May 4, 2018

Cloud Clarity:

Bringing Sunshine to Cloud Vendor Relationships

John J. Jablonski, Esq.
716.313.2082 | jjablonski@gerberciano.com

John J. Jablonski

Gerber Ciano Kelly Brady LLP

- **Data Security & Privacy** – policies, procedures, assessments, legal advice, opinions, IT and privacy governance, incident response
- **Audits** – Vendors and Audit Response Counsel
- **Technology Contracts** – cloud, managed services, software, DR, website, terms, conditions, security and privacy, negotiations and vendor management
- **Information Governance** – RIM, RRS, policies, procedures, legal holds (scope and process), audits and strategy

Managing Partner

Chair – Cyber, Technology and Social Media

jjablonski@gerberciano.com

P: 716.313.2082

Twitter: @InfoGovLaw

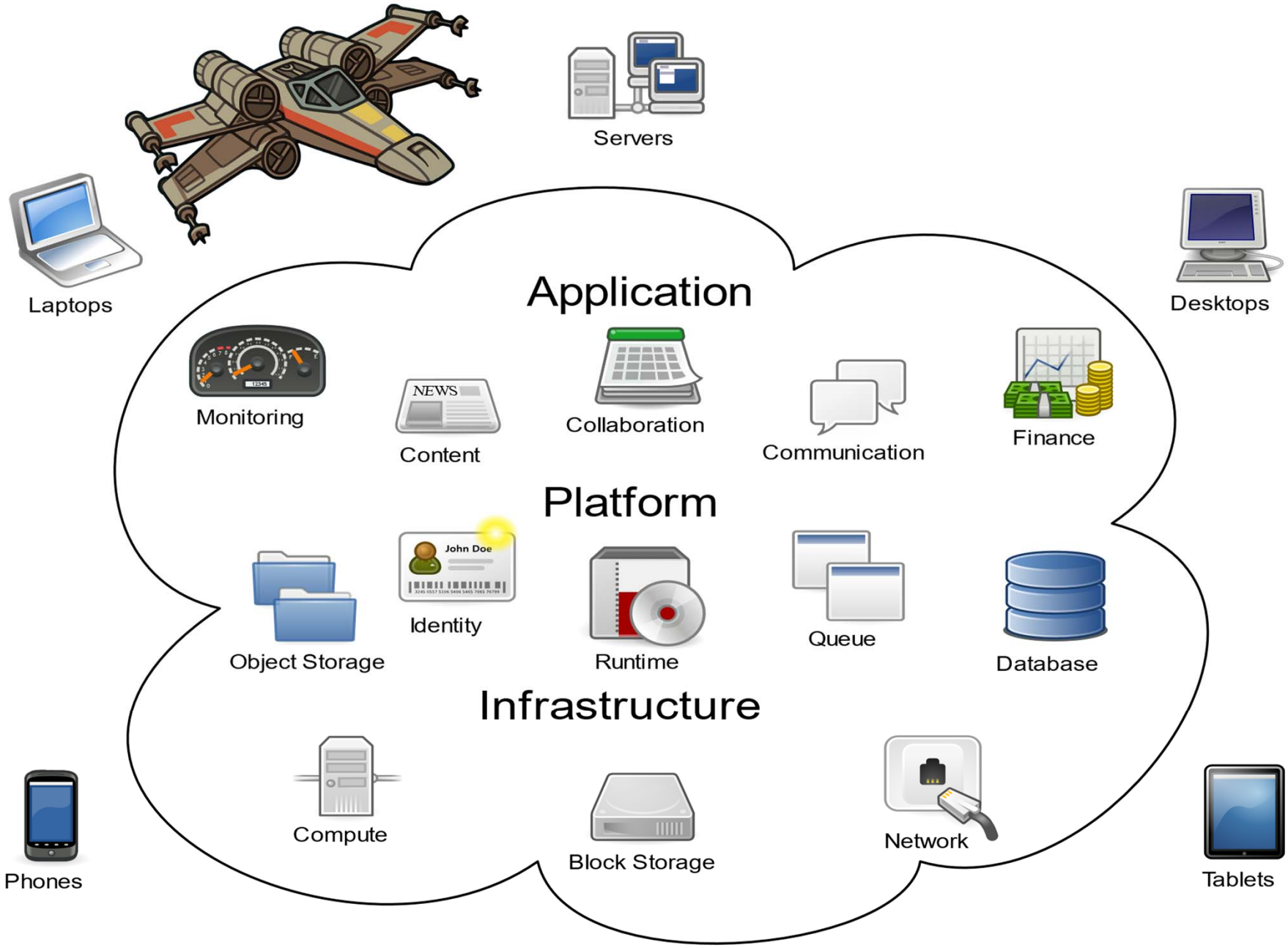
ARMA Board of Directors

Author: 7 Steps for Legal Holds of ESI & Other Documents

May the Fourth Be With You

Cloud Clarity:
Bringing Sunshine to Vendor Relationships

- Overview
- Privacy and Security
- Risk Assessments
- Service Contracts
- Negotiating Contracts


Servers
Laptops
Desktops
Application
Monitoring
Content
Collaboration
Communication
Finance
Platform
Identity
Object Storage
Runtime
Queue
Database
Infrastructure
Compute
Block Storage
Network
Phones
Tablets

Technophobia

"Fear or Dislike of advanced technology or complex devices and especially computers."

Vocabulary

- SaaS (software as a service)
- PaaS (platform as a service)
- IaaS (infrastructure as a service)
- DaaS (desktop as a service)
- Managed Services
- CoLo (co-location services)
- EULA (end user license agreement)
- SLA (service level agreement)

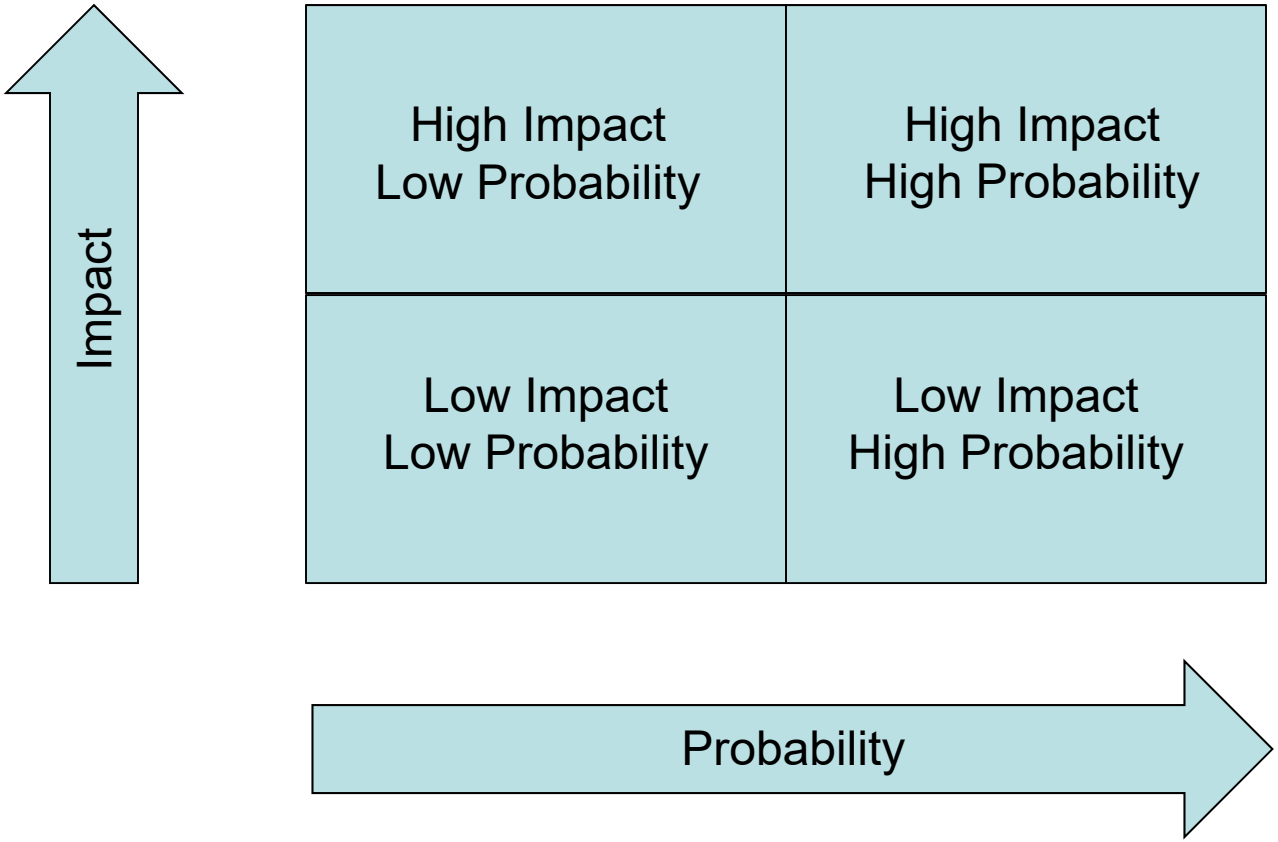
Privacy and Security

- Asset Management
  - Personal Information
  - Access (vendors, yours and customers)
  - Vulnerabilities/Mitigation
- Vendor Management
  - Due diligence
  - Do the security controls meet your needs?
  - Audit
  - Enforce

Vendor Risk Assessment

- Organization
- Employees
- Disaster Recovery
- Change Management
- Application/System Security
- Identity (Access) Management
- Third-Party Audits / Verification

Vendor Risk Assessment



Vendor Management Process

Where is your organization?

Hope for the Best!

Mature Procurement Process

Maturity

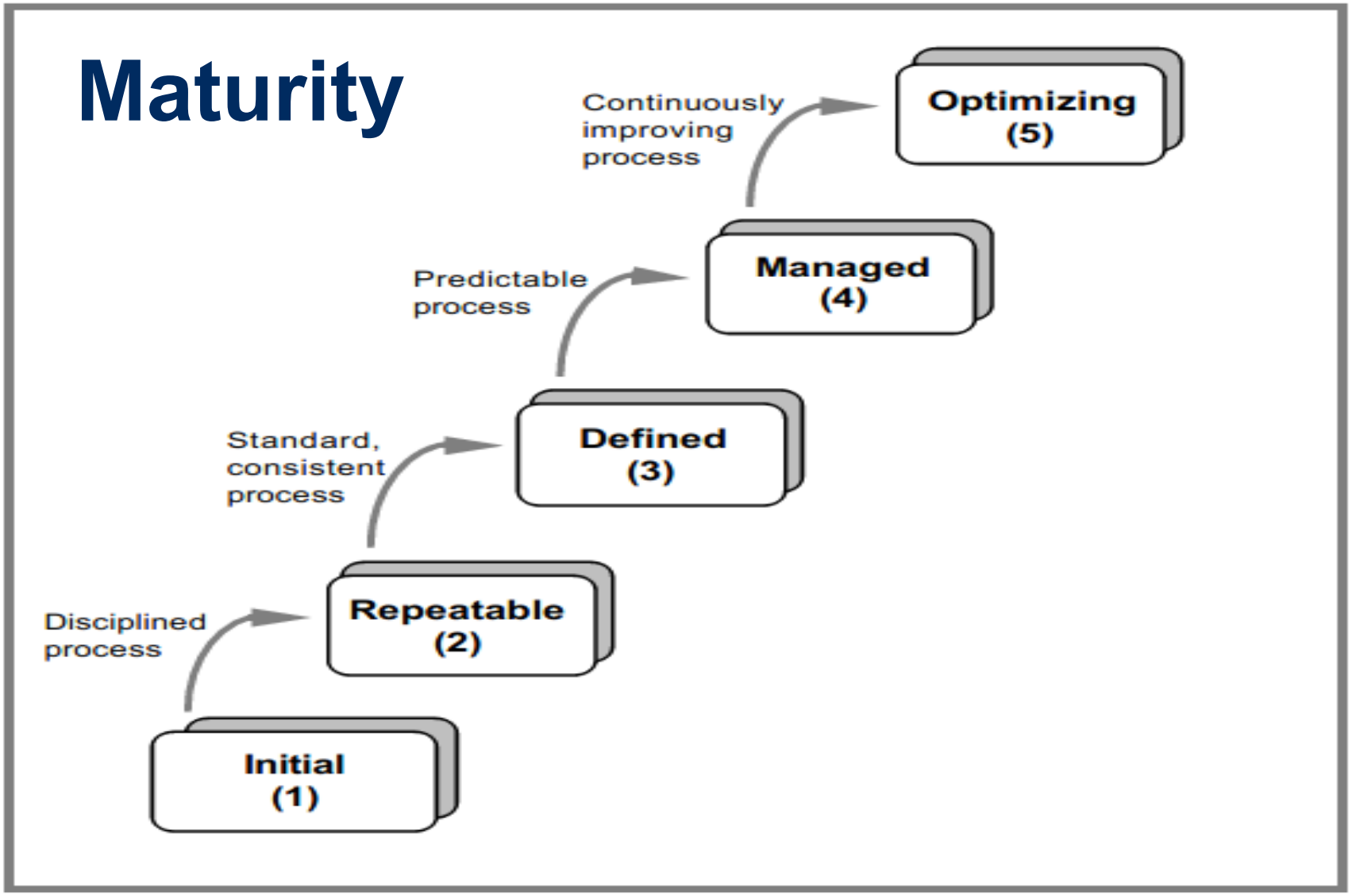


Figure 2.2 The Five Levels of Software Process Maturity

Service Contracts

- Master Service Agreement
- Statement of Work / Work Orders
- Services and Licenses
- Maintenance
- Terms and Conditions (Key!)
- Click-Wraps
- Service Level Agreements

Decoding SLAs

Service Level	Credit Percent *
≤ 2 hours	none
> 2 hours	20%
> 6 hours	40%
> 10 hours	60%
> 14 hours	80%
> 18 hours	100%

Contract Negotiations

- Plan, plan, plan ahead
- Critical to ability to enforce relationship
- Pay attention to contract provisions
  - notices, tenders, information sharing
- Handle breach of Agreements with an eye toward third-party recoveries
- How can you make others pay for *their* mistakes?
- How can you mitigate risks of your mistakes?
- Will your Agreements back you up?

Are Data Security Requirements Defined?

- **Personally Identifiable Information (PII)**
  Personal Information (PI)
  Protected Health Information (PHI)
  - Broad or Narrow definition
  - Does it cover your data?
- **Confidential Data**
  - Treated same or different from PII, PI, PHI?
- **Standard of Care for Protection of Data**
  - **Reasonable Care?**
  - **Security Standard?**
- **Security Incident Defined**
- **Data Breach Defined**
- **Remediation**

Are Breach Response Requirements Defined?

- **Notice Requirements**
  - When is notice to the company required?
    - Incident? Suspected Incident? Confirmed Breach?
  - Notice to others?
  - Prohibition of Notice without Your Consent?
- **Control of Regulatory Notice Process**
- **Cooperation with Investigators**
  - From the company
  - From the company's insurance carrier
  - State or Federal agencies

Can You Enforce Data Security Obligations?

- **Right to Audit Compliance with Data Security Requirements?**
  - Notice / Access / Results
- **Certificates of Compliance?**
  - Third Party Assessments
  - Third Party Certification
- **Ramifications of Non-Compliance?**
  - Ability to Cancel Contract
  - Right to Cure
  - Payment/Assistance for Transfer of Services
- **Insurance?**
- **Remediation?**
- **Obligation to Cure?**
- **Does non-compliance trigger no fee termination?**

Pay Attention to Contract Provisions

- **Definitions**
  - Confidentiality
  - Defining Events = Breach of Agreement
  - Ownership of data, systems, IP created during relationship
  - Personally Identifiable Information (PII)
  - Protected Health Information (PHI)
  - Security Requirements – Physical Controls
  - Security Requirements – Technical Controls
  - Audit (not allowed? Cooperation only?)

Pay Attention to Contract Provisions

- **Notices**
  - Of the breach of the Agreement
  - Tender of costs, defense
  - Intent to seek indemnity / cost reimbursement
  - To all carriers — including vendor / suppliers

- **Deadlines**
  - May be different than SOL
  - Some can be short
  - Failure to adhere can result in lost contract benefits

Pay Attention to Contract Provisions

- **Arbitration Clauses**
  - Covering all events?
  - Covering some events?
  - Generally consumer facing – but more cloud storage and other IT vendors are adding
  - Application of clause to particular circumstances

Pay Attention to Contract Provisions

- **Customer Requirements**
  - What security requirements are imposed on your organization by contract language?
  - Can you use a vendor?
  - If so, under what circumstances is it allowed?
  - Has your organization agreed to specific vendor requirements? (e.g. background checks?)
  - Specific Data Security Requirements
  - Responsibility for actions of your vendors / sub-contractors?

Handle breach of vendor Agreements with an eye toward third-party recoveries

- Admissions / explanations about cause?
- Negligence/Gross Negligence/Willful Conduct
- Descriptions of cause when providing notices
- How will costs be paid and why?
  - are they covered by insurance?
  - are they covered by indemnity agreements?
  - Cost of defense
  - Control of defense

Review Vendor / Supplier Contracts

- **Indemnity Language**
  - What triggers the indemnity?
    - Negligence? Malfeasance? Claims?
  - Pay attention to what costs and claims the vendor agrees to indemnify
  - Cost of Defense / Control of Defense $$$$
  - **Key**: Is any “claim” included or only those adjudicated to be the fault of the vendor?
  - What is the scope of the indemnification?
  - What “damages” are covered?
  - Defense costs?

Review Vendor / Supplier Contracts

- **Choice of Law**
  - "The parties agree that this agreement, any services provided under this agreement, and any disputes arising from it will be governed by and construed in accordance with the substantive laws of the State of Georgia."
  - **Key**: Need not be connected to the parties; but some courts will not enforce (e.g., cross-border agreements, statutory claims, if designed to discourage claims)

Review Vendor / Supplier Contracts

- **Choice of Venue / Consent to Jurisdiction**
  - "Any judicial proceeding arising under or in connection with this agreement or related to any matter that is the subject of this agreement must be brought in a court of competent jurisdiction in the State of Georgia and each party consents to the jurisdiction of state and federal courts located within Fulton County, Georgia."
  - **Key**: Strategic reasons to be/not to be in a particular jurisdiction

Review Vendor / Supplier Contracts

- **Damage Limitations / Disclaimers**
  - "Neither party shall be liable to the other party for any direct, compensatory, indirect or consequential damages, or lost sales or profits arising from any claim under this agreement."
  - **Key**: BEWARE of limited damage clauses.

Review Vendor / Supplier Contracts

- **Warranty Disclaimers**
  - Disclaim express or implied warranties imposed by UCC or law
  - "THE SELLER DISCLAIMS ANY EXPRESS WARRANTY OR IMPLIED WARRANTY, INCLUDING, BUT NOT LIMITED TO, WARRANTY OF MERCHANTABILITY OR FIT FOR A PARTICULAR PURPOSE."
  - **Key**: Cloud and technology vendors usually have strong warranty disclaimers.
  - **Key:** Time limits (60 or 90 days).

Review Vendor / Supplier Contracts

- **Certificates of Insurance – Cyber Insurance**
  - Make sure you have / actually look at them
  - Do they have enough insurance?
  - Do their policies cover cyber risks?
  - Do their policies cover the specific risks associated with your data and use of the vendor?
  - Review their insurance policies!
- **Additional Insured Status**
  - Do you require this?
  - Is confirmation documented in your contract file?

Review Vendor / Supplier Contracts

- **Time Limitations**
  - Agreement to period shorter than statute of limitations to bring a claim / file suit
  - "Any legal claim arising under this agreement must be commenced within one year of any claimed breach or such claim will be extinguished."
  - **Key**: time period must be "reasonable"

Thank You