Role of IT in Effective Regulatory Compliance

John Avellanet
Cerulean Associates LLC
www.CeruleanLLC.com

© 2010 Cerulean Associates LLC
Acknowledgements

andy villers
akos bartha
dan o’leary
nancy singer
becky rivas
tom lille
jon arakangas
ludwig huber
george smith
ted treece
martin browning
jim roberts
jackie cassada

© 2010 Cerulean Associates LLC
Agenda

why compliance
what is “IT compliance”
where are my challenges
how do I solve
Objectives

understand why IT plays a critical role in compliance

understand the challenges IT faces

familiarize self with IT compliance best practices

be able to avoid common mistakes

kick-start a lean IT compliance strategy
What is your opinion of regulatory compliance?

A
Compliance is a significant distraction to a company’s operations

or

B
Compliance is a significant part of a company’s financial results
More than 94% of all regulatory and judicial investigations...
Translation:

IT has a greater risk of causing damage than any other profession
$45,000,000.00
How much is one email worth?
$103
1 out of 2 CEOs today believe compliance has a significant impact on the bottom line.

Source: CEO and CIO magazines study
3 out of 4 CIOs believe compliance is a significant distraction.
“The question in compliance today is: where is IT?”

- A. Bartha, Director of Quality Compliance, AstraZeneca, 2008
What is IT Compliance
Which one is IT Compliance?

A
Nightly data backups

or

B
Virus protection

or

C
Electronic data management systems (EDMS, LIMS, etc.)
Small Business Solutions Program

Small businesses need to create, control, collaborate, approve, disseminate and store ever-increasing amounts of documents and information. But just as vital, small businesses can be faced with the same compliance requirements within their respective industries and need to do so as cost effectively as possible as global enterprises.

With the Small Business Solution your company can easily achieve compliance and almost instantly begin to recognize a return on your investment while:

- Easily control and manage content and documents for adhering to regulatory requirements in a familiar environment.
- Provide standardized and intuitive processes to all users for accessing the most up-to-date quality documentation and content.
- Provide customers with improved product and service quality while recognizing cost reductions and profit increases.

The Small Business Program includes:

- 2 Editors
- 1st Year Support
- 4 Hours of Remote Installation Support

```
All for $4,995.00 USD
```

“...can easily achieve compliance...”

“All for $4,995.00 USD”
Small Business Solutions Program

Small businesses need to create, control, collaborate, approve, disseminate and store ever-increasing amounts of documents and information. But just as vital, small businesses can be faced with the same compliance requirements within their respective industries and need to do so as cost effectively as possible as global enterprises.

You cannot Buy IT Compliance

- 1st Year Technical and Procedural Support
- 4 Hours of Web-based Administrator Training
- Remote Installation Support
- All for $4,995.00 USD
Which of these practices or beliefs have you ever observed?

__ a policy on the books that is not enforced
__ system documentation that is significantly out of date (or non-existent)
__ expectation of privacy when sending email through the company system
__ lots of system log files being gathered with no review or trending
__ significant business decisions that IT learns about after the fact
__ an assumption that firewalls & virus protection means e-records are safe
__ almost every system has a different username/password schema
__ an assumption that IT’s backups are the company’s long-term data archives

© 2010 Cerulean Associates LLC
What does the Regulator want?
Subjective PROOF

- Management Presence and Communications
- Walk-throughs
- Interviews
- Policies
- Standard Operating Procedures
- Experiences / History
- Culture
Objective PROOF

- Management Memos
- E-mails
- Organizational Chart
- Recorded vs. Reported Metrics
- Policy Enforcement Actions
- Data Integrity Testing
- Meeting Notes
- Resumes / CVs
- Training records
- Certifications (ISO, etc.)
- Independent Audit Reports
- System documentation
“The regulatory investigator doesn’t care about the compliance of a single computer system. He cares about the **overall compliance and integrity of the organization’s data** – it’s proof – because that data has direct bearing on the firm’s product and customers.”

- J. Arakangas, former EU regulatory investigator, 2008
“So what...?”
“The regulatory investigator doesn’t care about the compliance of a single computer system. He cares about the overall compliance and integrity of the organization’s data – it’s proof – because that data has direct bearing on the firm’s product and customers.”

- J. Arakangas, former EU regulatory investigator, 2008
Translation:

IT compliance is all about how IT proves control of e-data integrity.
Data Integrity Defined

Data...
...is **A**ccurate
...has **L**ong-term sustainability
...is **C**omplete
...is **O**riginal
...is **A**ttributable

Data have integrity “if they are fit for their intended uses in operations, decision making and planning.”

- wikipedia.org (data quality)
e-data integrity

- Systems controls
- Personnel controls
- Operational controls
- Record archival controls
this is
IT Compliance
How this looks in the real world....
“The [company name withheld] has failed to put in place procedures which ensure that LAN’s for each site are controlled. Complete system definition documentation has not been maintained. For example, the firm produced no appropriate diagrams identifying all sites/equipment.”

- FDA inspection observation, August 2004
“Data can be retrieved by anyone knowing where it is located… there are no systems to ensure data is not deleted or modified.”

- FDA inspection observation, June 2002
“Your operator was observed using a document that contained a list of so-called user passwords to access the computer....”

- FDA inspection observation, August 2007
Where’s the Love?
Why **IT** can’t rely on lawyers to tell you what to do
Electronic Data Discovery Amendment

- Published December 2006
- Based on 30 years of case law
- Does NOT include all state requirements
- Does NOT supersede any state requirements
- Further varies by individual court protocols
Industry-Specific

FDCA (food, drugs, medication, medical devices, tobacco)
FDAAA (food, drugs, medication, medical devices, tobacco)
HIPAA (privacy and security for health records)
DEA (control of drugs)
ITAR (military grade technologies)
GLBA (commercial and investment banking)
Bank Secrecy Act (commercial and investment banking)
FISMA (doing business with US government)
PCI (security for credit / debit card transactions)
Basel II (banking institutions and data capture)
General Laws & Regulations

Sarbanes-Oxley ("Sarbox")
Electronic Signature in Global and National Commerce Act
Export Administration Regulations
Occupational Safety & Health Administration (OSHA)
Equal Employment Opportunity Commission (EEOC)
Resource Conservation and Recovery Act
Uniform Preservation of Private Business Records Act (UPPBRA)
“Unless a specific period is designated by law for preservation, any business record that state law requires a person to keep or preserve may only be destroyed after the expiration of three years from the making of the record without constituting an offense under state law.”

- Chapter 31-08.1, Paragraph 2
“what the...?”
UPPBRA in Plain English

“Unless a rule says you have to keep something for __ years, assume that the record will need to be kept for 3 years after it was created.”
1. Firms may need to recreate record creation conditions for up to 3 years after document created.

2. And **IT** is responsible for e-record controls and conditions.

3. Thus, **IT** needs to retain (up to 3 years):
   - 1 copy OS/NOS/app + EULA or license
   - SDLC or other lifecycle documentation for those
   - Computer HW/SW disposal records
   - System access / security reports
   - Configuration management records (var.)
“Regulated” e-Records

typical business records

• Financial audit report
• Personnel files
• Purchase orders
• Product distribution records
• Press releases
• Contracts
• Policies & SOPs
• Org charts

regulations & statutes

• 18 USC 1520
• Title VII
• 21 CFR 301
• 21 CFR 820 and 821
• 17 CFR 230
• Uniform Commercial Code
• UPPBRA
• 29 CFR 1627
“Regulated” e-Records

typical IT records
- Security permissions to medical records
- Policies & SOPs
- Operating system
- EULA
- Security access log file
- Disposal of equipment
- Usability testing
- Training presentations

regulations & statutes
- 45 CFR 164
- UPPBRA
- USC Title 17 (copyright law)
- Part 11 or EAR
- EPA (Title 14 CA Reg 18660)
- Title VII (1981 interpretation)
- 29 CFR 1627 or UPPBRA
<table>
<thead>
<tr>
<th>Records</th>
<th>Owner</th>
<th>Location</th>
<th>Verified Date / Initials</th>
<th>Citation (Reg)</th>
<th>Retention Period</th>
<th>Retention Review Date</th>
</tr>
</thead>
<tbody>
<tr>
<td>Project X Spectral Analyses</td>
<td>Analytical chemistry</td>
<td>Lab notebook • Lab storage room • All others • Offsite vault, tape X-14</td>
<td>02/12/2007 BKM 02/10/2008 SHK 02/09/2009 JRA</td>
<td>21 CFR 58.195 (GLPs)</td>
<td>5 years after submission to FDA (est. 2012)</td>
<td>2017</td>
</tr>
</tbody>
</table>
Deadly Sins of IT Compliance
“Can’t we just outsource this?”
“Commercial systems, software and services cannot be compliant by default – [control] is to intended use. Same exact software at two different companies produces two different sets of risks and records....”

- G. Smith, Jr., FDA, 2009
0 ads for “record integrity”

18 ads for “computer compliance”
Who's in Charge?
Where Do You Fit in the Hierarchy?

1. President / CEO
2. Vice president
3. Director
4. Manager
5. Supervisor
Inner Circle of Accountability

President / CEO

Director

VP

manager
everyone else

supervisor
Is our documentation current?
“The [company name withheld] has failed to put in place procedures which ensure that LAN’s for each site are controlled. Complete system definition documentation has not been maintained. For example, the firm produced no appropriate diagrams identifying all sites/equipment.”

- FDA inspection observation, August 2004
Who’s our project manager?
“I thought IT was all about technology not information?”
Do we actually enforce our rules?
What good is training?
73% of CIOs are confused about what it takes to comply
External Challenges
Technology improves every 6 months
Regulations change every 12-16 years
Less than 4% of all U.S. senators and congressmen...
have any background in IT
In the average company, only 20% of compliance costs...
...don’t come from IT.
What are the options?
Implement a Lean IT Compliance Program

benefits

six-step process

more best practices
“The #1 benefit cited by non-IT executives of IT compliance is the improvement of business processes.”
0% Bottom Line Improvement

- IT Procedures & Policies
- Automated Tool Design, Implementation & Maintenance
- Test Tools to OEM Standards
- Maintain “State” in Production
- Maintain Documentation

5-7% Bottom Line Improvement

- Optimize Cross-Functional Processes
- Drive Business to Prioritize
- Fulcrum between Business and Compliance
- Lead Pro-Actively on Compliance
Six-Step Process

1. talk to management
2. assemble a team
3. educate & train
4. document practices
5. interpret controls
6. establish credibility
Talk to Management

Summarize learnings from today

• Show them sample enforcement actions that have humiliated other firms

• Explain the impact of **IT compliance** on the bottom line

• Suggest next steps to build momentum & refine focus
Talk to Management

Sell the benefit

**Save** money, time or resources

**Reduce** risk and legal liability

**Enable** a business strategy to succeed

**Improve** speed and productivity

© 2010 Cerulean Associates LLC
Talk to Management

Six short sentences

1. Business outcome
2. Business benefits
3. Risk reduction
4. Resources required
5. Data integrity help
6. Investment required
IT Compliance Team

Cross-functional steering team

• IT
• records management
• quality (and regulatory affairs)
• corporate compliance
• personnel (HR)
• finance / purchasing
• operational leaders (mfg, R&D, etc.)
IT Compliance Team

Avoid the blame game

Keep the **focus on the outcome**, not the “how”

Develop a 9-month plan to **prove data integrity**

Bring in other functional areas early to obtain “buy-in”
Create educational experiences

• In-person session for key personnel

• Webcast for all employees

• Provide refresher training every 6-14 months
Education & Training

Topics to consider

• How to write policies & procedures people will follow
• How to audit for compliance and get “buy in”
• Who should be involved in investigations
• Steps to control & monitor outsourced IT vendors
• How to follow-up on deviations and noncompliance
• How to document risk management activities
• What not to include in system documentation & testing reports
• The effects of poor & inefficient change control – and how to avoid it
• Putting in place an email etiquette policy
• Going from business strategy to specific IT controls

© 2010 Cerulean Associates LLC
Document IT Practices

Process maps

• work flows & decision-making
• tie-ins with other functional areas

Accountabilities

• organizational chart (CIO to supervisor)
Role-based reviewers

- Responsible for _____ implementation
- Accountable for the ______
- Consulted on the ______
- Informed about the ______

Think of these in the context of policies, change control, system security, configurations, etc.
Interpret IT Controls

Relationship to…

• consumer safety
• product quality (safety & efficacy)
• proof thereof (e.g., records)

“Here’s how we’re going to maintain the integrity of the records that prove…..”
Interpret IT Controls

Questions to answer

**Who** will be responsible for maintaining its state of compliance …?

**What** resources will be committed …?

**When** will the system be retired …?

**How** will you handle the migration of information and its context (data and metadata) …?
Establish Credibility

Pass the audit

• demonstrate continuous improvement
• demonstrate realistic, sustainable policies
• demonstrate awareness and control

Bring in outside expertise
Establish Credibility

IT audit “areas of concern”

Organizational accountability
  • direct reports v. matrixed v. virtual
  • employees v. outsourced IT vendors v. on-site contractors

Controlling changes
  • maintenance, software upgrades and patches
  • emergency changes

Documentation

Personnel qualification
  • resumes v. training
More Best Practices

• Schedule **six days** a year
• Skip the jargon
• Keep in mind **ALCOA** for e-data integrity
• Conduct e-data archive fire drills
• Consider an annual **“snapshot” archive**
Three secrets to passing an audit every time
Executive To-Do List

- review the list of IT compliance resources and bookmark the ones you like
- complete the self-assessment checklist
- summarize today’s session for your team or department
- schedule 1 hour a week on your calendar to focus on compliance issues
- determine if your company has a records retention schedule or matrix
- read the two article reprints in the reference material for more helpful tips and insights

© 2010 Cerulean Associates LLC
Key Takeaway Review

understand why IT plays a critical role in compliance

understand the challenges IT faces

familiarize with IT compliance best practices

be able to avoid common mistakes

kick-start a lean IT compliance strategy

© 2010 Cerulean Associates LLC
Bonus Material

www.ceruleanllc.com/MISRC/ (until September 30th)

- article reprint: Cost-Effective IT Outsourcing
- checklist: 27-point IT Compliance Self-Assessment
- article reprint: Why CIOs Should Commoditize IT
- trial subscription to Cerulean’s monthly lean compliance newsletter, SmarterCompliance
John Avellanet solves compliance worries. He is the author of *Get to Market Now! Turn FDA Compliance into a Competitive Edge in the Era of Personalized Medicine*, and writes and publishes the monthly executive *SmarterCompliance™* newsletter.

He has a breadth of experience designing, implementing, and maintaining IT, records management, quality systems and compliance programs for FDA 21 CFR 58, 210/211, 820/822, Part 11, the ICH and GHTF, plus ISO 13485, 17799, 17025, and 15489.

For more than 15 years, John served as an executive accountable for compliance, records management, and information technology. He was trained as a Part 11 inspector and spent 5 years as a CIO for a Fortune 50 combination medical device subsidiary.

In 2006, John co-founded Cerulean Associates LLC, an independent compliance advisory firm providing lean compliance expertise to clients worldwide.
Upcoming Events

- **Sept. 24th**: Keynote address (9th Annual Pharmaceutical Contracting & Outsourcing Conference)

- **Oct 7th**: Webinar on minimizing supplier risk (Park Avenue Presentations)

- **Oct 14th**: Webinar on preparing for FDA’s enforcement of 21 CFR part 11 (ExpertBriefings)

- **Nov 4th**: Webinar on 21 CFR part 11 lean IT compliance best practices (Thompson Publishing)
thank you