contact

Drs. Mike Chung RE

Manager

KPMG Advisory N.V.

E-mail: chung.mike@kpmg.nl

Mobile: +31 (0)6 1455 9916