SharePoint Deployment and Governance Using COBIT 4.1

October 20, 2011
UNF 2011 Cybersecurity Awareness Showcase
Timothy P. McAliley, CISA, CISM, CISSP, PMP, ITIL-F

Speaker Introduction:

- 12+ years in IT
- Currently work for Symantec and some Contract Consulting/Training
- Worked for:
  - Football Fanatics (Jacksonville, FL) (High Volume e-Commerce)
  - ASM Research, Inc. (Fairfax, VA) (Defense Contractor)
- Designed/Implemented:
  - Change/Configuration Management Processes/Policies
  - Business Continuity/Disaster Recovery Processes/Policies
  - Release Management Processes/Policies
  - Service Desk Operations (Incident/Problem Management)
- Production/Operations DBA for 9 years
- Information Assurance Manager for Pentagon-based System
- Florida State University Political Science Major
- Former USMC Enlisted/Former U.S. Army Commissioned Officer
Speaker Introduction:

- SharePoint Experience
  - Started IT Career Supporting Hummingbird Document Management
  - SharePoint Portal Server 2001
    - Configured /Administered
  - SharePoint Portal Server 2003
    - Configured /Administered
  - SharePoint 2007
    - Site Administrator
    - Data-Tier Administrator
  - SharePoint 2010
    - Configured/ Administer a Visual Studio Team Foundation SharePoint Server Portal
    - Testing Contributor to Symantec SharePoint 2010 Deployment
    - Designing and Implementing SharePoint 2010 Training for Symantec Technical Support Teams

Obligatory Dilbert Reference
What is SharePoint (2010)?

- SharePoint is the business collaboration platform for the enterprise and the Internet
- SharePoint enables your enterprise to
  - Deliver the best productivity experience
  - Cut costs with a unified infrastructure
  - Rapidly respond to business needs
- SharePoint does this by providing capabilities
  - Sites, communities, content, search, insights and composites
What is SharePoint?
SharePoint Products and Technologies

- SharePoint Foundation 2010
- SharePoint Server 2010 for Intranet Scenarios
  - Standard or Enterprise Client Access License
- SharePoint Server 2010 for Internet Sites, Standard or Enterprise
- Office Web Apps
- FAST Search for SharePoint 2010
- FAST Search for SharePoint 2010 for Internet Sites
- Search Server 2010 and Search Server Express 2010

- Developer Tools
  - Visual Studio 2010
  - SharePoint Designer 2010
- Clients
  - Office client applications
  - SharePoint Workspace 2010
  - SharePoint Mobile
- Servers
  - Duet Enterprise for Microsoft SharePoint and SAP
  - Project Server
  - Dynamics

Benefits
...content management and availability
Challenges

...securing and auditing access...

"We fixed the glitch."

What are the challenges presented by Deploying and Maintaining SharePoint?

- White Noise
- Failure to align with business needs
- Failure to align with regulatory/compliance
- Failure to meet ROI metrics
- Poor adoption from user community
- Solution Sprawl / “SharePlosion”
What are the challenges presented by Deploying and Maintaining SharePoint?

- Stale content litters “ghost towns”—sites that were once thriving areas for groups, now suddenly abandoned
- Steep declines in performance and supportability
- Lack of clarity on who is storing what in SharePoint
- Inability to track or audit who has accessed items stored in SharePoint lists and document libraries
What are the challenges presented by Deploying and Maintaining SharePoint?

A Governance Plan describes how your SharePoint environment will be managed.
- Roles, Responsibilities
- Architecture
- Monitoring & Reporting
- Content Utilization Auditing
- Enhancements, Change Requests, Incidents
What is a SharePoint governance plan?

- General Keys to an Effective Governance Plan
  - Vision statement
  - Roles and Responsibilities
  - Guiding Principles
  - Policies and Standards
    - Content Policies and Standards
    - Design Policies and Standards
  - Training and Communications

What is CobiT 4.1?

- CobiT 4.1 defines a set of principles, called domains, that are used to guide governance of information and related software management systems. CobiT consists of 34 processes, and 210 Control Objectives across the following four domains:
  - Plan and Organize
  - Acquire and Implement
  - Deliver and Support
  - Monitor and Evaluate
What is CobiT 4.1?

Figure 1—The Four Interrelated Domains of CobiT

- Plan and Organise
  - Acquire and Implement
- Monitor and Evaluate
- Deliver and Support

Source: ISACA, CobiT 4.1, USA, 2007

What is CobiT 4.1?

Figure 2—CobiT Framework

Source: ISACA, CobiT 4.1, USA, 2007
SharePoint 2010 Architecture

Roles and Topologies in SharePoint Farms (Physical Architecture):

Roles
- Web Front-End (WFE)
- Database (SQL)
- Application Server
  - Central Administration
  - Service Applications (SAs) such as search
  - Office Web Apps

Topologies
- Single-server: all roles
- Single WFE, SQL
- Two WFEs (redundant web apps and services), SQL
- Multiple servers providing redundancy and performance optimization based on the allocation of services, SQL cluster

Security Roles and Groups

Administration Hierarchy
- Server or Farm Administrators
  - Local Administrators
  - Farm Administrators
- Service Application Administrators
  - Service Administrators
  - Feature Administrators
- Site Collection Administrators
- Site Administration
- Content (Document Library or List, Item)
Securing SharePoint 2010 Information

- Securing a SharePoint Farm
- Securing a Web Application
- Securing Site Collections
- Securing Sites
- Securing Lists
- Windows PowerShell Security
- Service Application Permissions

How CobIT can be used to deploy and govern SharePoint 2010?

- Dave Chennault/Chuck Strain – “SharePoint Deployment and Governance Using CobIT 4.1: A Practical Approach”
- Authors mapped SharePoint deployment and governance to CobIT 4.1”
- Recommend a phased methodology
- Scorecard to Track Progress
How CobIT can be used to deploy and govern SharePoint 2010?

- Chennault/Strain Framework:
  - Scope Phase
  - Plan for Launch Phase
  - Prepare for the Operations Phase
  - Launch Phase
  - Operate Phase
  - Enhance Phase
  - Risk/Mitigation Strategies
  - Cloud-based utilization

Scope Phase

CobIT Process Mapped to SharePoint Activities
- PO1 Define a Strategic IT Plan
- PO2 Define the Information Architecture
Scope Phase

PO1 Define the Strategic IT Plan
A. Create a steering committee to guide deployment
B. Identify key strategic goals
C. Identify business unit that are participating in the project
D. Indentify strategic needs and map to SharePoint functionality
E. Identify key business owners for each initiative
F. Set priorities

Scope Phase

PO2 Define the Information Architecture
A. Identify scope of the site types in deployment
B. Identify owners
C. Identify roles
D. Develop process for site request, approval and creation with auditing, including content types and permissions
Plan for Launch Phase

CobIT Process Mapped to SharePoint Activities
- PO3 Determine Technological Direction
- PO4 Define the IT Processes, Organization and Relationships
- PO5 Manage the IT Investment
- PO6 Communicate Management Aims and Directions
- PO9 Assess and Manage IT Risks
- PO10 Manage Projects
- A11 Identify Automated Solutions
- DS1 Define and Manage Service Levels
- DS6 Identify and Allocate Costs
- DS11 Manage Data

Plan for Launch Phase

PO3 Determine Technological Direction
A. Align business requirements with SharePoint capabilities
B. Evaluate SharePoint email options
C. Identify integration opportunities with existing data systems
D. Identify MS Office integration needs
E. Identify integration opportunities with existing unstructured content stores
Plan for Launch Phase

PO4 Define the IT processes, organization and relationships
A. Determine tactical team members and responsibilities
   I. Operations Team
   II. Support Team
   III. Development Team
B. Identify location of staff

Plan for Launch Phase

PO5 Manage the IT Investment
A. Develop policies and procedures for usage and performance monitoring
B. Develop policies and procedures for ROI measurements
Plan for Launch Phase

PO6 Communicate Management Aims and Directions
A. Develop policies and procedures to collect and review business objectives with the business
B. Develop policies and procedures to review and prioritize business objectives
C. Identify the value of each requirement. Include ROI calculations. Align plan with business objective.
D. Develop reports, communicate and monitor progress in

Plan for Launch Phase

PO9 Assess and Manage IT Risks
A. Develop a risk management framework
B. Develop release and upgrade policies
C. Develop site provisioning policies
Plan for Launch Phase

PO10 Manage Projects
A. Review and assess the project management methodology
B. Review and assess the project management capability
C. Review and assess the resource planning capability and the ability to staff projects adequately for upcoming project phases

Plan for Launch Phase

AI1 Identify Automated Solutions
A. Define and maintain a business functionality review process
B. Define and review content risk analysis
C. Identify software tools required for solution
D. Identify hardware requirements based upon an agreeable architecture for indexing, searching, and serving web front-end and database needs
Plan for Launch Phase

DS1 Define and Manage Service Levels
A. Develop or review the service level framework
B. Define services and service level agreements for SharePoint
C. Define the searching requirements, including scope and result set
D. Define the indexing requirements and schedule

Plan for Launch Phase

DS6 Identify and Allocate Costs
A. Develop agreement between IT and affected groups on accounting policy and practice
B. Develop and agree upon service definition with all interested parties
C. Develop agreement between IT and business units on cost allocation policy and practice
D. Develop and review cost allocation reports and agree upon format with users
Plan for Launch Phase

DS11 Manage Data
A. Develop business requirements for data management needs
B. Develop processes to review data sources and data integrity
C. Create policies and procedures to review completeness of data
D. Develop policies and procedures to review error processing
E. Develop error log tracking and remediation processes
F. Develop storage requirements, including business and legal content life cycle and retention requirements
G. Develop data backup requirements
H. Review destruction-of-data policies and procedures
Plan for Launch Phase

DS11 Manage Data (continued)
I. Develop SLAs for restoring data at the virtual machine, physical machine and list item level
J. Develop security requirements for data backup media
K. Develop and review data restoration policies and processes for virtual and physical machines, including onsite, offsite and item level restore within required SLA

Prepare for Operations Phase

CobIT Process Mapped to SharePoint Activities
- PO7 Manage Human Resources
- PO8 Manage Quality
- A12 Acquire and Maintain Application Software
- A13 Acquire and Maintain
- A14 Enable Operation and Use
- A15 Procure IT Resources
- A16 Manage Changes
- DS2 Manage Third-Party Services
Prepare for Operations Phase

CobIT Process Mapped to SharePoint Activities (continued)
• DS4 Ensure Continuous Service
• DS5 Ensure Systems Security
• DS7 Educate and Train Users
• DS9 Manage the Configuration
• DS12 Manage the Physical Environment
• DS13 Manage Operations
• ME1 Monitor and Evaluate IT Performance
• ME2 Monitor and Evaluate Internal Control

Prepare for Operations Phase

PO7 Manage IT Human Resources
A. Develop and execute a training plan
B. Monitor estimated training completion v. actual completion
C. Monitor skill set development alignment with business and technical requirements
D. Align project portfolio human resource requirements with the project plan
E. Develop a policy for employee conduct and system usage
Prepare for Operations Phase

PO8 Manage IT Quality
A. Develop and execute testing plan to ensure quality of service and reliability for the delivered SharePoint farm

Prepare for Operations Phase

A12 Acquire and Maintain Software
A. Develop a high-level architecture
B. Review audit logging of how SharePoint is used and by whom
C. Review authentication schema
D. Review of 3rd party Web Parts and add-ins
E. Develop the quality assurance plan
F. Review and audit software license keys for compliance with laws and regulations to use SharePoint legally (and all of architecture)
Prepare for Operations Phase

A13 Acquire and Maintain Technology Infrastructure
A. Review vendor sourcing of hardware/software
B. Review virtualization strategy and support for SharePoint
C. Review backup practices and policies
D. Review disaster recovery practices and policies
E. Review the separation of the development, test, and production environments

Prepare for Operations Phase

A14 Enable Operation and Use
A. Develop incident reporting and support processes
B. Develop escalation policies and procedures
C. Develop and review incident notification policies
D. Develop and review operations (monitoring, backup, restore, escalation)
Prepare for Operations Phase

A15 Procure IT Resources
A. Review recruiting/contracting processes
B. Review sourcing selection processes
C. Review acquisition of hardware/software relationships and agreements

Prepare for Operations Phase

A16 Manage Changes
A. Develop policies and procedures to manage requests for change for SharePoint
B. Develop processes to prioritize change requests
C. Develop an emergency change request capability
D. Develop a change request tracking capability
Prepare for Operations Phase

A16 Manage Changes (continued)
E. Develop processes to approve or reject proposed changes to SharePoint
F. Develop change request closure processes
G. Develop process and procedures to create a training plan for changes to SharePoint resulting from a change request
H. Develop data migration policies for change requests

I. Develop content and migration policies and procedures for content associated with change requests
J. Develop integrity testing for migrated data associated with change requests
K. Develop a change request status and impact communications plan
Prepare for Operations Phase

DS2 Manage 3rd Party Services
A. Identify reliance upon 3rd party provider
B. Develop and review supplier risk management
C. Conduct intellectual property review

Prepare for Operations Phase

DS4 Ensure Continuous Service
A. Develop and review SharePoint continuity planning
B. Develop and execute training plan for continuity staff
C. Develop a backup strategy and plan, including any off-site capability
D. Develop disaster recovery processes and controls
E. Develop a post-recovery plan
F. Test the continuity plan with a dry run
Prepare for Operations Phase

DS5 Ensure Systems Security
A. Form a security management team, develop a charter, and hold regular meetings
B. Focus on security awareness and compliance
C. Manage user and service accounts
D. Manage permissions and audiences
E. Monitor usage and the system

Prepare for Operations Phase

DS5 Ensure Systems Security (continued)
F. Protect the system from viruses
G. Develop and review the password protection policies and practices
H. Examine the network security layer
I. Establish procedures and policies for storage and sharing of sensitive information
Prepare for Operations Phase

DS7 Educate and Train Users
A. Identify training for groups of users
   • Farm Administrators
   • Developers
   • DBAs
   • Site Owners
   • SharePoint readers/contributors
B. Evaluate the effectiveness of the training

Prepare for Operations Phase

DS9 Manage the Configuration
A. Document the proposed and as-built configuration of hardware / software
B. Document the proposed and as-built information architecture and site map
C. Maintain documentation of hardware/software as changes occur
D. Maintain documentation of information architecture as changes occur
Prepare for Operations Phase

DS9 Manage the Configuration (continued)
E. Develop and monitor the change management process for review of hardware, software, architecture, permissions, SLA changes.
F. Develop a periodic review process

Prepare for Operations Phase

DS12 Manage the Physical Environment
A. Document the data center layout and design
B. Ensure power-backup meets SLA requirements
C. Develop physical access requirements
D. Create and maintain an inventory of physical and data assets
E. Develop physical and data inventory processes and policies
Prepare for Operations Phase

DS12 Manage the Physical Environment
(continued)
F. Develop reports and monitoring capability of physical and data assets
G. Determine if hot-site capability is required
H. Review, document and maintain SLAs for hardware, software, and support
I. Test business resumption/restoration procedures and capabilities

Prepare for Operations Phase

DS13 Manage the Physical Environment
A. Document or review operations procedures
B. Document or review operational infrastructure monitoring policies and procedures
C. Review all operations policies and procedures to ensure that they meet regulatory and compliance goals
D. Review all operations polices to insure they meet SLAs
Prepare for Operations Phase

ME1 Monitor and Evaluate IT Performance
A. Define the monitoring criteria
B. Define the monitoring procedure
C. Maintain and review the performance logs
D. Define the assessment procedure
E. Define remedial actions

Prepare for Operations Phase

ME2 Monitor and Evaluate Internal Control
A. Create supervisory policies and processes to ensure compliance with security policies
B. Create polices and procedures to enable regular assessments of system usage by HR
C. Develop processes for information security staff to assess SharePoint regularly
D. Create processes and procedures to ensure that SharePoint in compliance with information systems audit controls
Prepare for Operations Phase

ME2 Monitor and Evaluate Internal Control (continued)
E. Create processes and procedures to ensure that SharePoint is in compliance with regulatory and compliance controls
F. Create processes and procedures to ensure that SharePoint is in compliance with 3rd party agreements and controls

Launch Phase

CobIT Processes Mapped to SharePoint Activities
• A17 Install and Accredit Solutions and Changes
• DS8 Manage Service Desk and Incidents
• ME3 Ensure Compliance with External Requirements
Launch Phase

A17 Install and Accredit Solutions and Changes
A. Develop and review a training plan including security awareness for IT and end users, usage policy and end-user training
B. Develop and review content and data conversion and migration policies
C. Develop or review data and content migration plans

(continued)
D. Develop or review integrity tests of converted or migrated content and data
E. Review the test plan documentation and communication to the affected user community
F. Review the policies to promote code and content among the test, staging and production environments
G. Review the post migration review and communication plan
Launch Phase

DS8 Manage Service Desk and Incidents
A. Develop a business continuity plan for coordinating support of SharePoint using support desk processes and staff
B. Develop a severity model and escalation path
C. Develop an SLA incident resolution based upon each type of incident
D. Develop agreed upon incident closure policies and procedures

Launch Phase

DS8 Manage Service Desk and Incidents (continued)
E. Develop a reporting format and feedback mechanism with business users, security and compliance, and IT
F. Develop best practices and a knowledge base to aid the support desk
G. Regularly review support request outcomes and enhance or adapt processes to improve support
Launch Phase

ME3 Ensure Compliance with External Requirements
A. Identify laws and compliance issues with impact on SharePoint use or content
B. Create information rights (IRM) policy templates to comply with regulation and business objectives
C. Audit IRM capabilities
D. Audit capabilities to review access by SharePoint users
E. Review audit reports with appropriate control and management staff

Operate Phase

CobIT Processes Mapped to SharePoint Activities
• PO5 Manage the IT Investment
• DS2 Manage 3rd Party Services
• DS3 Manage Performance and Capacity
• DS9 Manage the Configuration
• D10 Manage Problems
• DS13 Manage Operations
• ME4 Provide IT Governance
Operate Phase

PO5 Manage the IT Investment
A. Monitor actual vs. expected payback

Operate Phase

DS2 Manage 3rd Party Services
A. Monitor suppliers with regard to SLAs and review, data protection review, performance, security policy and performance, and change management policies and notification agreements
Operate Phase

DS3 Manage Performance and Capacity
A. Monitor current hardware performance and SLA achievement
B. Monitor growth trends
C. Develop enhancement and planning requests for future performance capability policies and procedures
D. Monitor data usage and capacity tools to determine adequacy

Operate Phase

DS3 Manage Performance and Capacity (continued)
E. Define architecture and capacity planning for each SharePoint component (indexing, storage, WFE, etc)
F. Develop processes for hardware and software procurement to meet capacity projections
G. Review and define IT staff training to support capacity requirements
H. Develop SharePoint administrator management policies and procedures
Operate Phase

DS9 Manage the Configuration
A. Maintain documentation of the hardware and software configuration as changes occur
B. Maintain documentation of the information architecture as changes occur

Operate Phase

DS10 Manage Problems
A. Monitor service incident requests and types
B. Monitor actual vs. agreed-upon SLAs for each incident type
C. Monitor all security incidents and develop policies and procedures to remediate quickly
D. Develop a schedule to review service and security incidents
E. Monitor user satisfaction with problem management
Operate Phase

DS13 Manage Operations
A. Conduct operational infrastructure monitoring

Operate Phase

ME4 Provide IT Governance
A. Maintain and update the governance plan as needed
B. Regularly review SharePoint governance policies and procedures to ensure alignment with business needs
C. Seek independent evaluation of governance policies and procedures
Enhance Phase

A. Gather and track feedback
B. Evaluate enhancement requests
C. Group enhancements into a cohesive plan
D. Communicate the progress and outcome of the enhancement scoping to the business

Getting Started

- Step 1 - Meet with IT and Project Management Staff
- Step 2 - Meet with Key Business Stakeholders
- Step 3 – Form a Steering Committee
Best Practices

- Form a steering committee consisting of key stakeholders
- Collaborate on a vision statement and guiding principles that align with business
- Establish clear roles and Responsibilities
- Develop and plan for capacity and growth
- Plan on Tiered control (higher for sites/site collections, lower for blogs, Wikis, MySites).

Best Practices

- Automate Monitoring, Reporting, Auditing, and Inventory Gathering
- Design and update Site/Infrastructure Documentation
- Design Detailed Site Map
- Design Detailed Service – Relationship Map
Tools

- Chennault & Strain’s Scorecard and Tools Matrix
- Idera SharePoint tools
- Quest SharePoint tools
- Axeler SharePoint tools
- AvePoint SharePoint Tools
- CodePlex – sample data
- Nintex – workflows and reporting
- Microsoft IRM Solution
- ScriptLogic – DACL/ACL scripting
- SharePoint Best Practice Analyzer
- SharePoint Capacity Planning Tool
- Symantec Compliance Suite for SharePoint

References for more information

Microsoft TechNet SharePoint 2010 Governance Portal
References for more information

Books:

- **Professional SharePoint 2010 Administration**
  by Todd Klinadt, Shane Young and Steve Caravajal
  Wrox Press © 2010 (840 pages) Citation
  ISBN:9780470533338

- **SharePoint Deployment and Governance Using COBIT 4.1: A Practical Approach**
  by Dave Chennault and Chuck Strain
  ISACA 2010 (176 pages)

References for more information

Books:

- **Microsoft SharePoint 2010 Administrator’s Companion**
  by Bill English, Brian Alderman and Mark Ferraz
  Microsoft Press © 2011 (1184 pages) Citation
  ISBN:9780735627208

- **Microsoft SharePoint 2010 Administrator’s Pocket Consultant**
  by Ben Curry
  Microsoft Press © 2010 (656 pages) Citation
  ISBN:9780735627222
References for more information

Whitepapers:

Implementing Governance in SharePoint 2010

SharePoint Server 2010 Governance model
http://go.microsoft.com/fwlink/?LinkId=200591

SharePoint 2010 Governance Planning
http://go.microsoft.com/fwlink/?LinkId=200589

SharePoint Server 2010 Governance Resource Center
http://go.microsoft.com/fwlink/?LinkId=200590

References for more information

Links/Videos/Webcasts, Training:

Getting Started with SharePoint Server 2010 for IT Pros

SharePoint 2010 Advanced IT Professional Training

Security and protection for SharePoint Server 2010

TechNet Virtual Labs (over 30, 90 minute labs):
Summary and Wrap-up

- What is SharePoint?
- What are the challenges presented by Deploying and Maintaining SharePoint?
- What is a SharePoint governance plan?
- What is CobIT?
- How CobIT can be used to deploy and govern SharePoint 2010?
- Getting Started/Best Practices
- Tools & Resources
- Q&A

Q&A?