

Risky Business: SaaS: Data Integrity and Risk-Based Approaches

Judy Baushke

Manager Analysis & Quality
Services

Rho, Inc.



DIA 2011
Chicago, Illinois



www.diahome.org

Disclaimer

- The views and opinions expressed in the following PowerPoint slides are those of the individual presenter and should not be attributed to Drug Information Association, Inc. (“DIA”), its directors, officers, employees, volunteers, members, chapters, councils, Special Interest Area Communities or affiliates, or any organization with which the presenter is employed or affiliated.
- These PowerPoint slides are the intellectual property of the individual presenter and are protected under the copyright laws of the United States of America and other countries. Used by permission. All rights reserved. Drug Information Association, Drug Information Association Inc., DIA and DIA logo are registered trademarks. All other trademarks are the property of their respective owners.



Identify and Manage Risks

- SaaS relationship review:
 - **Supplier: Duties as Data Processor, System Manager**
 - **Customer: Duties as Data Controller / Owner**
- Service Level Agreement (SLA)
 - **Details depend on amount paid, intended use**
- Define the Intended Use
- Then Define the Risks



SaaS

- Biggest Risks?
 - Hosting, support and maintenance services being provided to the customer by the supplier
- What are common industry concerns?
 - Disaster Recovery
 - Data Protection – Integrity
 - Security Provisions
 - Return of “Customer” Owner Data



SaaS Risk Considerations

- Intended Use
 - **Types of:** **System** **Data**
- Data Storage
- Ownership of Data
 - Storage and return of the data, destruction of data
 - Tenancy - Audit Rights - Contractual Provisions
- Do your homework – research – then audit!!
 - warning letters, press releases, web testimonials



Type of System

- **What is the hosted service?**
 - **Hardware**
 - **Security - storage - databases**
 - **Software**
 - **Are they the developers or simply the host?**
 - **User Administration?**
 - **Other (help desk services, etc.)**
 - **Data!!**
 - **Other services?**



Type of Data

- Safety
- Product Quality, Efficacy
- Regulatory Submissions
- Intellectual Property
- Confidential
- Financial
- Other



Data Storage

- Where location?
 - Data center, staff, backups - alternate site(s)?
- Who is operating it?
 - Credentials, training - use of subcontractors
- How using what procedures?
 - Security, Backup and Disaster recovery
 - Upgrades, maintenance to software and hardware
 - Support services -hosting or software problems
- When? Support hours



Data Integrity Questions

- What's the worst that could happen?
 - Agency rejects data, Sponsor requires rework
- How can integrity of data be compromised?
 - Poor monitoring, record integrity, and controls
- What activities provide assurance?
 - GDP, SOPs, monitoring, queries, validation
- How is it measured and maintained?
 - Deviations, queries, exception reports, audits



Risky Business

- 2 types of risk
 - Project(People/Business) Risks
 - Data Risks (Need/Retention/Regulations)
- 3 categories related to 2 types of risk
 - Manual, human error
 - Automation error
 - Development or configuration error
- Assessment, Analysis, Management, Control



Risk Control Categories

- Software/design-integrated controls
 - Roles, privileges
 - Modular components
 - Workflow guided processing
 - Audit trails
 - System & Business controls
 - Technology / Logins / Firewalls / Encryption
 - Contractual & Service Level Agreements
 - * Validation, Change Control, Configuration Management
 - Processes and practices (SOPs, training)
- Validation, testing, change control*
- Audits



Risk	Requirement	ALCOA+	Risk Response/Technique
Data or file corruption or loss	ICH E6-5.13, 11.10(c) Access	Legible	Mitigation, then Acceptance: Back-up and restore testing, Backups
Changes to data/metadata	ICH-E6 4.9.3, CFR312.62, 11.10(e) Audit Trails	Contemporaneous, Attributable	Mitigation: Testing/Change Control & Configuration Management → Validation Life Cycle
Unauthorized data changes	ICHE6-5.5.3, CFR 11.10(g) Permissions	Attributable	Mitigation: Audit trail, user log-Ins, roles and privileges
Authorized data changes	ICHE6-5.5.3, CFR 11.10(i, j) Training and accountability	Attributable	Mitigation: Audit trails, Unique user Ids, Signatures, Device authorizations
Loss of Confidentiality	11.30 Confidentiality, HIPAA, ICF	Attributable	Mitigation: Password/privacy policies, password lockout* (let's talk further about cloud computing)
Unauthorized access / user	11.10(d) Limited Access, 11.300(e)	Attributable	Mitigation: Firewall, intrusion testing, password lockout
Lost token	11.10(h) Devices, 11.300(c) Loss management procedures	Attributable	Mitigation: PIN requirement, SOP report lost tokens immediately
Software upgrades or patches	11.10(k) Revision and change control procedures	Contemporaneous, Attributable, Complete	Mitigation: CAB, CRB, system change history logs, source code management tools, Change Control & Configuration Management → Validation Life Cycle
System interfaces	11.10(h) Devices, 11.10(a) Validation, ICH E2B	Accurate, Attributable	Mitigation: Testing/Change Control & Configuration Management → Validation Life Cycle
Data Migration	11.10(a) Validation	Original, Accurate, Consistent, Attributable	Mitigation: Testing/Change Control & Configuration Management → Validation Life Cycle
Configurable User Interfaces, Custom Functions	11.10(a) Validation	Consistent, Accurate, Attributable	Mitigation: Testing/Change Control & Configuration Management → Validation Life Cycle
Record Retention (archival, purge)	11.10(a) Validation, 11.10(c) Record Retention	Original, Complete, Enduring, Available	Mitigation: Testing/Change Control & Configuration Management → Validation Life Cycle
Cloud Computing	Open 11.30 Controls for open systems. Include additional measures beyond 11.10 requirements	ALCOA - CCEA	"Public Cloud" . . . Avoidance . . . Hefty SLA's, Contractual Penalties
	Closed 11.10 Controls for closed systems	ALCOA - CCEA	"Private Cloud" . . . Mitigation: Testing/Change Control & Configuration Management → Validation Life Cycle

Controlled Documents (SOPs) and Training / LifeCycle Risk Monitoring

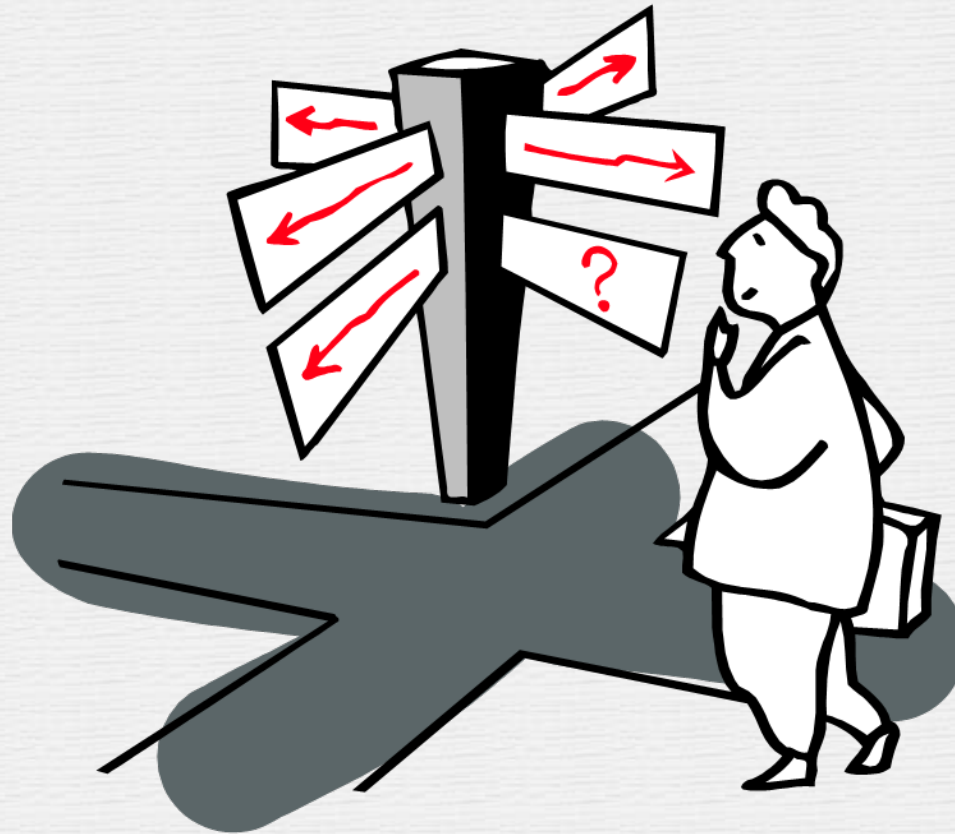
ALCOA+ Attributable-Legible-Contemporaneous-Original-Accurate - (Complete, Consistent, Enduring, Available)

Risk Responses: Avoidance, transference, mitigation, acceptance

- Manual error
- Automation error
- Dev or config error



Where do we begin?



Regulations / Guidelines / Good Practices

- GxP Decision Tree
 - FDA (GCP, GLP, GMP) regulations: 21 CFR Parts 320 And 820 And 312, 314, etc.
 - All ICH guidances, E2 (E2A, E2B), E5, E6 (E6 -section 5.5), E8, Q9
- CFR 21 Part 11
- Reflection Paper on Expectations for Electronic Source Documents Used in Clinical Trials, EMEA, 17 Oct 2007
- Computerized Systems Used in Clinical Trials, FDA, 1999
- All EU Directives as applicable (2001/20/EC, Directive 2005/28/EC, Directive 2001/83/EC, Regulation (EC) No 726/2004), EUDRALEX Volume 10
 - EUDRALEX Volume 4, Annex 11: Computerised Systems
 - PIC/S Good Practices for Computerised Systems in Regulated "GXP" Environments
- GAMP, ANSI, ISO/IEC, IEEE, PDA, ASTM, SWEBOK, TickIT (UK), ITIL, COBIT, NIST
- Others (SOX Compliance, SAS70 or SSAE 16 - Service Organization Control)
- Privacy, Data Protection
 - HIPAA, PII, EU 95/46/EC, Japan PIPA, Canada PIPEDA



21 CFR Part 11 offers Insight

- **Areas to be addressed by procedure(s)**
 - ✓ 11.10(c): **Back-up and Record Retention**
 - ✓ 11.10(d) and 11.300(c): **Password Control**
 - ✓ 11.10(i) : **Education, Training, and Experience**
 - ✓ 11.10(j), 11.200(a)(2) **Log-on Accountability**
 - ✓ 11.10(k)(1), 11.10(k)(2): **Change control**
 - ✓ 11.100(b): **Individuals verified** before assigned electronic signature authority
 - ✓ 11.300(d): **Security Reporting**
- **But doesn't specify SOPs on *service***



Vendor Quality System

- **Compliance** -
 - ISO certification
 - SSAE 16 SOC reports
- **Policies, SOPs**
- **Training /Qualifications**
- **Validation**
- **Risk Management**
- **Change Control / Configuration Management**
- **Disaster Recovery**
- **SECURITY!!**
 - facility, systems, reporting of intrusion attempts, breaches
- **Customer Support - Help Desk**
 - Incident Reporting & Tracking
- **Communication Methodology**
- **Internal Audit Program**
 - metrics, effectiveness
- **Continuous Improvement / CAPAs**
- **Supplier Qualification program**
 - (hardware, software, subcontractors, etc.)
- **Service Level Agreements**



Scope

- **Are they the software supplier?**
 - What's their development process and lifecycle management plan? SOPs and process docs
- **Validation – plan, test, report**
 - Master Validation Plan or Validation Plan
 - Testing/Qualification: IQ/OQ/PQ process layers
 - Validation Report
 - Did they execute the plan or deviate?
 - Demonstrate traceability requirements to test to outcome?
- **Change Control**



System Administrator

- **Configuration / Change Management**
 - **Implementation /roll-back practices**
 - **Environment management - test - production**
 - **Single- or Multi-tenant environment**
 - **Notification practices**
 - **User administration**
 - **Hardware, firmware replacement or addition**
 - **Retirement plans**
- **Do they have SOPs? Is training documented?**



System Management

- Security - Physical - Logical
- Redundancy - Uptime / Downtime
- Storage - Routine - Backups - Archival
- Disaster Recovery
- Resourcing
 - Staffing - Availability - Expertise - Training
- Reporting - Criteria - Escalation
- Communication
 - Obligation to notify the customer – when?



System Management and Monitoring

- Tools – Security, Monitoring and Reporting
 - Firewalls and Cryptology used
 - Virus protection mechanisms
 - Operational management alerts:
 - **Disk space, performance, intrusion attempts**
 - Virtual systems
 - Testing of the tools
 - Vendor qualifications
 - Help Desk /CRM
 - Logs and Reporting

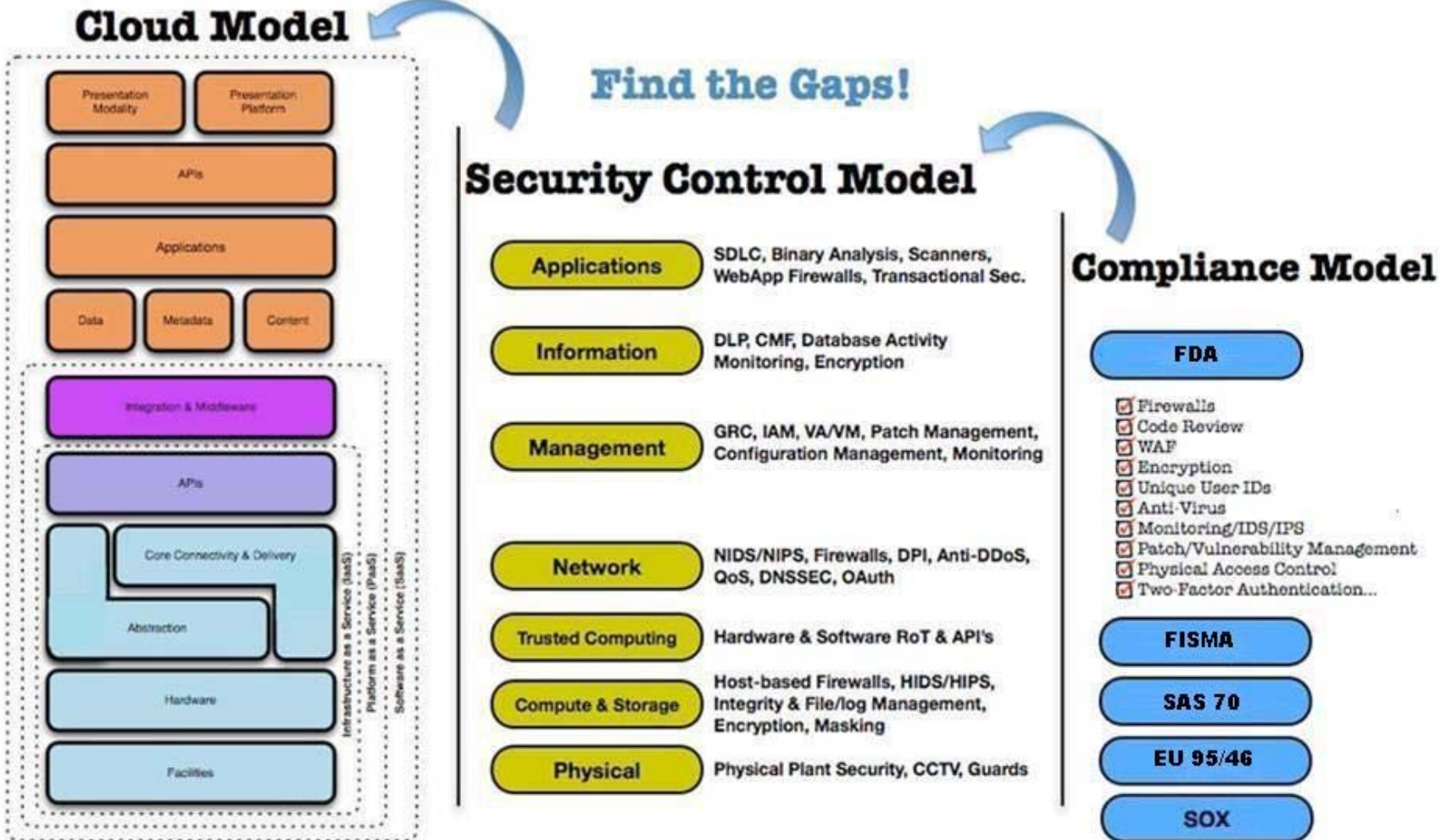


Cloud Security Alliance

- Cloud Security Alliance
 - Not-for-profit organization promoting best practices and education
- www.cloudsecurityalliance.org
- <https://cloudsecurityalliance.org/csaguide.pdf>
- <https://cloudsecurityalliance.org/research/projects/cloud-controls-matrix-ccm/>
 - Security controls framework



Cloud Model¹



¹Security Guidance for Critical Areas of Focus in Cloud Computing v2.1, Cloud Security Alliance, 2009 (and SQA: Cloud Computing, Compliance and Security: A Panel Discussion, 2011)

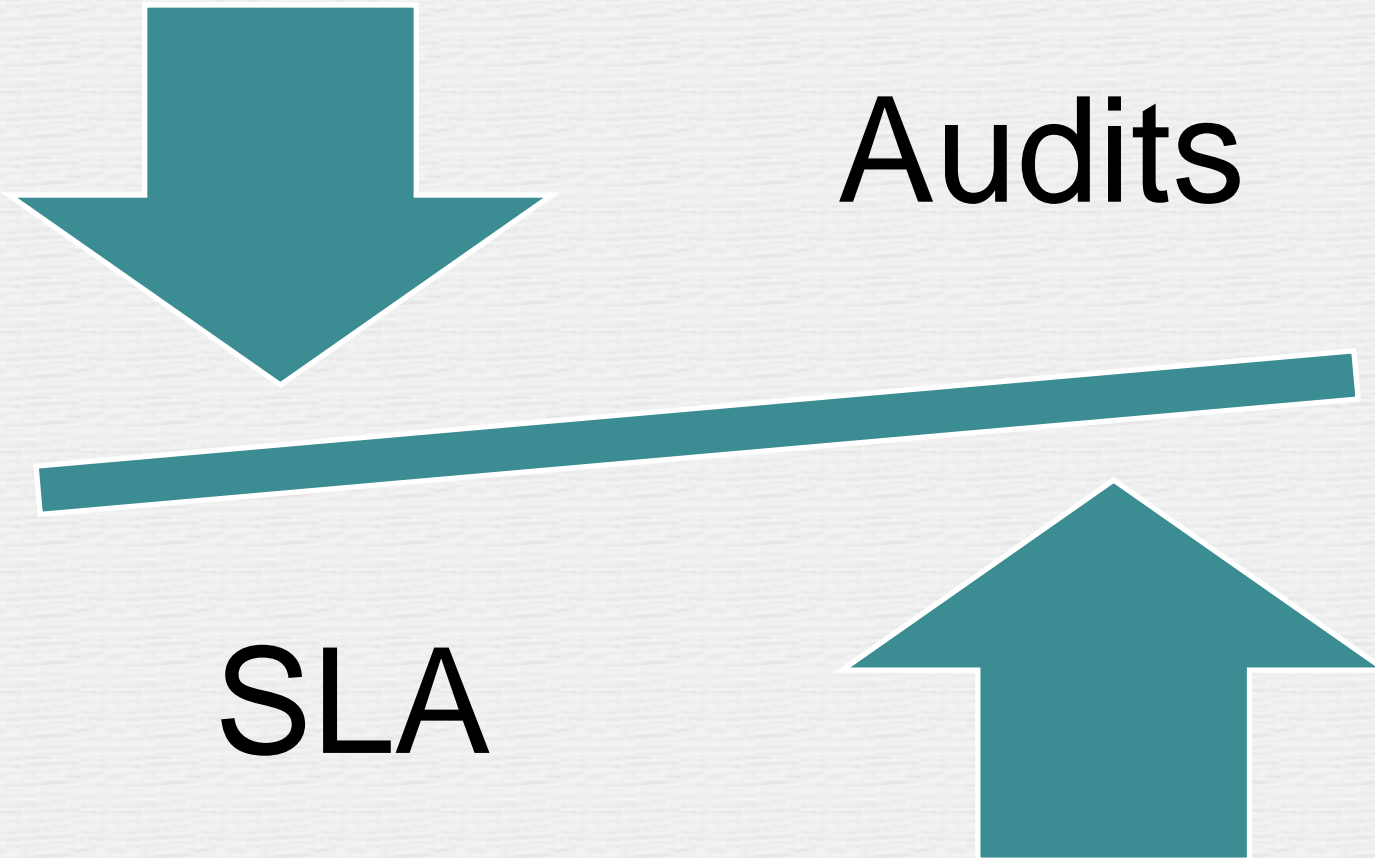
Cloud Controls Matrix¹

- CO - Compliance – Audits, Regulatory Mapping (6)
- DG - Data Governance - Intellectual Property (8)
- FS - Facility Security (8)
- HR - Human Resources Security (3)
- IS - Information Security (34)
- LG - Legal - Non-Disclosure, Third Party Agreements (2)
- OP - Operations Management (4)
- RI - Risk Management (5)
- RM - Release Management (5)
- RS – Resiliency (8)
- SA - Security Architecture (15)

¹Cloud Controls Matrix, version 1.1: Cloud Security Alliance, December, 2010



Risk Mitigation Strategies



References

- “A New Era of GCP Accountability: FDA Aggressively Targets Clinical Trial Oversight and Data Integrity”, FDLI, Aug 2009
- Guidance for Industry, Computerized Systems Used in Clinical Investigations, FDA , May 2007
- “Reflection Paper on Expectations for Electronic Source Documents Used in Clinical Trials”, EMA, October 2007
- General Principles of Software Validation; Final Guidance for Industry and FDA Staff, FDA, 2002



References (cont.)

- Computerized Systems Used In Clinical Trials, Apr 1999
- GAMP 5: The Good Automated Manufacturing Practice (GAMP) Guide: A Risk Based Approach to Compliant GxP Computerized Systems, ISPE, 2008
- ISO 9001:2000, Quality management systems - Requirements, ISO, 2000
- General Principles of Process Validation, FDA, 1987



References (cont.)

- FDA Guidance for Industry Part 11, Electronic Records; Electronic Signatures – Scope and Application, August 2003.
- Global Harmonization Task Force Study Group 3 Process Validation Guidance, January 2004.
- Service Management – ITIL (IT Infrastructure Library) Version 3, Office of Government Commerce, 2007
- Cloud Security Alliance, 2009
www.cloudsecurityalliance.org



References (cont.)

- NIST (National Institute of Standards and Technology) Special Publication 800-37, rev.1, February 2010, *Guide for Applying the Risk Management Framework to Federal Information Systems, A Security Life Cycle Approach*,
- NIST Special Publication 800-53, rev.3, August 2009 (updated May 2010), *Recommended Security Controls for Federal Information Systems and Organizations* (contains 9 pages of references to legislation, policies, standards, guidelines, etc.)

