Security Governance Best Practices for SharePoint 2013 & Office 365 | SharePoint Online

By Errin O'Connor posted Aug 28, 2014 8:47 AM

Options Dropdown

0 Recommend

Security Governance Best Practices for SharePoint 2013 & Office 365 | SharePoint Online

EPC Group understands that security has never been a hotter topic in IT, but in most cases, even though it is being discussed by members of the organization and dominates a good deal of technology news coverage, it is still often not properly addressed in many SharePoint deployments.

In many SharePoint deployments, the organization's Active Directory (AD) deployment may have a good deal of duplication, custom groups, or old and expired information that have been created and stored over many years.

Implementing a best practices SharePoint security strategy requires in-depth planning and knowledge of the overall information architecture (IA) design as well as an understanding and awareness of the capabilities available.

The members of your organization's project team may be security experts but not necessary SharePoint security experts so there must be knowledge transfer, demos, and conversations around its capabilities to ensure all team members are on the same page.

It is important to not only understand what SharePoint's security can do as well as what it may not be able to do out-of-the-box to meet specific or custom requests.

Protecting the content and intellectual property that is stored within SharePoint 2013 and/or Office 365 should be the number one goal of the project. Your organization's intellectual property is what drives your business as well as what give you a competitive advantage.

Depending on the type of organization and business sector you are in there are a variety of regulations and compliance laws that you may be subject to so implementing a SharePoint security model that will ensure a reduced or zero liability footprint is key.

Understanding the granular details of the compliance framework and granular requirements faced by your business, as detailed in the image below, is key to designing your SharePoint security roadmap.

For example, if your organization is in the health care sector, you know that you are subject to HIPAA, PHI, and PII regulations but what about the newly enacted laws around HIPAA HITECH?

There are a wide range of laws, compliance regulations, and related security considerations that you must be aware of to avoid compliance violations, fines, sanctions and any possible reputation impacts that your company could entail in facing these issues.

The following are high-level examples of security considerations and corresponding scenario implications:

Intellectual Property

- New product release information, loss of competitive advantage, loss of marketing message or related efforts

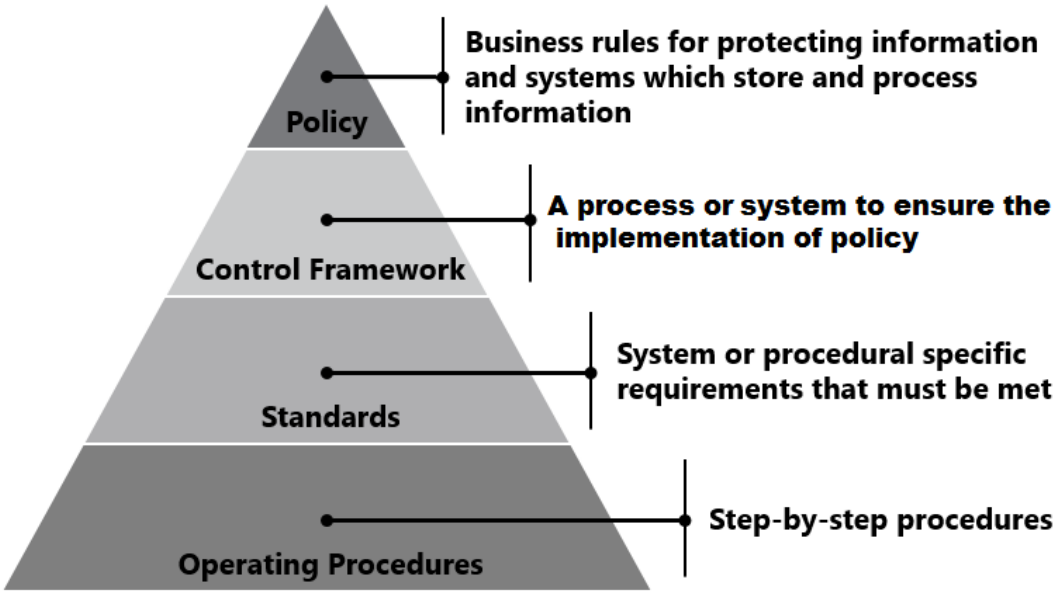
Public Health

- Health records, insurance fraud, etc.

Public Safety or Deployment Success

- Protect classified or sensitive information and mission plans

Overview of EPC Group's Compliance Management Framework



EPC Group's Permissions Management Strategy

When implementing your permission management strategy there are some core standards you can begin with such as ensuring that the accounts running services:

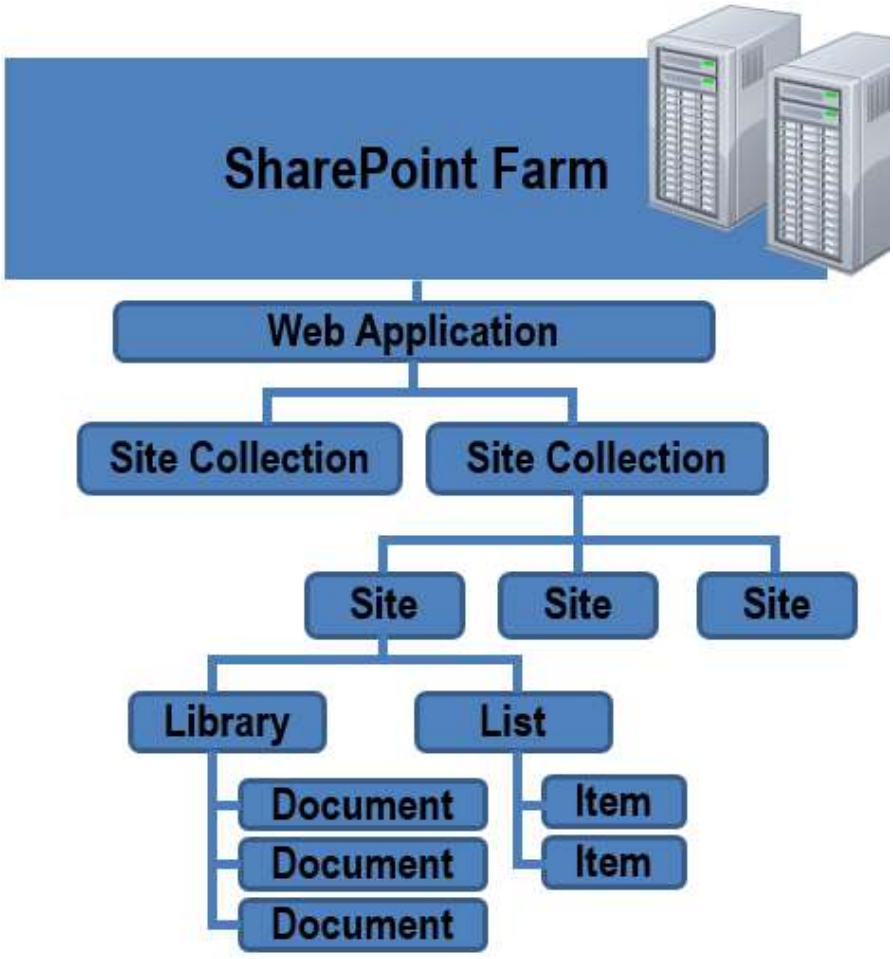
- Should be Active Directory (AD) domain accounts
- Should not be personal administration accounts
- The is a central email account configured for all managed accounts

In most cases, the organization's employees and contractors with existing Active Directory accounts will be granted access to the appropriate SharePoint Site Collection, Sites, Lists and Libraries, as shown in the image below, using the employees' AD account and password.

User permissions and related permission policies should be implemented as follows:

- User Permissions
- Permissions available within permission levels at site collection level
- Permission Policies
- Define groups of permissions (similar to permission levels)
- Only place with a "Deny" capability (i.e. default: deny write, deny all)
- User Policies
- Assign permission policies to users and groups for the entire web app (i.e. Deny group from deleting items within an entire web app – applicable to public facing web app)
- User access will be also be managed through the use of SharePoint groups
- Permissions will not be directly assigned to either Active Directory groups or individual user accounts
- A combination of Active Directory groups and individual user accounts will be utilized as appropriate for individual and specific situations and added to the SharePoint group to control permissions

Overview of SharePoint's Hierarchical Architecture



Requests to access specific Site Collections should be made through the Site Collection Administrators through a built-in access request function.

Access to specific Sites is controlled by the Primary Site Owner as determined via the Site Access Request setting and handled through the built-in Access Request function.

This practice is designed to provide the greatest flexibility and ease of management for security, content targeting, and communication.

Office 365 Compliance & Standards

In planning you organization's Office 365's security roadmap, it is key to take into consideration its published compliance and related standards as detailed below:

Category	Certification	Audience
International Standards and Controls	ISO 27001	All Customer
	Data Processing Agreement	
	SSAE 16 (Statement on standards for Attestation Engagement)	
	SOC 1 (Type I & Type II) compliance	
Industry Specific Compliance & Standards	FISMA	US Government
	HIPAA/BAA	Healthcare Customers
	FERPA	EDU Customers
Geography Specific Standards	EU Safe Harbor	EU Customers
	EU Model Clauses	

SharePoint & Office 365 Governance "From the Consulting Trenches"

I will continue EPC Group's SharePoint & Office 365 Governance blog series in the weeks to come to touch on the real-world "from the consulting trenches" approach that EPC Group has successfully implemented for hundreds of organizations throughout North America.

As detailed in EPC Group's new book "SharePoint 2013 Field Guide: Advice from the Consulting Trenches"