



IT Compliance in the real World

Comm Solutions

CREATE ♦ CONNECT ♦ SECURE



Business Mission

Comm Solutions is a network and systems technology integrator providing end-to-end solutions that ensure business integrity for enterprise-level customers. From design through deployment, Comm Solutions teams with customers to help align their business and IT objectives. We architect and implement IT solutions spanning computing infrastructure, enterprise management, and security.

Defining Compliance

Compliance:

The state of a business' adherence to widely accepted business standards, practices and regulations.

- Not all Compliance is:
 - Regulatory in nature
 - Domestic in nature
 - Not all compliance requirements are currently written
 - Not all compliance requirements are externally generated
- Unlike Y2K IT Compliance is a recurring event
- Compliance is not something that can be ignored

Compliance Pressures

- Governmental/Legislative/Legal
- Marketplace
 - Customers
 - Suppliers
 - Competition
- Business
 - IP or other information liabilities
 - Human Resources
 - Business Integration

Compliance Drivers

- **SOX – Sarbanes-Oxley, 2002**
 - Effective controls for financial reporting
- **Gramm-Leach-Bliley (Financial Services Modernization) Act, 1999**
 - Security of individually identifiable financial information
- **European Union Data Protection Directive,**
 - Baseline data protections for EU citizens.
- **Basel II, 2006**
 - Int'l banking mandate requiring proven operational IT Security practices
- **Bank Secrecy Act, 1970 & Patriot Act, 2001**
 - Anti money laundering efforts
- **The Federal Information Security Management Act (FISMA), 2002**
 - Security auditing of Federal Government Agencies and Contractors
- **Payment Card Industry Data Security Standard (CISP), 2001**
 - Instituted by Visa and MasterCard to protect cardholder data
- **Stock Markets**
 - SEC, NYSE, NASD records retention
- **HIPAA (Health Information Portability Act), 1996**
 - Security of protected health information
- **FDA**

Compliance Costs

- \$25 billion in 2005 for compliance in the US Securities Industry – 93% of costs for all Companies were staffing related [SIA, 56 Member Companies surveyed]
- 238 SEC accelerated filers' total average cost for SOX 404 compliance was \$3.8 million in 2005 - \$904.4 million - while costs can double for Companies over \$1B [FEI survey]
- SOX Compliance cost for GE in 2004 – 30 million [GE]
- 1,295 restatements of financial earnings in 2005 -1 in 12 Public Companies - doubling from 2004 [Glass, Lewis & Co. LLC]
- Closer to home - 2005 Taxes:
 - Individuals, businesses and nonprofits will spend an estimated 6 billion hours complying with the federal income tax code [Special Report]
- Other costs:
 - Duplication of efforts
 - Business impact – Capital, Opportunity
 - Resource & Project impact
 - External expertise
 - Education

Compliance Status

- Compliance is generally considered (or becomes) a disruptive force.
- In many Companies “Compliance” is forced upon staff and into systems.
- “Speed of Business” issues (disruption, cost, time, staffing, etc.) are sited as primary reasons for not pursuing compliance.
- Many business hide from Compliance until it is too late.

Compliance Examples

Compliance in Operation:
Starbucks, Jiffy-Lube, McDonalds

Industry Compliance:
The new tunnel
RFID everywhere

Legislative Compliance:
Environmental Impact

Corporate Compliance:
“How does this application work?”
400 APs in 90 days
Patching

Legal Compliance:
Illicit materials on the server
Information walking out the door

International Implications
CNIL & McDonalds, Global Ethics and
Walmart

Business Integration
Compliance, Acquisitions & the new
CIO

Driving Compliance

Every organization should plan for success - hope is not a plan.

Plan & Organize:

- Publish a clear technical roadmap
- Ensure Management, Employees and vendors understand their roles and responsibilities.
- Manage costs
- Manage initial requests
- Manage projects
- Communicate

Acquire & Implement:

- Identify solutions
- Manage change requests
- Manage costs
- Ensure a “set to production” process exists
- Take time to document solutions

Driving Compliance

Deliver & Support

- Establish service benchmarks – providers & systems
- Educate users
- Ensure secure operations
- Manage issues
- Provide consistent day to day Systems Operations
- Allocate costs

Monitor & Evaluate:

- Monitor & Evaluate internal and overall IT Performance
- Ensure regulatory compliance
- Ensure IT is aligned with Business goals & objectives

Compliance Lessons

- Survey your compliance landscape – avoid duplication, start as small as needed.
- No framework or standard is inclusive - but look to established practices.
- Being process oriented puts you ahead of the game – if it isn't documented it didn't happen.
- Publish your “menu of services”.
- Publish a clear technical roadmap.
- Communicate frequently.
- Users indoctrinated into a process generally follow that process – use this to your advantage.
- Implement sound request and change management procedures.
- Leverage existing systems and internal resources – consensus & a team approach.
- Transition planning is critical to providing consistent service.
- Service metrics are critical to providing proof of service delivery.
- Remove other options – limit items that can circumvent .
- Processes allow you to arbitrate with your Auditors.
- The good news is that while complacency rules Security is slowly becoming a factor in business strategy.

Thank you for your time.

www.commsolutions.com