Enterprise-wide Cloud Governance Considerations

Ronnie Brunner and Jason Brazile
Netcetera
S06.5

JAZOON'12

netcetera bbv IBM

SET 2012

Most Employees in Your Company Likely…

- Have used a personal Google/Yahoo account for work
- Have installed a personal app on their company desktop/laptop
- Have shared work files using Dropbox/Pastebin/…
- Have used Skype for work
- Have created an Internet user account for company use
- Have been convinced of a product by reading a technical or business “success story”
- Bought project / work related things online with a credit card
- Think it is possible to save money by using “The Cloud”
- Aren’t 100% confident they know their firm’s current strategic goals at least with respect to cloud services

These can be ***good***. These can be ***not so good.***
What decides this?

Goals of This Talk

- Convince that governance should be more about encouraging than punishment
- There's no universal "X is always good" or "Y is always bad"
- The important role of a firm's strategic goals and structural organization
- Governance happens – at least chaotically if not deliberately

Employees ***tend*** to do the ***right thing***
if it is ***easy***, ***logical***, and ***they know what*** it is

What is Governance? Is it Something…

> …that gets in your way when you need something?

> …that is called for after trouble has been discovered/publicized?

> …you've once been rewarded for secretly bypassing?

> …that efficiently keeps common workflows running smoothly?

> …that enables the firm to realize its business goals?

> …that you've gladly helped to update/improve recently?

It can be ***any*** combination of these things

Suggested Definition of Governance

Governance is: ***The system used for exercising authority***

It happens anyway – whether deliberately defined or not

Governance goal: ***Encouraging Desirable Behavior***

Peter D. Weill, Jeanne W. Ross: “IT Governance: How Top Performers Manage IT Decision Rights for Superior Results”, Harvard Business Press, 1. June, 2004

Why Cloud Instead of "Just" IT Governance?

Cloud-first (U.S. govt.) end 2010:

- All CIO's had to define ≥ 3 projects
- By Q4 2011, 1 must be deployed
- By June 2012, all 3 must be

"Beginning in FY 2013, we expect cloud migrations to save agencies about $100 million a year, a[nd] that is for email alone."

Steven VanRoekel, Federal CIO, 2012-06-07

But first of all…

FEDERAL TIMES.com SEARCH

PAY & BENEFITS PERSONNEL AGENCY NEWS TRAVEL IT ACQUISITION FACILITIES, FLEET & ENERGY CONGRES

Start moving to cloud now: Launch 3 projects by June 2012

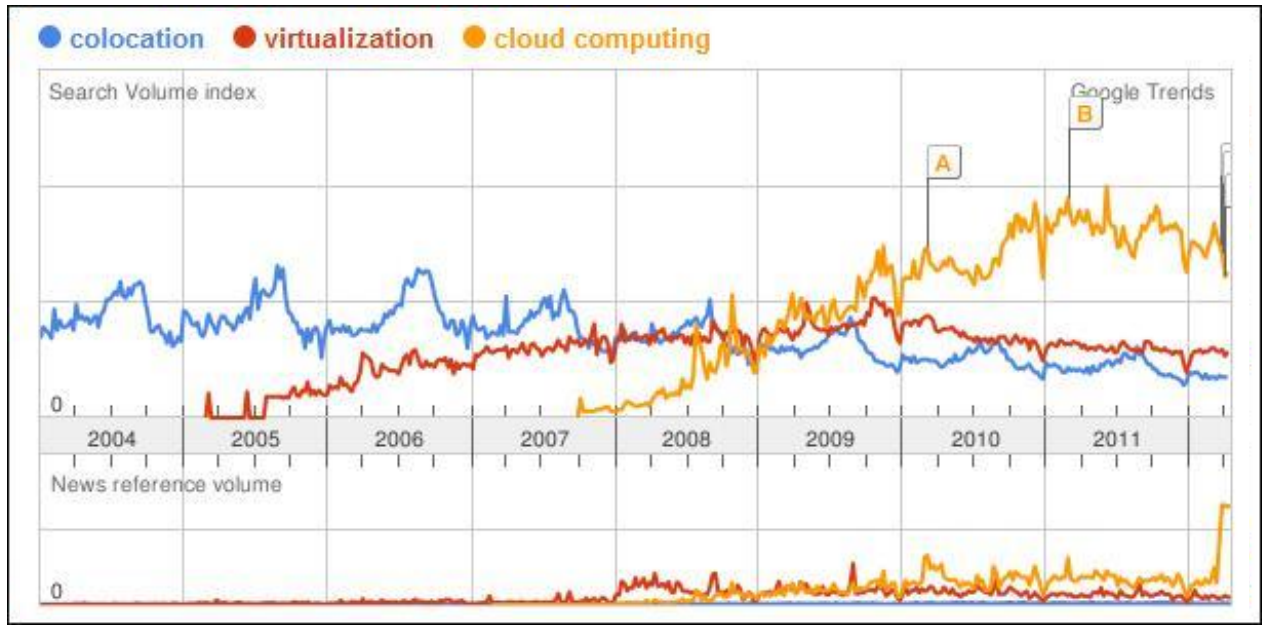
By NICOLE BLAKE JOHNSON | Last Updated: December 13, 2010

Comments (1) Recommend Like 6 Tweet 8 SHARE

Security concerns won't be enough to stop cloud computing.

Chief information officers have three months to identify a minimum of three systems they deem suitable for cloud operations and to create a strategy for moving them. A year from now, at least one of the three systems must be operating in a cloud environment, and by June 2012, all three must be.

Further, "when evaluating options for new IT deployments, OMB will require that agencies default to cloud-based solutions whenever a secure, reliable, cost-effective cloud option exists," according to the Obama administration information technology reform plan, which is posted on the CIO Council website.



Cloud Computing

Cloud Computing supports those who wish to "try first, justify second"

James Staten, Forrester, 2009

Cloud Computing is

> On-demand

> Self-service

> Pay-as-you-go

Cloud Enablers / Cross platform solutions

enStratus, RightScale, cloudkick, SCALR, rPath, newScale, zimory, libcloud, nimsoft

Software as a Service (SaaS)

Microsoft Office 2010 Web Applications, Google Apps, slideshare, Basecamp, ZOHO Work. Online, webex, Taleo, NETSUITE, GoToMeeting

Platform as a Service (PaaS)

Google App Engine, force.com platform as a service, hadoop, intuit, Windows Azure, heroku, appscale, Engine Yard

Infrastructure as a Service (IaaS)

amazon web services, bluelock, rackspace, GoGrid, terremark, linode.com, CloudSigma, Eucalyptus

Traditional Risk Management View of Governance

Risk	Examples	Result
Re-invention of wheel	Portal proliferation; User account mess	Poor services, inefficiency
Individual “contracts” via credit card	Critical service is down because key person‘s individual credit card expires	Service failure, data mess (where’s what?)
Single actor can chose wrong direction quickly	Introduction of a proprietary SaaS solution that (only) provides a quick fix	Unmanaged service portfolio, not reaching strategic goals
Costs can’t be tracked well	Monthly bills unpredictable due to irregular demand. Lots of hard to track small transactions with many providers	Financial exposure and uncertainty
Costs slowly increase	Nobody cleans up hard disks or gets rid of unused virtual machines	More expensive over time, unclear what‘s still needed
Data gets leaked	Data protection violation, leak of industry partner’s (or member state‘s) secrets	Financial liability, loss of trust
Data loss	NASA‘s moon landing tapes, hacker data vandalism, Provider default	Image/brand damage

Traditional Governance Measures I

Provider	Measure
	• User manages permissions to a fine grained level • Platform allows delegated authentication - what is authenticating users? • Organization controls where users can log in from • Multiple methods for download/backup via API
	• Manage individual S3 and EC2 account rights • Get users to send checksums for ensuring data integrity • Firewalls must be configured securely • New segregation of duties issues between management of cloud resources and management of instances • Encrypted file systems • Local backup of critical data and EBS/AMI backup to S3 • EBS snapshots which can be moved across zones • Versioning

Source: Tim Weir, “Cloud computing: The Role of Internal Audit”, Ernst and Young, Oct 2009

Traditional Governance Measures II

Provider	Measure
	• Ensure own compliance and privacy policies • Links to internal authentication system • Data Backups • Replication to internal systems
	• Distributed authentication, provisioning/de-provisioning • Administrative control panel rights • Restrict documents/file sharing to just your domain • Backup your own data

Source: Tim Weir, “Cloud computing: The Role of Internal Audit”, Ernst and Young, Oct 2009

Proposal For Approaching Cloud Governance

The Big Picture

> Which decisions have to be made and who should best decide them

Communication

> All (management) knows the principles – everybody can trace measures back to corporate strategy

Corporate Strategy

> Governance must be tightly linked with corporate strategy

Desirable Behavior

> And when possible, prefer to encourage desirable behavior rather than punish undesirable behavior

Big Picture – What & Who (Weill/Ross)

The Basics:

- **What decisions to make?**
- **Who should make them?**

Who (decides):

- "**Monarchy**" (CEO, CFO)
- "**IT Monarchy**" ("IT guys")
- "**Feudal**" (BU as individuals)
- "**Federal**" (BUs as a group)
- "**IT Duopoly**" (IT + …)
- "**Anarchy**" (each individual)

What (Decisions):

- **Principles** (Op model, desirable behaviors)
- **Architecture** (What data/ processes are standard?)
- **Infrastructure** (What must be in-house?)
- **Business App needs** (Identification, assessment, ownership)
- **Investment/Prioritization** (What's ASAP? BU vs Org**)**

Source: Peter D. Weill, Jeanne W. Ross: *IT Governance*, Harvard Business School Press, 2004

Big Picture – How (Observed results) (Ross/Weill)

Comparing IT Governance Arrangements of Organizations

	IT Principles		IT Architecture		IT Infrastructure		Business App Needs		IT Investment	
	Input	Decision	Input	Decision	Input	Decision	Input	Decision	Input	Decision
Business Monarchy	0	27	0	6	0	7	1	12	1	30
IT Monarchy	1	18	20	73	10	59	0	8	0	9
Feudal	0	3	0	0	1	2	1	18	0	3
Federal	83	14	46	4	59	6	81	30	93	27
Duopoly	15	36	34	15	30	23	17	27	6	30
Anarchy	0	0	0	1	0	1	0	3	0	1
No data / Don't know	1	2	0	1	0	2	0	2	0	0

Most common input for all enterprises

Each cell is the percentages of the 256 enterprises studied in 23 countries

Source: Peter D. Weill, Jeanne W. Ross: *IT Governance*, Harvard Business School Press, 2004

Big Picture – How (Observed results) (Ross/Weill)

How Top Financial Performers Govern

	IT Principles	IT Architecture	IT Infrastructure	Business App Needs	IT Investment
	Decision	Decision	Decision	Decision	Decision
Business Monarchy	Profit Growth	Profit	Profit	Profit	Profit Growth
IT Monarchy			Profit		
Feudal					Growth
Federal				Profit	
Duopoly	ROA	ROA	ROA	ROA	ROA
Anarchy					

Most common pattern for all firms

Profit, ROA, Growth = Firms with significantly higher or increasing average three-year industry adjusted profits, ROA or growth

Source: Peter D. Weill, Jeanne W. Ross: *IT Governance*, Harvard Business School Press, 2004

From Objective to Desirable Behavior

Objectives	Desirable Behavior	Potential Mechanism
Holistic view of business, incl. IT	Seamless management incorporating IT	Executive and senior management committee
Identify strategic technologies and standards - enforcement	Business-driven IT decision making	Architecture committee
Take process view using IT (and other assets) effectively	End-to-end process management	Process teams with IT membership
Consider IT as another business investment	Prudent IT investing - different approaches for different investment types	Capital investment approval and budgets
Specify and measure IT service	Professional supply and demand	Service Level Agreements
Recoup IT costs from business	Responsible use of IT	Charge-back
Measure IT investments and contribution to business value often using balanced scorecard	Makes transparent goals, benefits and costs	Formal tracking of business value of IT

Source: *Effective but challenging governance mechanisms,* MIT Sloan School CISR

An Encouraging Rather Than Punitive Attitude

Example adjustments:

- L “Can’t go live w/o backup”
- J Provide access to easy-to-use backup services

- L “Don’t sign-up for video chat XYZ”
- J Provide corporate accounts for a variety of easy-to-use collaboration tools

- L “Don’t use AWS EC2” (e.g. regulatory compliance)
- J Offer properly located Eucalyptus-based alternative

Additional Encouraging Examples (DR/BC)

- Offer standard procedures for synchronizing data remotely. These procedures encrypt data using the strongest encryption possible
- Offer virtual machine images with the same operating system, tools, core applications, and libraries as production systems
- (Optionally) provide tools (not just procedures) to automate/configure processes
- Provide escrow for all key authentication data
- Offer to test restoring infrastructure remotely based on current data

Measures Must Be Traceable Back to Goals

Example traceable goals:

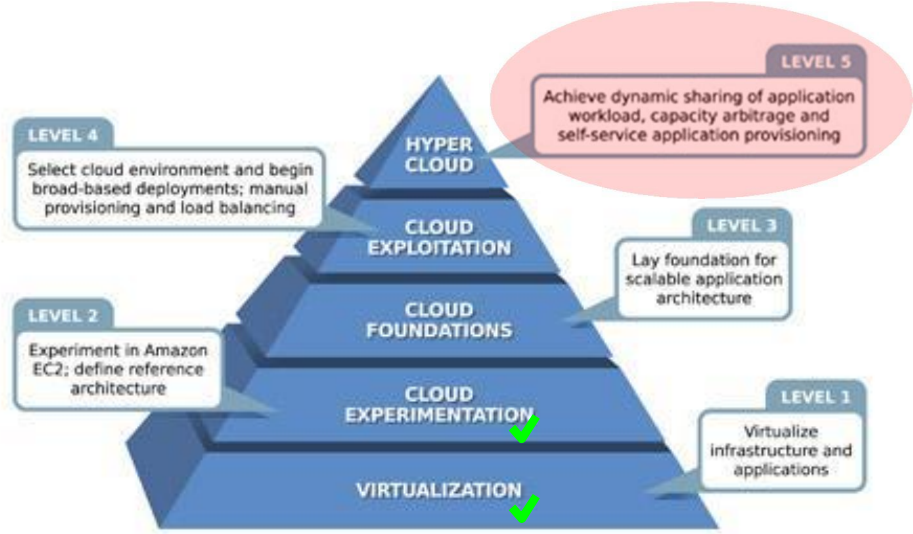
- Maximize **profit**
- Maximize **ROA**
- Maximize **growth**
- **Standardize** capabilities
- **Focus** on core competencies
- …

Communication tasks:

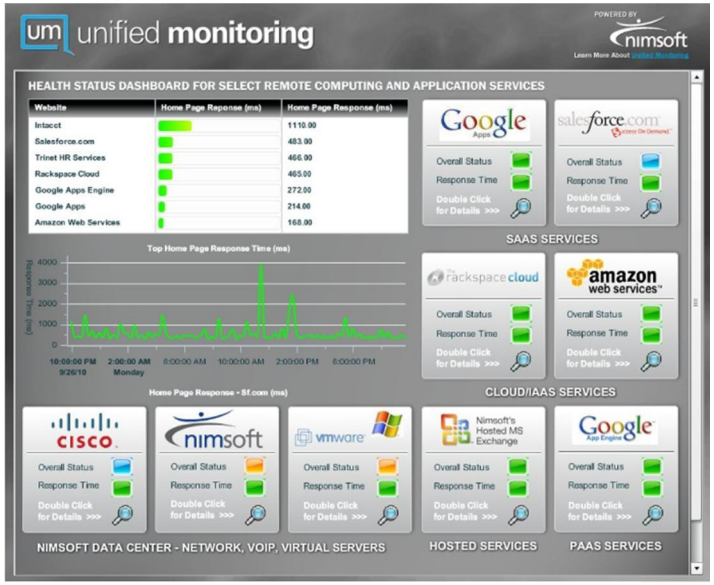
- Trace back to goals
- Publicize traceability
- Publicize exception handling process
- Publicize exceptions
- Executive-driven

Goal: Max. Profit à e.g. Consolidate, Cost-control

- Centralized "dashboard"
- Your 1st movers are actively sharing best practices experience
- Know the "true cost" of internal IT
- Governance measures known and respected by all



Source: Jake Sorofman (rPath), "How to Achieve the Strategic Value of Cloud While Delivering Real ROI", 3 March 2009

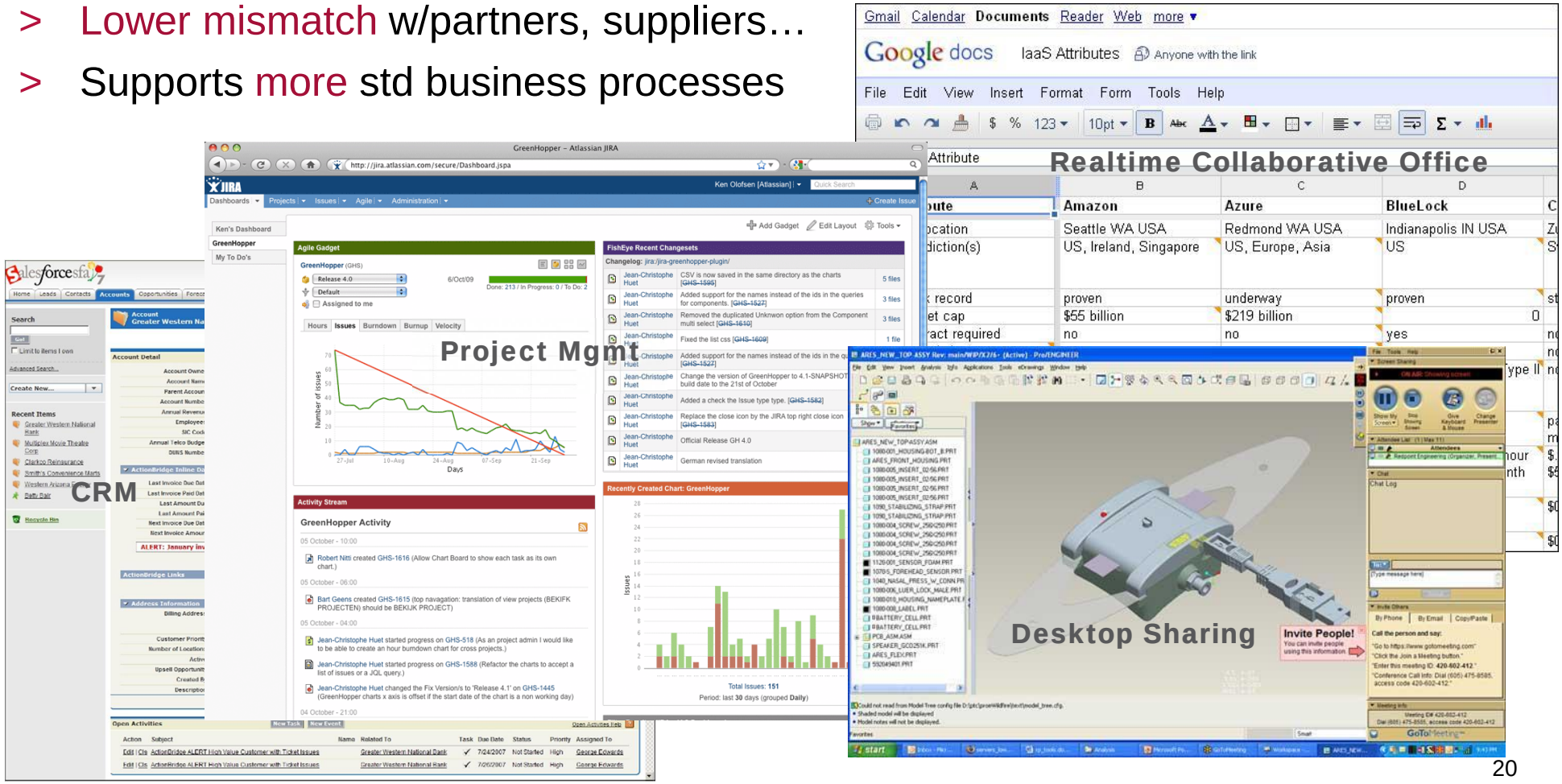


From Virtualization to "Hypercloud":

- Dynamic sharing of app workload
- Capacity arbitrage
- Self-service application provisioning

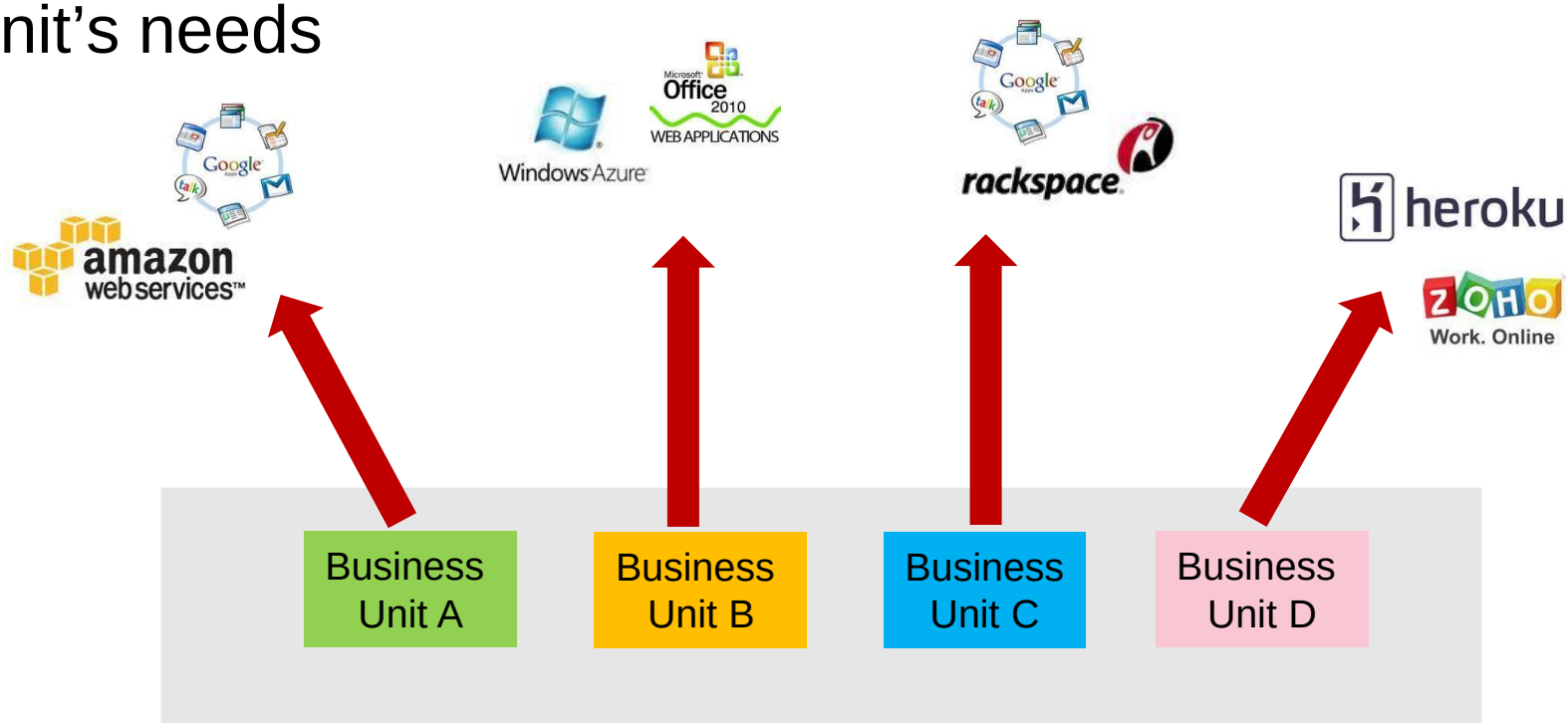
Goal: Standardize/Raise Capabilities à SaaS

- Market leading browser-based offerings (work anywhere)
- Higher "collaborativity" e.g. simultaneous editing
- Lower mismatch w/partners, suppliers…
- Supports more std business processes



Goal: Maximize Growth à De-centralize

- > Empower business units to drive IT investment
- > Embed IT professionals in business units to focus on unit's needs
- > Sacrifice integration for functionality and speed
- > Less substantial enterprise-wide infrastructure



Source: Peter D. Weill, Jeanne W. Ross: *IT Governance*, Harvard Business School Press, 2004

Takeways of This Talk

Governance goals

- Choosing the right governance structure mainly depends on the strategic goals
- Encourage desirable behavior is likely to be more successful than punish
- Make goals and measures transparent (and traceable) to support encouragement

No universal "good/bad"

- The same can be an excellent or very bad decision, it really depends on the strategic goals
- To be able to decide in any specific case: Are standard processes traced to executive strategy and are exceptions covered by a known exception process?

Ronnie Brunner
ronnie.brunner@netcetera.com
+41-44-247 79 79

Netcetera
Zypressenstrasse 71
CH-8040 Zürich
+41-44-247 70 70

Jason Brazile
jason.brazile@netcetera.com
+41-44-247 79 25