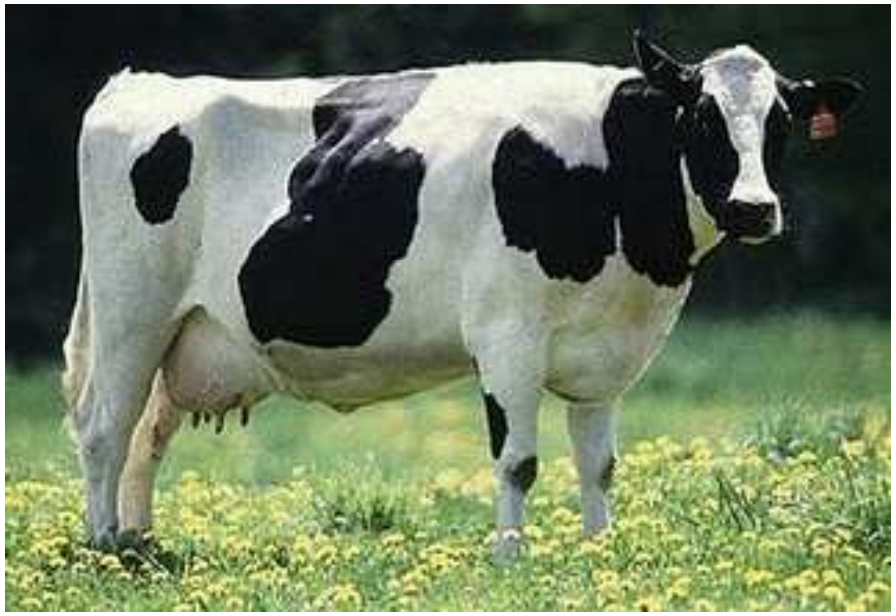
ISACA®
Trust in, and value from, information systems
San Francisco Chapter

Governance and Control in the Cloud

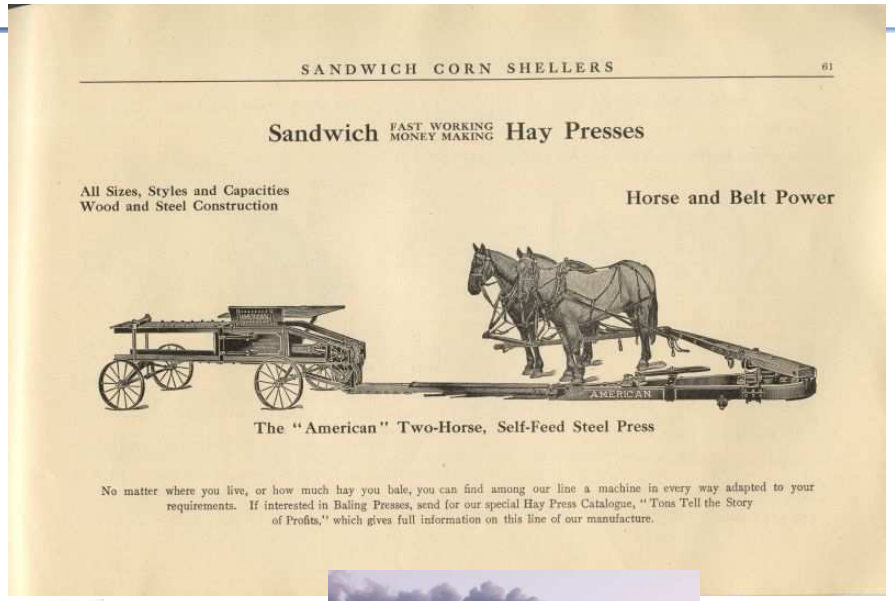
Infrastructure as a Service

ISACA®
Trust in, and value from, information systems
San Francisco Chapter

Cows



The Triumph of the Utility



SANDWICH CORN SHELLERS 61

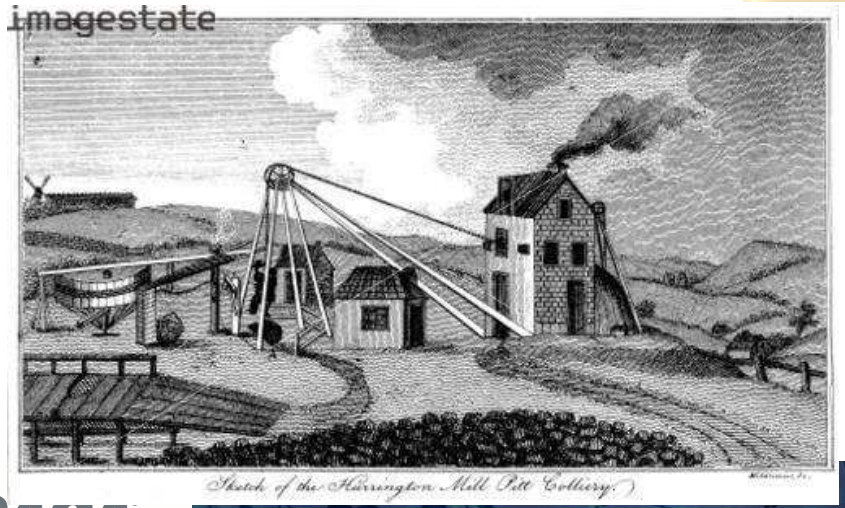
Sandwich FAST WORKING MONEY MAKING Hay Presses

All Sizes, Styles and Capacities
Wood and Steel Construction

Horse and Belt Power

The "American" Two-Horse, Self-Feed Steel Press

No matter where you live, or how much hay you bale, you can find among our line a machine in every way adapted to your requirements. If interested in Baling Presses, send for our special Hay Press Catalogue, "Tons Tell the Story of Profits," which gives full information on this line of our manufacture.



ISACA
Trust in, and value from, information systems
San Francisco Chapter

Back to Business

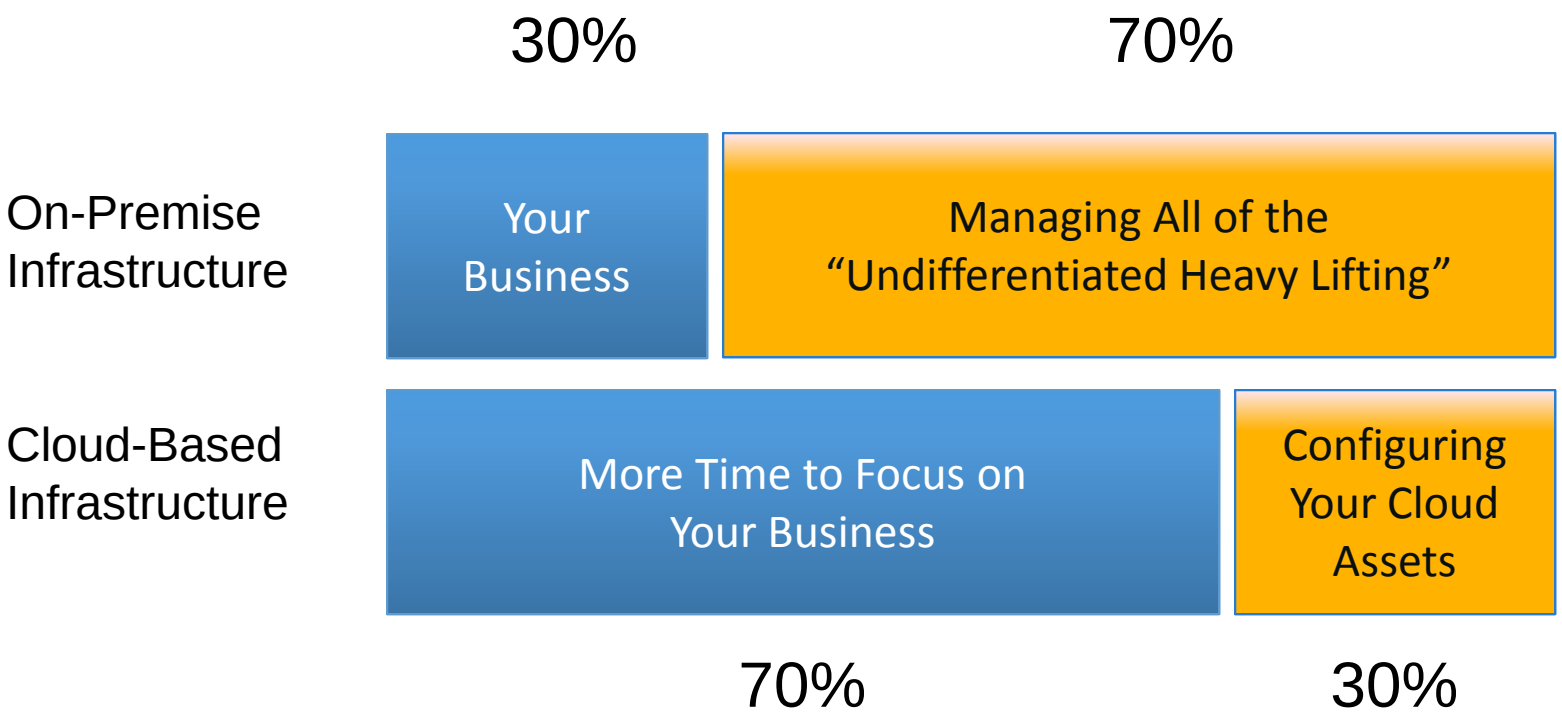
Our Discussion

- How we'll talk about Governance and Controls today
- Not an IT-assurance methodology discussion; an evaluation of controls based on IaaS-focused cloud services
- The next presentation will cover PaaS and SaaS controls

IaaS/Customer Shared Responsibilities

- Moving IT infrastructure to an IaaS creates a model of shared responsibility
- This shared model can help relieve customer's operational burden as the IaaS operates, manages and controls IT system components
- This customer/IaaS shared responsibility model also extends to IT controls

What to spend time on?



Evaluating and Integrating IaaS Controls

- Achieving information security compliance can be done:
  - In a detailed way (looking at individual controls)
  - In a general way (looking at an entire control environment, including subjective factors)
- When working with IaaS providers, you also have options:
  - Require service provider to publish specific controls, with pass/fail audits
  - Require service providers to adhere to a broad standard, and rely on a process or security certification

IaaS Control Governance - Summary

- Four categories of controls:
  - **General control considerations** – these are general considerations and are primarily mitigated by cloud provider selection
  - **Technology controls** – these are features of the service offered that allows the customer to implement and validate their own controls
  - **Report/certification controls** – IaaS service providers can identify specific controls, either in a SOC1/SOC2 report (specific identification) or an industry certification to a known standard (general reliance)
  - **SLA controls** – These controls can be implemented in the Service Level Agreement (SLA) and/or in the Enterprise Agreement (sales contract)

IaaS Control Governance
General Control Considerations

- Who owns which controls?
- Is compliance with industry-specific objectives (HIPAA, PCI, etc.) possible?
- Capability to Scale. Does the provider allow customers to scale beyond the original agreement?
- Provider Sustainability. Does the service provider company have long term sustainability potential?

IaaS Control Governance Technology Controls

- Network, Server, and Application Security - Does the provider follow good security practices for these areas?
- Client-side Protection - Does the cloud provider allow customers to secure and manage access from clients, such as PC and mobile devices?
- Data Location - Where does customer data reside?
- Multi-tenancy security - Is customer segregation implemented securely?
- Data isolation - Does the cloud provider adequately isolate customer data?
- Data Erase Practices - Can new customers access “deleted” data from another customer?
- Hypervisor vulnerabilities - Has the cloud provider addressed known hypervisor vulnerabilities?
- Encryption - Do the provided services support encryption?
- Identity and Access Management - Does the service include IAM capabilities?
- Data portability - Can the data stored with a service provider be exported upon customer request?
- Customer business continuity - Does the service provider allow customers to implement a business continuity plan?
- Backups - Does the service provide backups to tapes/optical media?

IaaS Control Governance Report/Certification Controls

- Vulnerability management - Are systems patched appropriately?
- Employee User Access - Does the provider effectively control internal and vendor user access?
- Logical Security - Does the provider follow good logical security practices?
- Physical Security - Does the provider follow good physical security practices?
- Environmental Safeguards - Does the provider ensure environmental safeguards are in place?
- Data Integrity, Availability and Redundancy - How does the provider ensure data integrity, availability, and redundancy?
- Right to Audit - Can customers perform audits on CSP's premise?
- Third Party Access - Are third parties allowed access to the cloud provider data centers?
- Privileged Actions - Are privileged actions monitored and controlled?
- Insider Access - Does the cloud provider address the threat of inappropriate insider access to customer data and applications?
- Physical and Environmental Controls - Are these controls operated by the cloud provider specified?
- Service Provider Business Continuity - Does the service provider operate a business continuity program?

IaaS Control Governance
SLA Controls

- Data Ownership - What are the cloud provider's rights over customer data?
- Price Increases - Will the service provider raise prices unexpectedly?
- Composite Services - Does the cloud provider layer its service with other providers' cloud services?
- Scheduled Maintenance Outages - Does the provider specify when systems will be brought down for maintenance?
- Service Availability - Does the provider commit to a high level of availability?
- Data Durability - Does the service specify data durability?
- Distributed Denial Of Service (DDoS) attacks - How does the provider protect their service against DDoS attacks?
- E-Discovery Support - Does the cloud provider meet the customer's needs to meet electronic discovery procedures and requirements?

IaaS Questionnaires - Out of Date Questions

Questions sometimes asked that will no longer be applicable using IaaS providers:

- Does the provider regularly back up all data to tape and store it offsite?
- Will the provider implement feature X or product Y in their data centers?
- How many people have access to the provider's facilities?
- Is the customer permitted to approve any maintenance, updates, or changes?

IaaS Opportunity – SOX

- SOX - key controls and obtaining “reasonable assurance” over the controls for financial reporting process
- Processing critical financial data in the cloud? If not, SOX generally does not apply directly
- If ITGC is key, a SAS70/SSAE 16 should suffice, as long as the report has coverage on needed ITGC controls
- If specific controls are key, then these controls will likely need to be called out on the SSAE16 report (more applicable to SaaS than IaaS)
- Substantive procedures also are possible as an alternative for some controls
- In the real world, most of the SOX controls will be controlled by the customer, as they manage and secure the OS, databases, transactions, etc.

IaaS Opportunity – PCI

- PCI compliance for an IaaS means that they manage Requirement 9, and you manage everything else (with some possible exceptions depending on the service)
- A “shared hosting provider” is not a service provider type defined by PCI; IaaS providers must be classified under the “other” category
- If your IaaS is a validated service provider, your QSA can rely on the CSP’s QSA work
- You need to define what is your responsibility vs. the CSP’s responsibility; the CSP will prepare a document outlining responsibilities by PCI DSS requirement for your QSA

ISACA®
Trust in, and value from, information systems
San Francisco Chapter

Questions?

Bio
Chad Woolf has spent the last 13 years working with cloud technologies, focused on the development and implementation of internet-delivered software, platforms, and infrastructure. He has specialized in managing the complexities of security, continuity, risk and compliance in a distributed IT environments and has advised large technology companies such as Microsoft, Computer Associates, Expedia, and Yahoo! Chad is a CPA and CISSP and is currently the Risk and Compliance Leader for Amazon Web Services.

You can connect with Chad in LinkedIn.