



W. David Snead, P.C.

The Second International Conference on Evolving Internet

INTERNET 2010

Understanding, preparing for and developing compliance plans for regulatory issues governing cloud computing

W. David Snead
Attorney + Counselor



Roadmap

- Cloud definition workshop
- Understanding a cloud transaction
- Negotiating a cloud contract
- Understanding a compliance plan
- Evaluating risk in a cloud transaction
- Creating a compliance plan



Creating a cloud compliance plan

Business risks

Operational risks

Legal risks

Regulatory risks

Case Study

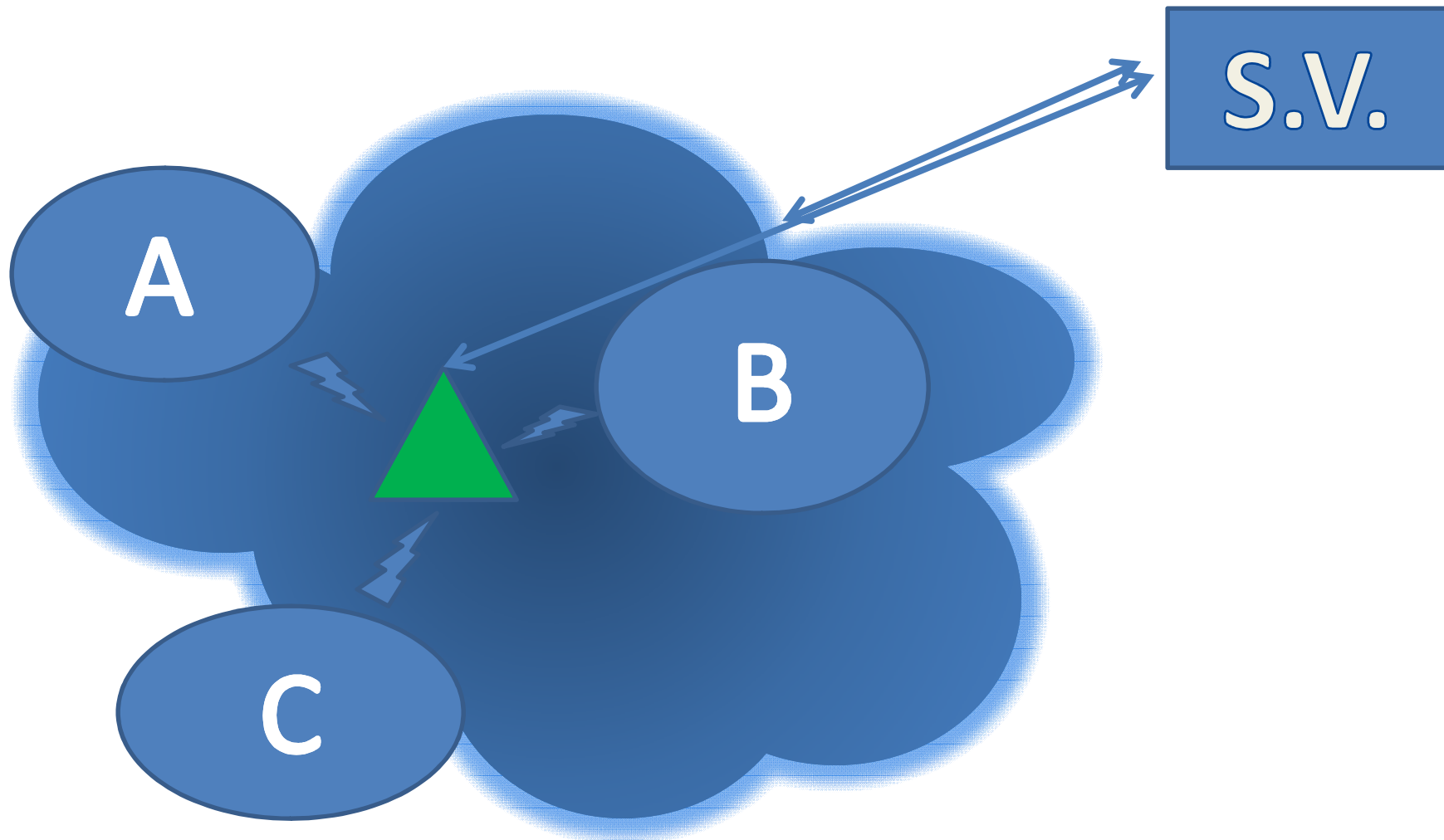


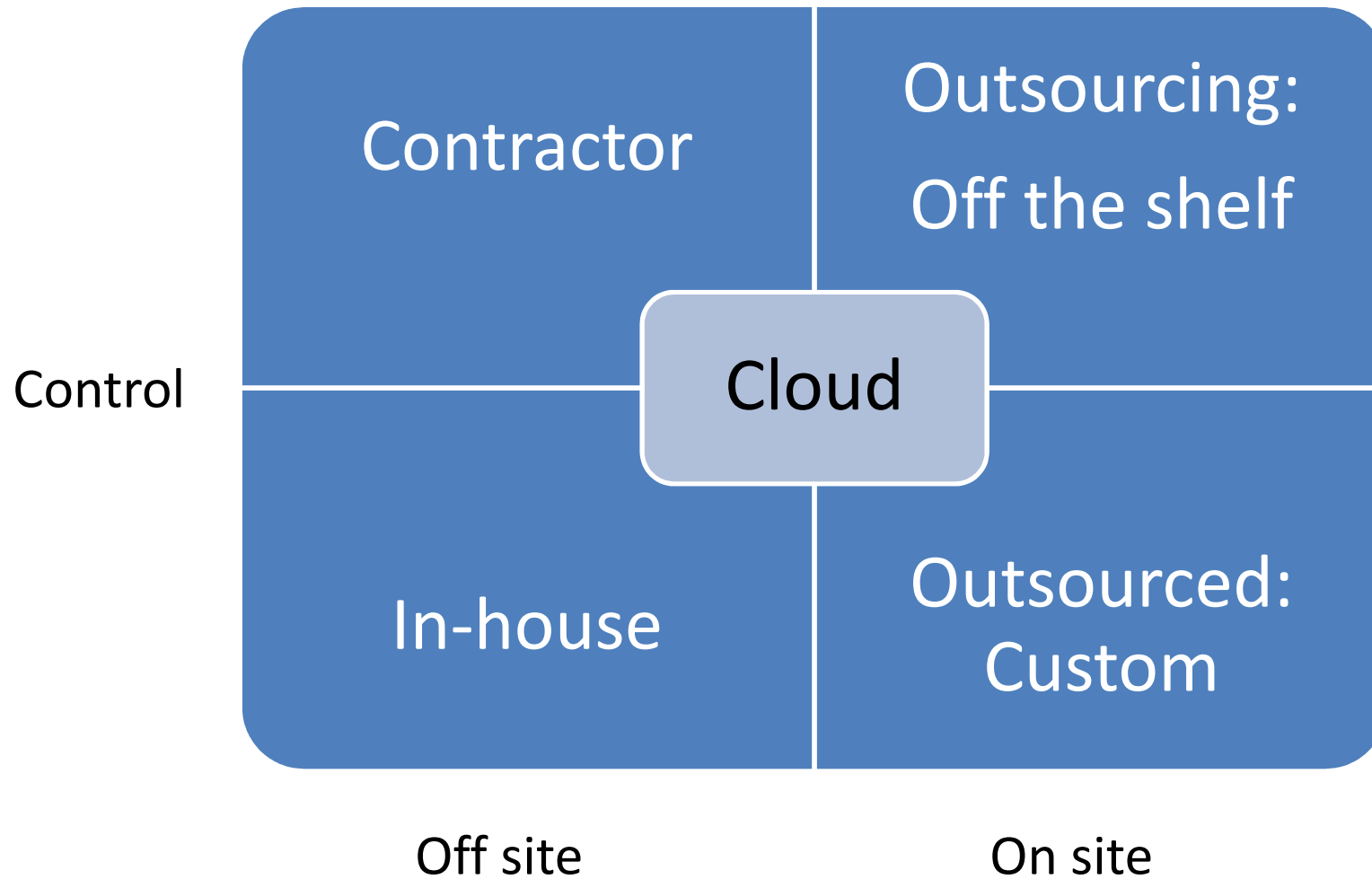
W. David Snead, P.C.

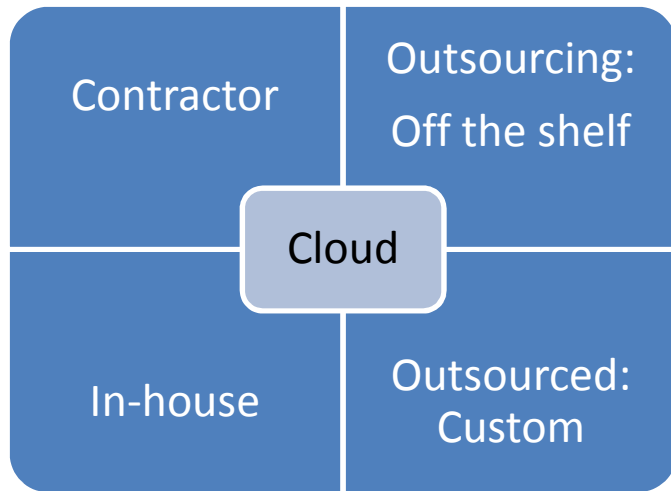




- Email
- Office Applications
- Payroll
- Backbone







- Email
- Office Applications
- Payroll
- Backbone



Platform

Software

Infrastructure



Platform as a Service - PaaS

- Infrastructure
 - computing platform
 - “solution stack”
 - uses distributed infrastructure components
- Supports cloud applications
 - allows deployment of customer applications
 - vendor assumes management of underlying hardware and basic software



Software as as a Service - SaaS

- Software as selling point
 - COTS software
 - Centralized patch management
 - data preservation / backup
- Distributed delivery
 - Web access
 - one to many distribution



Cloud definitions

Infrastructure as as a Service - IaaS

- Cloud is the platform
- Virtual data center
 - No capital outlay
 - A-la-carte hardware use
- Billed as a utility
 - Pricing feature or use based



Cloud definition workshop

- Email
- Office Applications
- Payroll
- Backbone
- Servers
- Software
- Data Center Space
- Network Equipment
- Development Resources
- Feature Updating
- PaaS
- SaaS
- IaaS

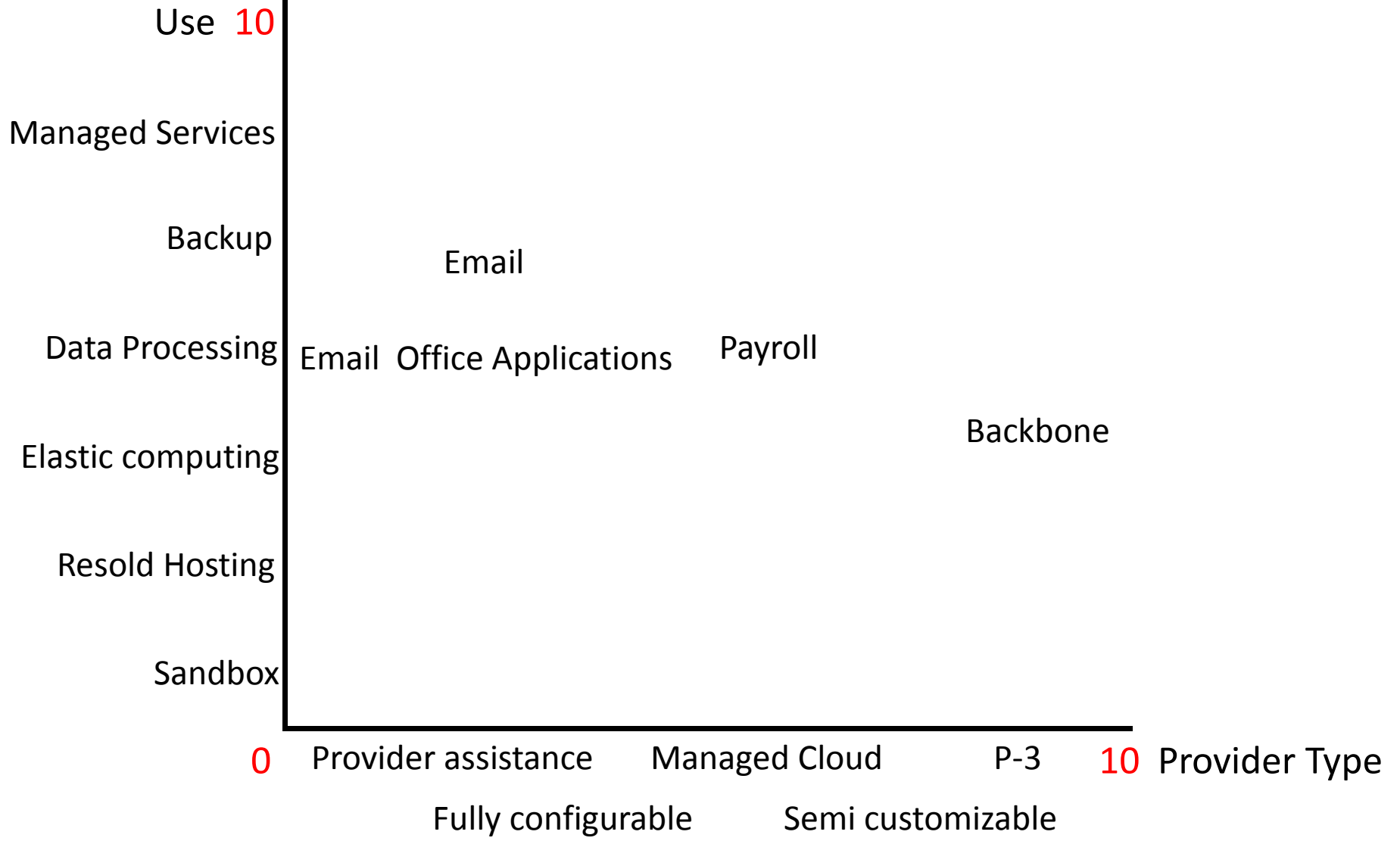


Creating a cloud compliance plan

- Email
- Office Applications
- Payroll
- Backbone
- Servers
- Software
- Data Center Space
- Network Equipment
- Development Resources
- Feature Updating



Understanding Risk





In what country is the provider located?



Where is the provider's infrastructure?



Will other providers be used?



Where will the data be physically located?



Should jurisdiction be split?



How will data be collected, processed, transferred?



What will happen to the data on termination?



Negotiating contracts



Security



Data transfer



Disposition of data on termination



Change of control



Access to data



Security

- Define “breach”
- Determine when a breach happens
- Assume there will be data breach laws
- Review any laws that may currently exist
- Understand who will be responsible for security
- Create enforceable contract terms
- Remember post termination issues
- Understand that you may not be made whole



Data Transfer

- How is the cloud structured?
- Understand concepts like: controller, processor, transfer and aggregation.
- Limit uses
- Require flow down and flow up contract terms
- Evaluate whether “Safe Harbor” is appropriate
- Create methods to address data leakage



Disposition of data upon termination

- Review data retention laws
- Specify terms for deletion / transfer
- Set out obligations for security post termination



Change of control

- Specify who owns the data
- Set out access terms
- Define what information may be sold



Access to data

- Understand how cloud is outsourced / subcontracted
- Review your obligations to provide access to police
- Review your provider's obligations to provide access
- Research your laws about third party police access
- Set out notification and consent provisions



Privacy Regulations



Jurisdiction



Data Subjects, Controllers and Processors:

Data Subjects: originators of the data

Controllers: collectors of the data

Processors: manipulators of the data



Negotiating contracts



Jurisdiction over the contract



Whose law governs

Where the dispute is heard

Change in judicial presumptions



Jurisdiction over the data



Data protection directive

Export control laws



Negotiating contracts

- Email
 - Office Applications
 - Payroll
 - Backbone
 - Servers
 - Software
 - Data Center Space
 - Network Equipment
 - Development Resources
 - Feature Updating
 - PaaS
 - SaaS
 - IaaS
-
- Notification of breaches in security
 - Data transfer
 - Disposition of data on termination
 - Change of control
 - Access to data
 - Jurisdiction
 - Privacy






Business risks

Operational risks

Legal risks

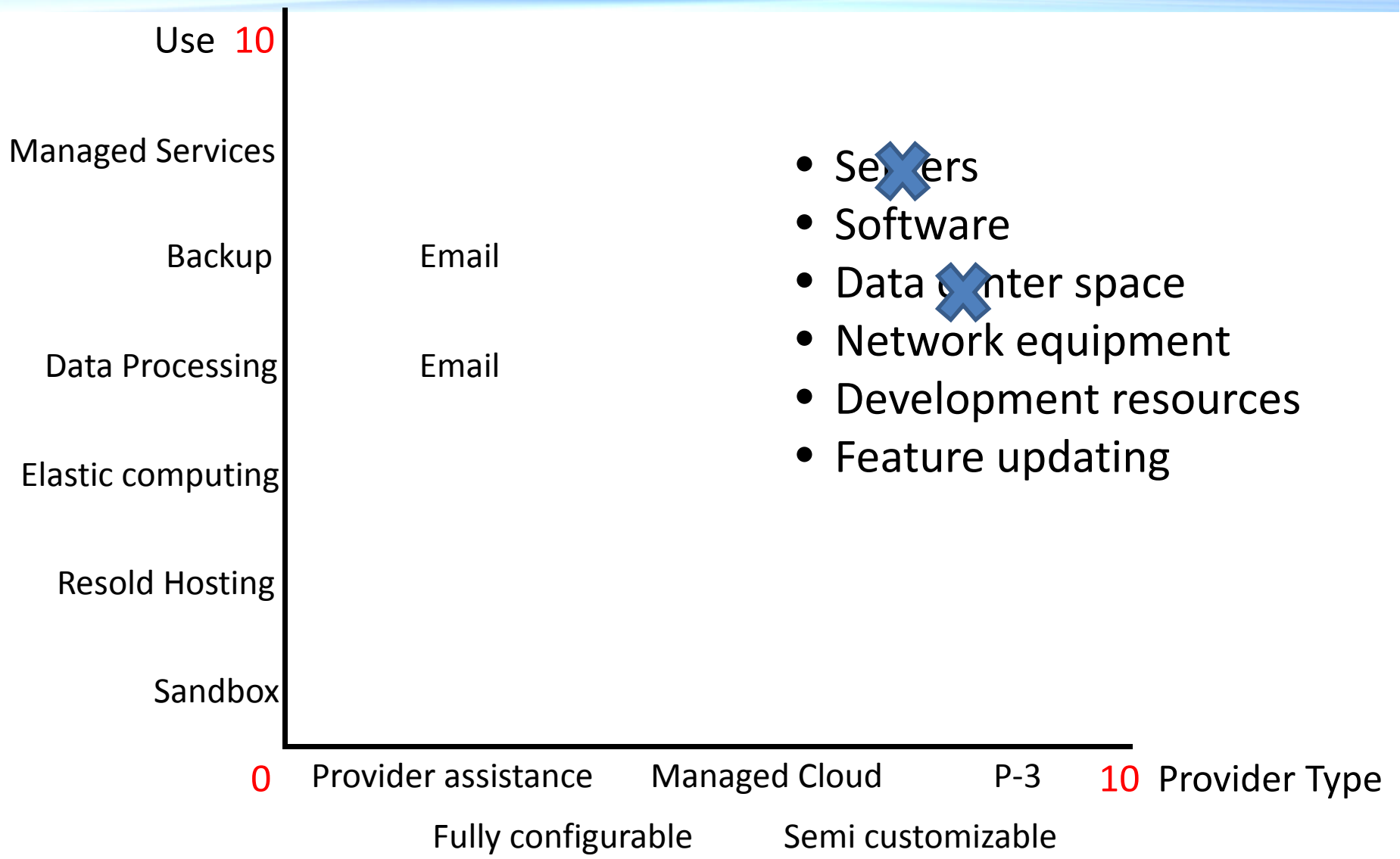
Regulatory risks

1. Identify gaps 
2. Craft policy
3. Build infrastructure 
4. Training and communication 



Craft policy – email outsourcing

W. David Snead, P.C.





Craft policy – email outsourcing



Security



Data transfer



Disposition of data on termination



Change of control



Access to data



Contract provisions

- Breach: malicious.
- Breach: parties, third parties, subcontractors, vendors
- Breach laws: Germany, U.K., possibly U.S.
- Responsibility for security: parties, third parties, subcontractors vendors
- Post termination issues: data belongs to sol vidro, breach liability extends post termination.
- Security policy: made part of contract. Revisions subject to sol vidro review. Flow down to subcontractors and vendors



Contract provisions

All data, including, but not limited to, metadata, transactional information, and IP addresses is the sole and exclusive property of Sol Vidro, its affiliates, subsidiaries and assigns. Vendor warrants and represents that this claim of ownership shall be included in all contracts and agreements with third parties who have access to this data. The provisions of this paragraph shall survive termination or expiration of this Agreement. Any limitations of liability set out in this Agreement shall not apply to a breach of Vendor's obligations set out in this paragraph.



Contract provisions

Vendor has provided Sol Vidro with a copy of its current security policy (Policy) as it applies to the services to be performed by Vendor pursuant to this Agreement. Vendor represents and warrants that this security policy represents best of breed security procedures in its industry. Vendor shall give Sol Vidro no less than sixty days prior written notices of any changes in the Policy that impact the services provided to Sol Vidro. Should Sol Vidro determine that these changes materially impact the security of the services, Sol Vidro shall have the right to terminate this Agreement. In such a case, Vendor shall provide reasonable assistance to Sol Vidro to transition its services to another provider.



Policy provisions

- Breach definition matches contract
- Internal notifications
- External notifications
- Law enforcement activity
- Investigation
- Secure / mitigate personally identifiable information



Contract provisions



Data transfer

- Are you a controller? Processor? Transferor? Aggregator?



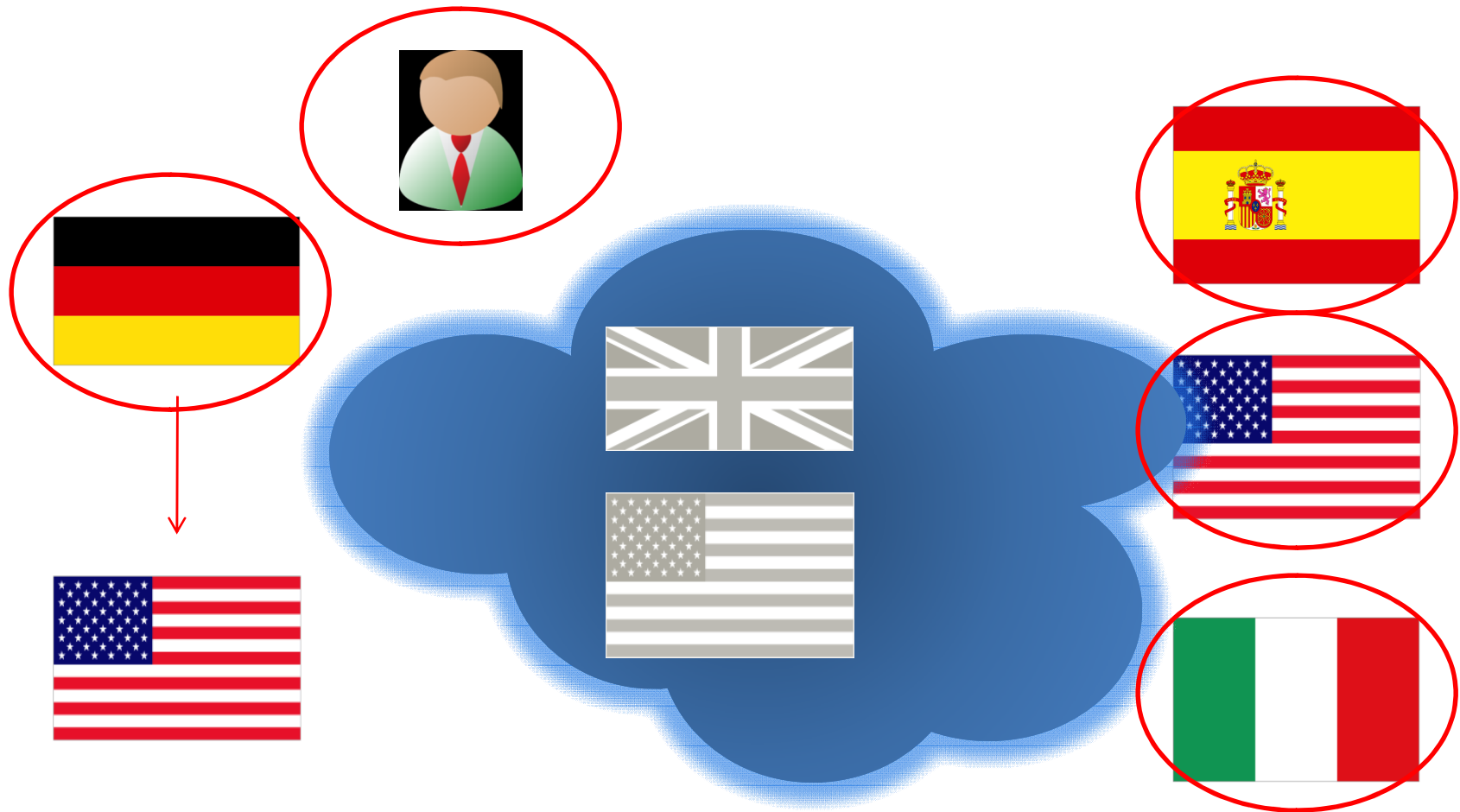


Craft policy – email outsourcing

- Are you a controller? Processor? Transferor? Aggregator?
- Determine who owns or originates the data.
- Review the level of interaction with the data
- Look at position in the transaction



- Are you a **controller**? Processor? Transferor? Aggregator?





Contract provisions

- Ensure compliance with member state law
- Require compliance with safe harbor
- Include flow down provision in contract
- Restrict processing of data in contract

Vendor represents and warrants that all affiliates, subsidiaries, vendors and partners having access to the data are either within the U.S. Department of Commerce's Safe Harbor program, or are located entirely within an E.U. member state.



Contract provisions

- Restrict processing of data in contract

Vendor shall have no access to the data. Further, Vendor shall limit its manipulation, processing and interaction with the data to those actions strictly necessary for Vendor to carry out the obligations set out in this Agreement.



Policy provisions

- Create methods to address data leakage.
- Require confidentiality agreements
- Secure the data, not the perimeter
- Enforce your policy around the data, not the enterprise or state boundaries.
- Insist on standardized SLAs



Contract and policy provisions



Disposition of data on termination

- Review data retention laws
- Employment
- Securities
- Government contracting
- Transactional information (IP addresses / email records)
- Industry specific



Contract provisions

- Specify terms for deletion / transfer
- Set out obligations for security post termination

Upon termination or expiration of this Agreement, Vendor shall delete all data and provide Sol Vidro with written confirmation of this deletion. Vendor shall also instruct any entities who have had access to the data to also delete it and provide Vendor with written certification of this deletion. The security obligations set out in this Agreement relating to the data shall survive termination or expiration of this Agreement until such time as the data is completely deleted by Vendor and/or Vendor's suppliers. Vendor shall require this provision, or one similarly protective of Sol Vidro's rights in all its contracts with suppliers or other vendors who provide aspects of the Services.



Policy provisions

- Document data to which you have access
- Limit the number of employees who have access to data
- Create and implement access policies
- Create and implement deletion policies
- Flow down contract terms to vendors
- Do not assume security ends upon termination



Contract provisions

Sol Vidro shall retain all right, title and interest in the data. Vendor shall have no rights in the data, other than as necessary to fulfill Vendor's obligations set out in this Agreement. Under no circumstances shall Vendor sell and/or commercialize any of the data or information related to the data. Vendor shall require this provision, or one similarly protective of Sol Vidro's rights in all its contracts with suppliers or other vendors who provide aspects of the Services.



Policy provisions

- Document data to which you have access
- Segregate by customer and/or use
- Create and implement access policies
- Maintain access logs
- Flow down contract terms to vendors



Contract and policy provisions

- Understand and define law enforcement access
- Don't assume your country's laws will prevail
- Don't let stereotypes interfere with a legal analysis
- Try to create definition



Contract provisions

Vendor shall provide Sol Vidro with no less than ten days prior written notice of any governmental request for access to the data. For the purposes of this paragraph only, the term “governmental” includes any law enforcement or similar entity. Should Vendor be prohibited by law from providing this notice, Vendor shall strictly limit any disclosure of the data to that which is required by the law and the written document upon which disclosure is based. Under no circumstances shall Vendor provide access without a written request of disclosure which cites the law requiring such disclosure. Vendor shall require this provision, or one similarly protective of Sol Vidro’s rights in all its contracts with suppliers or other vendors who provide aspects of the Services.



Craft policy – email outsourcing



Policy provisions

- Require written notice
- Don't assume validity
- Create and implement access policies
- Centralize decisionmaking
- Include legal advisor



Toolkit



Determine how services will be used



Evaluate cloud structure



Understand data collection, processing and transfer



Security breach notification



High risk regulatory areas



Disposition of data on termination



W. David Snead, P.C.

The Second International Conference on Evolving Internet

INTERNET 2010

W. David Snead

Attorney + Counselor

david.snead@dsnead.com

www.dsnead.com