COLLABORATION AND CONTENT STRATEGIES

Methodologies and Best Practices

burton GROUP™

Website Governance:
Guidance for Portals, SharePoint, and Intranets

v1, March 16, 2009

AUTHOR:
   Craig Roth
   (croth@burtongroup.com)

TECHNOLOGY THREAD:
   Collaboration

Publishing Information

Burton Group is a research and consulting firm specializing in network and applications infrastructure technologies. Burton works to catalyze change and progress in the network computing industry through interaction with leading vendors and users. Publication headquarters, marketing, and sales offices are located at:

If you do not have a license to Burton's *Collaboration and Content Strategies* service and are interested in receiving information about becoming a subscriber, please contact Burton.

Table of Contents

Introduction

Few concepts have generated as much interest to website and portal owners as governance. Unfortunately, few concepts have been as misused as well. Governance has been viewed as a project, a document, a synonym for "maintenance," and a magic-bullet solution for website pain. But governance is none of those things. Website governance is a process that uses people, policy, and process to resolve ambiguity, manage short- and long-range goals, and mitigate conflict within an organization. Organizations instantiate website governance because a well-governed site is more likely to be cost-effective, achieve the critical mass of users and information exchange necessary to sustain network effects, align with architectural principles (e.g., single vendor or best of breed, Java or . NET centricity), and meet the needs for which it was designed.

Lack of governance is at the heart of many forms of website pain, including:

- **Dysfunctional internal competition among similar information sharing and communication mechanisms:** When employees have multiple choices for their homepage and multiple places they can have a discussion, post a document, or perform searches, all of the technologies will struggle to achieve a critical mass of users. For example, if an organization has SAP Portal, Oracle Portal, and Microsoft SharePoint, where should a user post a particular discussion or document?
- **Difficulty finding information across sites:** When common navigation, metadata, categorization, and design do not exist across sites, users who need to work across them may miss important information or waste time trying to find it. Unfortunately, the type of employees who most often need to work across website silos are highly valuable information workers: executives, program managers, team members of complex cross-functional projects, and those interested in horizontal issues such as security.
- **Wasted investments in time and software:** Hard cost (i.e., actual impact to margin) losses can result when investments are optimized at the departmental rather than enterprise level. Overlapping web-based information systems may be a conscious choice based upon architectural principles (e.g., time-to-market or best-of-breed preference) or business structure (e.g., fully autonomous business units), but should not be the result of careless, ungoverned decisions.
- **Interpersonal conflict that can fester and impair other endeavors:** Arguments between website owners may become heated and participants may dig into their positions.
- **Posting of abusive, frivolous, offensive, and possibly legally actionable information:** Inappropriate or time-consuming uses of web information resources can spread without clear usage policies.

All but the smallest websites benefit from governance, although intranets tend to be the most chaotic. This chaos comes from the tendency of ungoverned intranets to lack formal ownership, grow organically, have minimal business involvement, and have internal competition with other information sources. By contrast, extranet and Internet websites tend to be more controlled in terms of ownership, direction, and funding because the organization recognizes that websites are their public face to the world. For more information about the evolving role of intranets, read the upcoming *Collaboration and Content Strategies* overview "Making Smart Choices for Online Workplaces."

4

Website governance is just as important—if not more so—when portal technology and concepts are applied. Portals are a form of website that marries a set of back-end integration and front-end delivery capabilities that provide information in context, personalized to a user's role and needs. For more information on the role of portals, read the *Collaboration and Content Strategies* overview "[Communication and Collaboration in Portals: Half the Battle](#)." While the expense of portals and the presence of administration and policy-management tools can help enforce some governance processes, portal implementers have reported continuing difficulties with "portal proliferation." The portal proliferation problem occurs when multiple, competing portals that are built on siloed architectures spring up in organizations. This problem has gotten worse as portal technology has become embedded in superplatforms, such as those from IBM, Microsoft, Oracle (which currently offers four separate portal-related products), and SAP. This embedding sets up more conflicts among competing portal solutions. Also, a lack of focus on the day-to-day roles involved in the care and feeding of portals causes too many of them to wither and die out.

One reason for a resurgence of interest in website governance is the proliferation of Microsoft SharePoint. SharePoint, whether in the form of Windows SharePoint Services (WSS) 3.0 alone or together with Microsoft Office SharePoint Server, has enjoyed strong adoption since its 2007 release. But SharePoint has proven to be particularly vulnerable to chaos when ungoverned for these reasons:

- **Ease of deployment:** Because SharePoint is easier to license and install than other portal products, more parts of the organization are tempted to set up servers. Decentralized installation and setup of the servers often leads to siloed installations that do not conform to the organization's best practices or technology standards.
- **Grass-roots nature:** SharePoint's ease of use has proven to be a double-edged sword. Although it opens up self-help collaboration and content capabilities for a broader swath of information workers, it also places creation in the hands of a large number of non-IT users who are minimally monitored. This can lead to poor findability and an inconsistent user experience.
- **Lack of multifarm management:** SharePoint lacks enterprise-wide management features that other portal products have had for years. The highest level of management in SharePoint is the server farm, but enterprises wanting unified policies and governance across multiple server farms have few tools to accomplish this. Microsoft has made a step to remedy this situation with its [Cross-Site Configurator](#), which was specifically developed "in the context of IT management challenges that have arisen with the rapid growth of SharePoint deployments." However, this product is unsupported sample code, not a part of the official WSS build.
- **Frequent overlaps with other installed capabilities:** SharePoint provides an integrated set of capabilities that often exist in separate products an organization may already have installed. A team that has been overseeing a content management, search, collaboration, or portal system for years may wake up one day to find users starting to leverage SharePoint for the same capabilities. The result is information segregation and a quick call to the chief information officer (CIO) to determine whether to shut down one of the overlapping alternatives or to let them coexist.

5

These problems can arise whether SharePoint is deployed as an intranet, a portal, or just leveraging one of its capabilities (e.g., document management, reporting center, and collaboration workspace). For more information about portals built in SharePoint, read the *Collaboration and Content Strategies* report "[Building Portals in SharePoint 2007](#)."

Although some intranets and portals rise above all these problems, it is rare and difficult for them to do so without a governance structure in place. This *Collaboration and Content Strategies* Methodologies and Best Practices (MBP) document will provide a methodology for putting together a governance structure, as embodied in a statement of governance (SOG). This methodology applies equally well to websites, portals, and SharePoint because the governance drivers and steps are similar in each case. Differences will be pointed out and examples will be used where applicable. Henceforth, we will generically refer to the governance as "website governance" and the document as a "website SOG" or "SOG."

Definitions

Before diving into how to create a SOG, it is worth defining some of the terms that will be used. This section will provide definitions of governance, compliance, decentralization, centralization, and federation as well as context that explains their importance in a SOG.

Website Governance: It's Important, but What Is It?

The most common question about website governance is "what is website governance?" Management and website owners have heard the term applied in other areas and get the general idea that it involves smoothing out issues above the technical level that often get overlooked, such as goals and ownership. But definitions vary greatly and seem to encompass everything from management to operations.

In the worst cases, website governance is narrowly defined as one specific task or element of the overall governance picture. For example, a one-page organization chart for a portal's ownership and maintenance may have the title "Governance Plan for Portal XYZ" slapped on it. The danger of narrowly defining governance is that those with the task of instantiating it for the portal will consider the job complete even though a slew of other governance issues remain unaddressed.

Burton Group's definition of governance as applied to websites is:

> *Website governance* uses people, policy, and process to resolve ambiguity, manage short- and long-range goals, and mitigate conflict within an organization.

Each portion of this definition serves a purpose in ensuring the smooth operation of the website:

- **"People, policy, and process":** These are the tools used to ensure governance of the website. This list is important for the three items it mentions as well as for all of the items it

intentionally leaves out, as will be described in the "[Walking Through the Statement of Governance](#)" and "[What Website Governance Is Not](#)" sections of this MBP document.

- **"Resolve ambiguity":** Without governance in place, unspoken rules and assumptions about goals guide website development teams. Getting these unspoken rules and assumptions into the open and having management clarify them will help get all of the website stakeholders marching in the same direction.
- **"Manage short- and long-range goals":** Website governance optimizes for the organization as a whole rather than for the ease, cost, or expediency of individual projects. The difficulty of persuading website owners to take a longer or more difficult road than needed to meet their specific goals is one reason executive buy-in is so important for a SOG.
- **"Mitigate conflict":** A major value proposition for governance is that it helps to pre-decide who wins in arguments before they come to a head. For example, determining whether research and development (R&D) teams should set up RandD discussion groups in a new SharePoint installation or use the existing portal may be a painless intellectual discussion before the SharePoint roll out. However, it can turn into a battle royale if the website owners wait until a year after the roll out. By then, users and management will have a stake in one system or the other and may refuse to move.

Compliance: The Pointy End of Governance

Once an organization establishes the need to create a SOG, it should give thought as to how it will measure and enforce governance. A SOG that is not going to be followed up on is nothing more than a stack of paper or a webpage. The term for this measurement and enforcement is "compliance." Burton Group defines compliance rather simply:

Compliance is a process used to assure that governance is being followed.

The term "compliance" often brings up visions of enforcement committees and approvals. Sometimes these are indeed a part of compliance, but they are not the only methods to monitor and encourage compliance. Benchmarking and measurement help to monitor compliance (see the "[Measurements](#)" section of this MBP document) and need to be a part of any website governance, even if triggers and punitive actions are not detailed in the SOG. Humans, being social creatures, can be steered away from noncompliance through social enforcement rather than central control. Peer pressure (e.g., circulating measurements to a peer group or discussing poor performance in group meetings) is a highly effective form of compliance. For social enforcement to be effective, socialization of the SOG must occur so that a common understanding of its precepts and importance will guide group practices.

Decentralization, Centralization, and Federation: The Governance Model Continuum

Before starting to author a SOG, the website owner should determine how much freedom individual website owners should have and how much control the central authority should retain. There is a continuum of governance models that ranges from the "Wild West" of decentralization to the locked-down, authoritarian rule of centralization (see Figure 1).
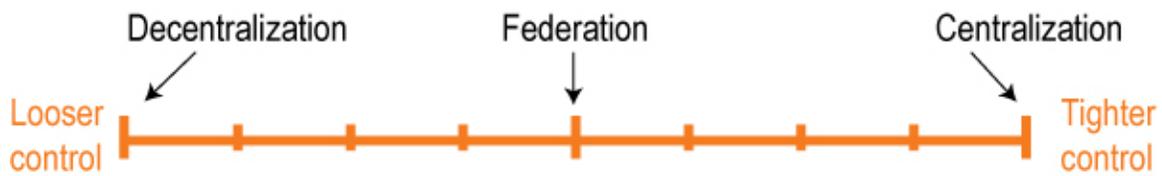
Figure 1: *The Governance Model Continuum*

Here are more formal definitions for these three common governance types:

- *Decentralization* is a form of governance in which groups in an organization are free to make their own decisions without regard for decisions made by other groups.
- *Centralization* is a form of governance in which a single, central authority makes decisions for all subgroups in an organization.
- *Federation* is a form of governance in which groups in an organization recognize a central group's right to set high-level policy but retain the freedom to make their own decisions within the bounds of that policy.

Although there is no "best" approach in general, federated website governance seems to have the most success. Organizations accomplish this by setting the boundaries within which the site owners have freedom. For example, an organization with a divisional organization structure may dictate that all divisional websites have common navigation, look and feel, and search, but that those sites are free to use any technologies or products within those bounds.

It is important to take the organization's current place on the spectrum into consideration. For example, an organization whose culture and organizational structure has traditionally emphasized significant autonomy for business units will have more success picking a point on the continuum that is closer to the decentralized end of the spectrum. For more information on moving an organization's placement on the continuum over time, see the "Timelines" section of this MBP document.

For many organizations, their place on the continuum acts like a pendulum, swinging between decentralized autonomy and tight control before settling on a federation point somewhere in between.

What Website Governance Is Not

Getting people to agree on all the good stuff that should go into a SOG is not difficult. Most reasonable stakeholders understand that business goals are important, organizational structures should be clear, and policies should be written down somewhere. But it is difficult to get proponents to clearly spell out what is *not* part of website governance. After all, there are few chances that website owners get to formally communicate with executives and website stakeholders, so it takes restraint to pass up an opportunity to throw everything into the SOG and pass it out with a CxO's blessing. Still, a SOG is much more effective if it keeps a laser-like focus on people, policy, and high-level processes.

Accordingly, a website SOG is not the same as a maintenance manual, information architecture, a list of approved technologies and standards, or a provisioning procedures manual. Although it may seem harmless to include those items in a SOG, there are four good reasons not to:

1. The modification pace of these documents differs. For example, including maintenance processes within the SOG anchors that section to the slower release cycle of the SOG. As another example, approved technologies will change continually throughout the year while the SOG might change only once a year.
2. The audiences for these documents differ. Business stakeholders and executives will not want to read a SOG that is heavy with procedures on how to delete users or sync repositories. Likewise, technicians may yawn at high-level business goals and details of organization structures and committees when all they want is a list of approved standards. The main audience for the SOG is owners of websites and portals, including the business owner and his/her IT partner. The secondary audience goes up the chain (to executives) and down the chain (to designers and developers). Accordingly, IT professionals are a secondary audience and will need their own detailed documents separate from the SOG.
3. The authority of the SOG derives from executive buy-in, which will be difficult to obtain with low-level details. If these details are present, no one will believe the chief executive officer (CEO) signed off on, for example, which host server is the single source of truth for the taxonomy and its replication schedule to other server farms. And the CEO may not want to sign off on details he/she does not understand.
4. Those items are full documents of their own and are distractions to covering people, policy and process. When they are present, it is generally at the expense of a focus on people, policy, and process, which will need to be addressed at some point anyway.

The SOG offers a framework of people, policy, and process that other documents (e.g., a maintenance manual or an information architecture guide) can fit into. Accordingly, the SOG helps to ensure the success of these other documents, but their details belong in a separate place. Admittedly, this guideline sometimes gets fudged a bit, which is where the appendices can provide a useful but separate place for some details (see the "Appendices" section of this MBP document).

A higher level than the website SOG may also provide guidance. Where there exists IT governance, enterprise architecture, or business policy statements, the SOG should connect upward to fit into those documents. This hierarchy of documents, from higher-level guidance to the website SOG to detailed technical documents, is illustrated in Figure 2.
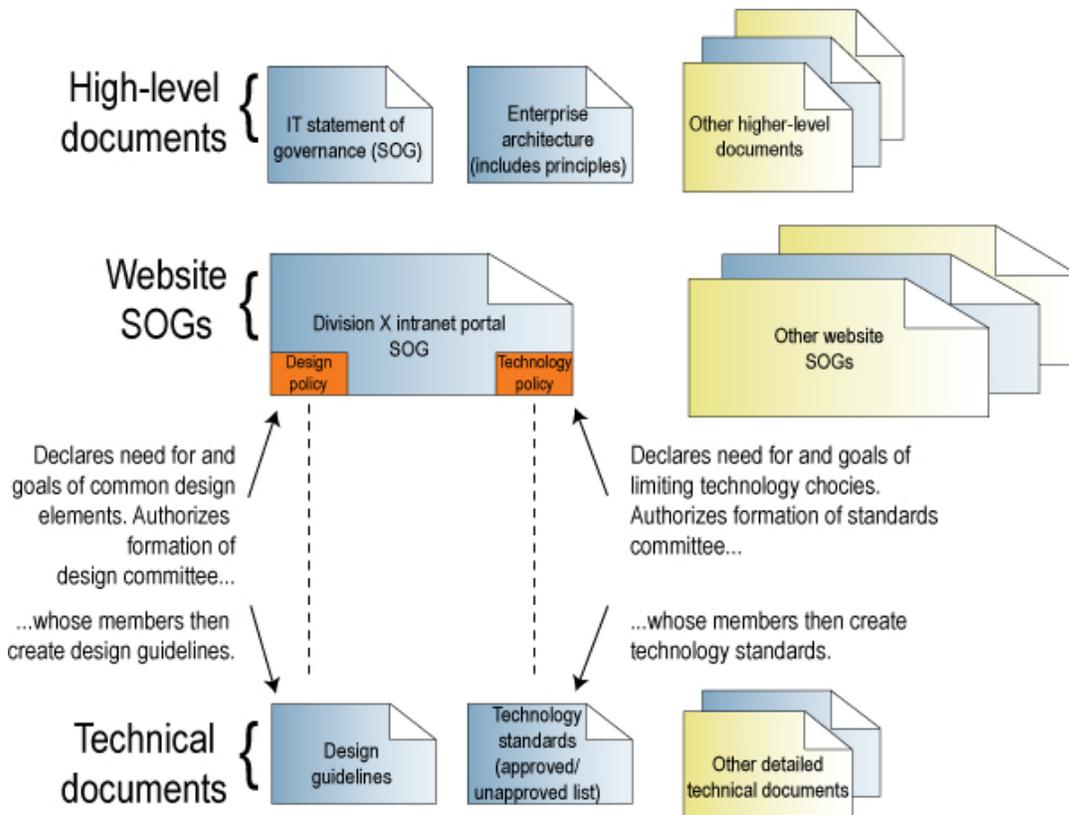
Figure 2: *Document Relationship Hierarchy Example*

Walking Through the Statement of Governance

Once the purpose of the statement of governance (SOG) is clear and the basic terms are understood, it is time to begin writing. As stated in our definition of governance (see the "Website Governance: It's Important, but What Is It?" section of this MBP document), the SOG should focus on people, policy, and process. Accordingly, those are the core sections of the SOG with a few other sections bookending that core. The template we recommend is as follows:

Statement of Governance
   I.   Introduction
  II.   People
 III.   Policy
 IV.   Process
  V.   Measurements
 VI.   Timelines
    A. Appendices

Introduction

The introduction of the SOG should level-set the reader on what is being governed (scope) and what it is trying to achieve (problem statement).

Scope

Even though this MBP document is generically referring to "website governance," using that exact title for an actual SOG would beg the questions, "Does the authority of this document extend to all websites? Internal and external? Every division and department?" A similar question could pertain to a generic portal or SharePoint SOG as well. Therefore, a SOG should specify up front the domains it covers.

The SOG should also specify the intended audience.

Problem Statement

The maxim "art for art's sake" makes a strong statement that art is a worthwhile endeavor even without any practical application, but governance for the sake of governance is truly useless. The introduction must include a problem statement that succinctly describes what problem the SOG is trying to address. This statement ties the SOG to business values and drives the rest of the document.

The problem statement can be worded from a positive standpoint, a negative standpoint, or a combination of the two according to the needs of the situation and the best motivational strategy for the enterprise culture. A positive problem statement describes the high-level, positive outcome the SOG is trying to achieve. Examples of positive problem statements include "improving employee productivity and satisfaction," "projecting a more consistent brand image across our websites," and "reducing costs" (or, to tie more specifically to stated business objectives, "contribute to the stated financial goal of reducing core IT operating expenses by 18% by FY2011").

A negative problem statement describes negative impacts that are occurring today or that are to be avoided. Examples of negative problem statements include "avoid redundant purchases of portal products," "reduce the difficulty and confusion employees face when navigating our websites," and "reduce the inconsistency and chaos caused by the 800 SharePoint sites currently deployed." Negative problem statements are effective when tied to recognized pain points.

One client required this section to be described in terms of the "current view of the situation" and the "better view of the situation." This approach worked quite nicely, and can span both positive and negative problem statements.

People

Clarifying the roles involved in a website addresses both the "resolve ambiguity" and "mitigate conflict" components of the website governance definition (see the "Website Governance: It's

Important, but What Is It?" section of this MBP document). Ambiguous authority is dangerous whether it takes the form of two people believing they have decision rights for the same task or nobody stepping up to a task, which leads to a task falling through the cracks. Conflict can result from ambiguous authority, at which point arguments that should be resolved on their business and technological merits become personal instead. Settling these issues before they come to a head is the goal of the people section of the SOG.

The people section lays out the scope of authority for all of the key roles involved in the website. There is no single "right" answer for which boxes on the org chart should accommodate each role. The decisions are influenced by several factors:

- Historical attempts at governance, for websites or other technologies, can suggest how the roles can best be filled. Successful past governance plans can be duplicated, and unsuccessful ones provide cautionary guidance.
- An organization's place on the governance model continuum will help determine which roles should be filled centrally and which should be parceled out to individual site owners.
- Roles involving significant buy-in or expense may be skewed toward parts of the organization where the most pain is being felt due to website sprawl and chaos. Ideally, all potential benefactors of the governance would be equally involved. However, from a practical standpoint, it can be difficult to involve departments that see governance as a solution to a problem they don't have.
- Even when pain is not a driver, some individuals and portions of an organization are more enlightened about the benefits of governance and will step forward more quickly. It is prudent to take advantage of this buy-in wherever it exists.
- The maturity of the organization and level of grass-roots interest may suggest a community-building effort is appropriate, such as birds-of-a-feather (BOF) groups, special-interest groups, or communities of practice.

Whatever approach is used to fill the governance roles, the process should be fair, open, and as inclusive of the whole organization as possible. Invitations should be sent to all relevant parts of the organization, and higher-level positions should rotate among members.

Plan on different roles for initial planning versus ongoing operations. Generally, more intensive work is required up front when websites are first organized, which yields to a less intensive set of ongoing roles to handle occasional duties or monitoring as operations reach a steady state. Additionally, if some areas are underrepresented in the initial bootstrapping efforts because they do not feel governance pain or do not buy into the governance process at first, plan to revisit their participation at a later time when the benefits of governance are more apparent.

Roles

The following is a list of common roles that should be defined for website governance. Every situation is different, but this list provides a good starting point:

- **Governance committee:** The governance committee guides the efforts to create the SOG and divvies up the tasks for recruiting resources, explaining the governance effort to each part of the organization, and campaigning for buy-in. In larger organizations there may be a governance steering committee as an offshoot of the IT steering committee, and any number of working groups where designates of the steering-committee members tackle more detailed issues such as taxonomy, design, reporting, or development models:
  - Governance steering committee
  - Governance working groups

- **Executives:** The authority of the SOG—its ability to pre-decide who wins in arguments—comes from the preemptive support of the CxO executive for the organizational structure, policies, and processes it describes. There are three critical roles that may exist in one person, although they are separated here for clarity:
  - Approver (CxO)
  - Champion (executive)
  - Sponsor (financial)

- **Owner:** It is best if one person is in charge of the website and responsible for its function, but at times there are business and IT co-owners. If there is one person in charge, traditionally that owner resides in IT, given the understanding of website creation and provisioning processes required:
  - The single person (or IT and business co-owners) in charge of and responsible for the website (including compliance unless delegated)

- **Resources:** The SOG should notify people who have been targeted as necessary for the website effort, whether dedicated to the project or just borrowed as needed from other teams. This list also serves as a chance for people excluded from the list to petition for inclusion if desired:
  - IT personnel responsible for infrastructure, architecture, and contingency planning
  - Developers and designers of the website infrastructure
  - Content management, search, and taxonomy personnel
  - Support and training personnel
  - Information managers/corporate librarians
  - Security architects

- **Stakeholders:** The term "stakeholders" includes everyone previously mentioned in this list as well as representative users and website developers:
  - Users
  - Developers of new websites covered by the SOG

Policy

Once the people involved in website governance have been determined, attention can turn to defining website policy. The policy section of the SOG is like a constitution for the website—it lays out intentions and direction that processes will attach to. Properly written governance policies should

address the question "why?" Rather than simply dumping a set of processes onto website owners and users, the organization should explain why the processes are important and how they connect to enterprise goals. Accordingly, the policies will grant authority and justification for the governance processes in the next section.

Another reason to take the time to describe the policies driving website processes is to indicate the "spirit of the law," so overall policy can guide situations not captured by written processes. Some organizations fall into the trap of trying to write detailed procedures within processes to cover every possible situation and loophole they can think of. But it is impossible to cover every possible situation with processes, so why try? With policies in place, even cases not covered by processes can be handled in a manner that is compliant with the overall website policy.

Even though use, design, and information-security policies exist in most website SOGs, each organization designs additional policies to address its needs and business-stakeholder concerns. Table 1 lists a set of policies often present in a website SOG. The author of a SOG needs to make policies actionable rather than simply a set of statements that get head-nodding agreement. Accordingly, the "Application" column describes how each policy will be used to spawn a set of processes, launch a committee, justify creation of a related document, or spark a set of conversations. If a policy will not have any processes attached to it or act as the impetus for other concrete action, it does not belong in the SOG because "fluffy" statements water down the authority and effectiveness of the website's governance.

Policy	Purpose	Application
Business risk policy	Prevent potential channel conflicts, legal issues, damage to brand image, and other impacts that could be caused by information sharing with external parties	Supports the need for risk to the business and risk to customers/partners to be mitigated. Used to facilitate regular conversations with business partners about channel risks
Design policy	Define standard themes, navigation, accessibility requirements, and controls for consistent user experience	Establishes principles to support common navigation and "look and feel." Describes design freedom site owners have. Provides basis to form design committee which, in turn, creates guidance

Financial policy	Scope website capabilities and service level to fit within the financial expectations of its sponsors	Provides expectations for where funding will come from (e.g., centralized or decentralized) and forms basis for chargeback processes
Information management policy	Improve findability by defining navigation, categorization, taxonomy, ageing, and metadata	Provides basis to enlist information architects, design information management architecture, purchase/implement related technologies, and enforce compliance
Information security policy	Provide a framework and processes to identify threats, vulnerabilities, and consequences with regard to website information	Describes the need for the business to create a document that defines threats and vulnerabilities along with the recommended mitigation of such threats, audit procedures, and resolution responses
Technology policy	Constrain the technology choices for portal, content management, BI, search, forms, and collaboration	Supports the need for a standard set of web technology. Provides basis for technology and standards selection committees who will then publish a (separate) document with approved, preferred, and unapproved options for each capability
Use policy	Define what constitutes abuse or misuse of the website	Provides clear instruction on how and when users should work with the website. Establishes justification for future action and defense via a mix of up-front warnings and human monitoring, compliance process, and violation process

Table 1: *Website Governance Policies*

Process

Just as policies answer the question "why?" processes answer the question "how?" for each policy. Each policy should have one or more processes defined. But the key to a long-lasting, workable SOG is to find the right level and type of processes to include. Details on all the website processes the author can think of could span hundreds of pages, rendering the SOG into an imposing procedure manual with a slim veneer of people and policy.

So which processes should be defined in the SOG? This is where the "resolve ambiguity" part of the [governance definition](#) comes into play. Think about the high-level questions site owners would ask and guide them with processes so that they don't make up answers that meet only narrow, short-term goals. It may be sufficient to describe a policy in the SOG and point to another document that provides the step-by-step instructions. For example, consider an organization with a design policy that restricts page design to enable better usability across websites. A design-review process beneath that policy might describe a set of approved reviewers that validate the design of new departmental homepages (but not each page within a new departmental site). For the details on how that review is done, the SOG may simply point to another document dedicated to the website design standards and procedures.

The following is an example of how processes may be created to drill down into each policy and answer the question "how?":

- Use policy:
    - Designation of compliance officers
    - Regular spot checks for inappropriate postings in discussion forums and document repositories
    - Compliance policy: three-strikes rule

- Design policy:
    - Compliance reporting procedures
    - Link to design committee's site detailing standards

- Technology policy:
    - Procedures for architectural reviews
    - Submission of exception requests
    - Link to list of approved, preferred, and unapproved technologies

Of course, not every process should be defined. The term "practices" is often used to describe the way people do things, with the implication that "the way things are done" is not necessarily defined, written, or repeatable. Information workers retain significant amounts of autonomy for myriad reasons, including job satisfaction, accommodating different personalities and situations, and because their work may not be repeatable. In fact, a [McKinsey study](#) showed increasing levels of tacit (undefined) processes in developed economies. Efforts to turn tacit work into transactional work by defining strict repeatable processes for them will be resisted or fail in many instances. Continuing the design-review example, management may decide it's best not to strictly define the procedures that the design reviews follow in order to allow for autonomy and flexibility by those designated as design experts.

Measurements

In the previous section, [processes](#) were defined to ensure that [policies](#) are actionable. In this section, those processes are attached to measurements to ensure that action is taken. In fact, understanding

which actions will be taken based on the measurements can guide the creation of processes and policies. Too many SOGs are ignored or fail to achieve the goals they were created to address. Setting forth policies and processes without any sort of follow-up or measurements creates a bad first impression by indicating a lack of seriousness about governance.

Figuring out what to measure can be challenging. Accurate—but useless—metrics abound from web servers and log files. But measuring against business objectives is more useful. We recommend approaching measurement at two levels: measuring compliance and the effects of compliance. Compliance measurements are generally found by drilling down on processes, and measuring the effects of compliance is generally accomplished by drilling down on policies.

Measuring Compliance

Measuring compliance generally involves attaching accumulators to processes, such as automated counters or manual tallies. The positive aspects of a process can be measured by tracking process iterations over time. The idea is to tabulate how often the approved process has been executed (grouped by categories as necessary, such as by department or content type) to show increasing application of the governance process over time. The negative aspects of a process are measured as the decreasing instances of problems caused by noncompliance, measured over time.

As an example, consider the first set of sample processes from the "Process" section of this MBP document that derive from the use policy (see Table 2).

Policy	Process	Compliance measurement
Use policy	Designation of compliance officers	None. This process is possible to measure (e.g., number of officers or how long they have been on rotation), but measurement is probably not necessary
	Regular spot checks for inappropriate postings in discussion forums and document repositories	A tally kept by compliance officers of the number of inappropriate postings they have found (a negative measure of noncompliance) versus the total number they've checked (a positive measure of iterations)
	Compliance policy: three-strikes rule	A tally kept by human resources of the number of employees that have had three flagged postings

Table 2: *Compliance Measurement Sample*

Measuring the Effects of Compliance

Simply treating execution of designated processes as success is short-sighted. Each process is supposed to drive a positive result as defined by the policy it is attached to. Therefore, measuring whether higher-level goals are being met often requires figuring out how to measure policies. For each policy, consider how its effect would be observed and determine the best method to extract those observations. The answer usually lies in conducting surveys or polling rather than automated counters.

To continue with the same example, consider the use policy that the previous processes connect to (see Table 3).

Policy	Effects of compliance measurement
Use policy	Survey question in annual website satisfaction survey: "Do you feel that the website is free of inappropriate or offensive material?"
	Survey question in annual website satisfaction survey: "Has anyone expressed to you that they were offended by material on the website?"
	A tally kept by human resources of the number of formal complaints and legal actions filed by employees
	A tally kept by the legal department of the total dollars paid out in "hostile workplace" fines and settlements due to inappropriate or offensive material on the website

Table 3: *Effects of Compliance Measurement Sample*

It should be noted that there are many other measurements needed for a website to succeed other than those related to governance. Administrators may need information about how workload is being distributed across servers, hit counts, and free disk space, but these statistics do not directly relate to the goals in the SOG, so they belong in separate documents.

As a final comment on measurements, the importance of capturing pre-governance internal benchmarks—both for compliance and the effects of compliance—cannot be overstated. Without accurate measurements of how things were before the SOG went into effect, it will never be possible to demonstrate the total impact it has. Benchmarking for policies, probably through surveys, is particularly important because historical data on attitudes will be difficult to capture later.

Timelines

The timelines section contains a roll out schedule for the website governance. This may seem like a simple detail, but there is actually a deeper concept at work here: Governance doesn't happen overnight. Conceiving of an ideal state of how people, policy, and process would work for a website is easier than figuring out how to get there. Not only is creating an ideal-state document that goes into

effect tomorrow inadvisable, it can actually be harmful. Each failed attempt at governance makes the next attempt more difficult because workers become trained to ignore governance efforts or just wait them out.

The SOG should not be written in such a way that the day after it is released, most website owners are in violation of it. Once those noncompliant website owners survive to face day two, they will notice that no corrective action took place, so they may as well wait. Instead, publish a schedule of when new processes will take effect and desired metrics over time. The SOG may phase in the governance by department or type of website. The goal is to slowly decrease the degree of variance present in the environment compared with the ideal state (see Figure 3). This approach allows management to take a portfolio approach (based on an inventory of all websites in the division) toward the path to full compliance rather than allowing each website owner to decide if and when to comply. Even at the endpoint, there will still be some freedom allowed, but much less than the "anything goes" environment that existed before the SOG.
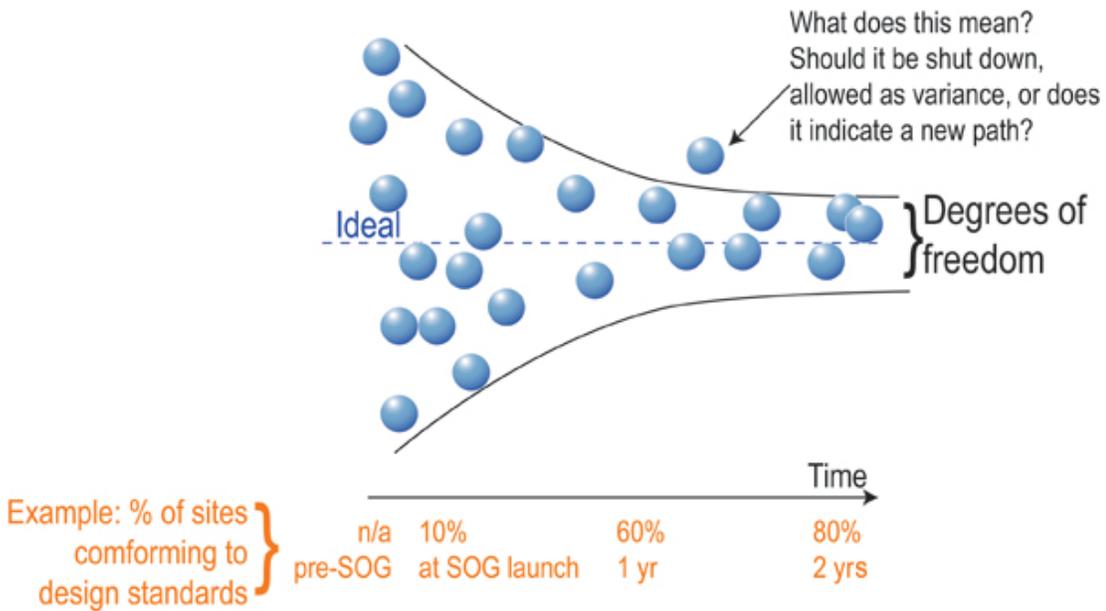

Figure 3: *Governance Doesn't Happen Overnight*

Predetermining how to handle instances that fall outside the bounds of the governance can make the SOG more resilient. For example, the dot shown outside the funnel in Figure 3 may not indicate a failure. This may be an allowable variance, or it could indicate that conditions have changed over the year since the SOG was implemented and therefore the SOG should be modified to allow for different boundaries. The SOG should be approached as a "living document" that is never "done" and, rather, is continually under construction. In many cases, website governance is being implemented in organizations where a culture of conforming to governance does not exist. It is especially important in those cases to adopt governance gradually (two or more years is not uncommon).

The bottom of Figure 3 shows an example of variation being reined in over time. Do not try a quantum jump to the "ideal state" governance level. Instead, determine the current level and concentrate on moving up just to the next step. Also, recognize that the ideal level may not always be "federation"; it could be simply formal cooperation or, if tight control is desired, centralization. The steps in Figure 4 correspond to a typical progression of governance maturity in an organization.
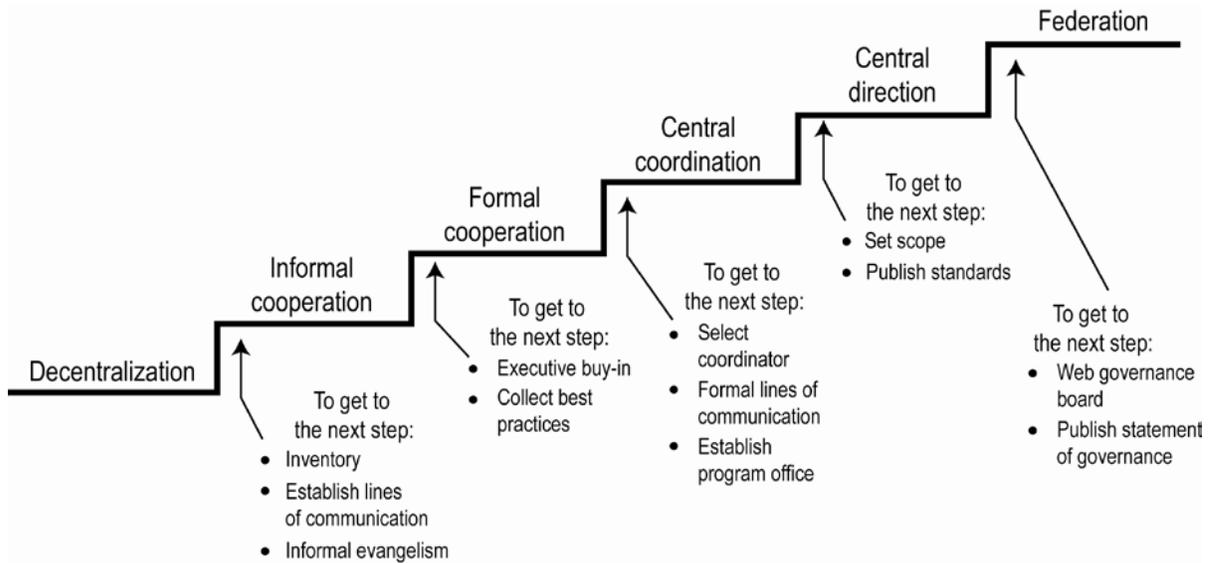

Figure 4: *Website Governance Stepping Stones*

The steps are defined as follows:

- **Decentralization:** This is the "Wild West," where anything goes. There are no rules in place that restrain websites.
- **Informal cooperation:** In the absence of an executive mandate or formal project, interested parties can self-organize an informal community of interest to coordinate projects and exchange best practices. They can actively seek out other members to participate on a voluntary basis, by using the argument that they all have a better chance of achieving their goals if they can learn from each other.
- **Formal cooperation:** Management takes the bare minimum of interest by encouraging all parties working on websites to just "work together." A committee is created with a regular meeting agenda.
- **Central coordination:** A centrally located individual is tasked with coordinating all website efforts in the organization in order to monitor them and help share best practices. The individual does not create or force standards on anyone but helps disseminate information across the organization. This is based on a program-management office structure.
- **Central direction:** A central group sets standards for products and processes and disseminates these standards (though they might have no means of enforcement). Once

central direction is established, an organization can head down one of two paths: centralization, where the central group makes practically all decisions for portal framework and sites; or federation, the more common route in the current IT environment.

- **Federation:** A base level of decisions is made centrally, but each group is free to make many decisions within that structure.

Appendices

Up until this point, we have dictated that the SOG focus on people, policy, and process in order to win credible executive sanction, maintain a reasonable pace rate for the document, and avoid the tendency to overwhelm high-level guidance with low-level administrivia. However, in practice some detailed technical information often gets published as part of the SOG to simplify the approval process and take advantage of the SOG's publishing cycle.

At a minimum, to retain the focus on people, policy, and process, Burton Group recommends putting a minimal amount of low-level detail in appendices at the end of the SOG. Preferably, they are separate websites linked to by the SOG to avoid differences in publication pace rates.

Examples of additional information often attached to SOGs in appendices:

- Parameter lists:
  o Disk or database quotas
  o Aging parameters

- Service level parameters (by tier if desired):
  o Uptime target
  o Response time target
  o Backup history and recovery time

- Cost list:
  o Chargeback costs for various levels of service and features

- Report list:
  o Compliance reports

- Benefits reporting
- Usage reporting and demographics

Top Five Website Governance Pitfalls

This MBP document has focused on the best practices for creating a website SOG. But it is also useful to be aware of common pitfalls that await the SOG author. This section describes the five most common pitfalls in creating website SOGs.

1. Governance Ignored: Document Gathers Dust on Shelves

Ideally, a SOG has a positive measurable impact when it is implemented. But it is not at all uncommon to find even well-written SOGs that are simply ignored. Usually, a principled-sounding SOG gets published, but it is far from what its audience needs. Peers and management don't seem to be discussing the SOG, so its audience ignores it.

How to avoid: This pitfall can be avoided by paying attention to three areas. First is diplomacy. Actively seek out potential dissenters to address their concerns early in the process. For areas whose stance on governance is not known, set up meetings to learn about their needs and potential issues with the governance structure. Second is timelines. Slowly reining in variance over time will have a better chance of avoiding rejection. Third is socialization. Keeping in touch with all stakeholders as the SOG is being created, walking it around in person rather than just publishing it, and constantly eliciting feedback will help build the governance into the social fabric of the organization as well as the organization's formally defined processes.

2. Authors Focus on What They Know

Authors presented with a set of topics to address have a tendency to focus on those they know best. If the author of a website SOG is a portal administrator or developer; this sometimes results in a SOG with a few pages of business-focused pablum followed by dozens of pages of techie administration details.

How to avoid: The website will need information about maintenance procedures, provisioning steps, and coding advice, but these should be separate, dedicated documents. The SOG should focus on people, policy, and process. Make sure the primary author of the document is capable of and dedicated to working with non-IT personnel and stakeholders to identify the organizational structure and policies the website will need. A good rule of thumb is that no more than half of the document should be dedicated to the process section. Finally, asking a wide range of reviewers from numerous roles across the organization to indicate sections they believe are missing or need more detail can identify gaps.

3. "So What?"

"In order to improve the efficiency of workers at Acme, websites on the intranet need to be well-designed and easily navigable." Not many people would disagree with a generic, high-level statement of principle such as this. But a SOG that mostly consists of these kinds of statements leaves readers wondering what to do differently. If the policy statements are not actionable, the SOG may not be vocally protested, but it will not have any effect either. Readers will read the SOG, think "so what?" and go back to their work without remembering anything in it.

How to avoid: Start with defining an actionable problem statement in the introduction. Then make sure to drill down into policy to yield processes that connect to the daily lives of the audience.

4. Writing a Book

If the SOG makes a loud "thud" sound when dropped on the desks of its audience, that's a good sign it is probably too large and not likely to be read. It is not uncommon to see a SOG balloon to 50 pages or more, which delays its publication—assuming it is ever completed at all.

How to avoid: Aim for a target of about 15 to 25 pages. This strict limit can be achieved by focusing on high-level guidance about people, policy, and processes and breaking off large, detailed sections into their own documents with links back to the SOG.

5. Forgetting to Distinguish Initial Bootstrapping from Ongoing Operations

A major new website initiative often places severe and short-lived demands on a limited group of people who are involved in its creation. Once the website is launched and into production, it can soon transition to a steady-state model that incorporates a broader set of existing groups (e.g., helpdesk, operations, and training) to take over maintenance. A SOG that focuses on just one of these two stages will not be useful over the long run. A SOG will be quickly outgrown if it focuses on intensive first-year roles and tasks but not the stable state that follows. Likewise, a SOG should not focus on ongoing governance and the demands of steady-state personnel at the expense of allowing for temporary roles and processes for the initial intensive setup period.

How to avoid: Distinguish between intensive roles needed initially (such as creating an initial taxonomy and defining metadata) from stable-state roles (such as approving taxonomy-change requests and reporting on metadata compliance).

Conclusion

Enterprises use website governance to prevent overlapping technology, to present a consistent interface, and improve findability and shareability. It applies equally well to all major websites, including those created as portals or with Microsoft SharePoint. A statement of governance (SOG) should clarify who owns critical roles, why the organization is implementing governance, and how to comply.

The SOG should be written at a high level, providing a foundation (and links) for other documents that provide more technical details. Ultimately, the journey is the destination when it comes to creating a website SOG, so be prepared to learn during the process.