PORTALGUARD

NIST 800-53 Compliance Guidelines: How PortalGuard Can Help

Tech Brief

v.3.2-001

PistolStar, Inc. dba PortalGuard
PO Box 1226
Amherst, NH 03031 USA

Phone: 603.547.1200
E-mail: sales@portalguard.com
Website: www.portalguard.com

NIST 800-53 Security Controls for Federal IS/O

National Institute of Standards and Technology—August 2009

NIST 800-53 is widely recognized as the benchmark for not only Federal Information Systems and Organizations but it also serves as the foundation for many private sector IS guidelines and procedures.

Because of its all encompassing nature that includes comprehensive guidelines on policy and procedures, training guidelines, facility protection as well systemic requirements we believe there is no single application or platform that can address every component within the guidelines as there are just too many and they are too diverse.

With that said, there are a number of areas that a strong authentication platform like PortalGuard can help you with when it comes to compliance. We strongly believe PortalGuard is able to provide capable, customizable, and cost efficient protection.

To help you understand where we can help we're providing the attached matrices to help you better understand the requirements and to see how PortalGuard can help.

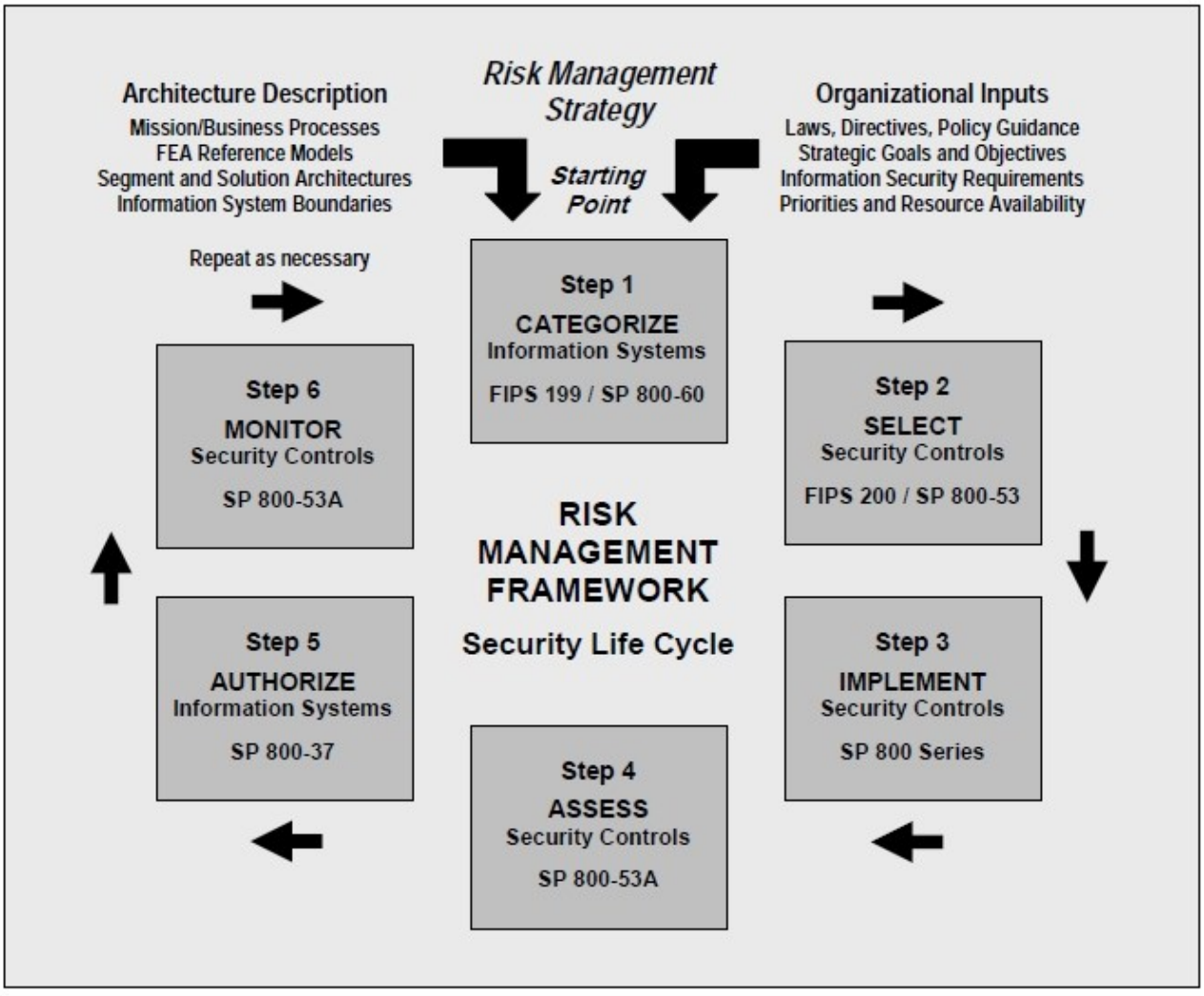

FIGURE 3-1: RISK MANAGEMENT FRAMEWORK

PortalGuard Summary Matrix

NIST 800-53 has 16 unique sub-categories designed to address each component in an in-depth manner. PortalGuard provides one of the strongest authentication platforms in the industry and can help your organization meet and exceed a number of 800-53's requirements. Click on the appropriate control to see the specific controls and how PortalGuard can help.

Group	Name	PortalGuard Feature
AC	Access Control	✓
AU	Audit & Reporting	✓
CA	Security Assessment	✓
CM	Configuration Management	✓
IA	Identification & Authentication	✓
IR	Incident Reporting	✓
RA	Risk Assessment	✓
SC	System & Communication Protection	✓

AC—Access Control

Control No.	Control Description	PortalGuard Feature
AC-2	b. Establishing conditions for group membership; c. Identifying authorized users of the information system and specifying access privileges; d. Requiring appropriate approvals for requests to establish accounts; e. Establishing, activating, modifying, disabling, and removing accounts; i. Granting access to the system based on: (i) a valid access authorization; (ii) intended system usage; and (iii) other attributes as required by the organization or associated missions/business functions	PortalGuard provides the ability for the administrator to assign users to a specific group based on preset criteria via user credential, location and risk level.
AC-5	c. Implements separation of duties through assigned information system access authorizations.	User access is controlled by administrator by User ID
AC-6	The organization employs the concept of least privilege, allowing only authorized accesses for users (and processes acting on behalf of users) which are necessary to accomplish assigned tasks in accordance with organizational missions and business functions.	User access is controlled by administrator by User ID
AC-7	a. Enforces a limit of consecutive invalid access attempts by a user during b. Automatically when the maximum number of unsuccessful attempts is exceeded. The control applies regardless of whether the login occurs via a local or network connection.	System is able to set time limits, number of strikes for wrong passwords and reset criteria, all of which are user definable.
AC-8	a. Displays an approved system use notification message or banner before granting access to the system that provides privacy and security notices consistent with applicable federal laws, Executive Orders, directives, policies, regulations, standards, and guidance and states that: (i) users are accessing a U.S. Government information system; (ii) system usage may be monitored, recorded, and subject to audit; (iii) unauthorized use of the system is prohibited and subject to criminal and civil penalties; and (iv) use of the system indicates consent to monitoring and recording; b. Retains the notification message or banner on the screen until users take explicit actions to log on to or further access the information system;	PortalGuard is fully customizable allowing for seamless brand integration (e.g. Company logo and policies @ startup). Source: Tech Paper
AC-10	The information system limits the number of concurrent sessions for each system account.	PortalGuard prevents concurrent sessions
AC-11	a. Prevents further access to the system by initiating a session lock after of inactivity or upon receiving a request from a user; and b. Retains the session lock until the user reestablishes access using established identification and authentication procedures.	PortalGuard has the ability to set lock-out parameters based on the number of failed user logins along with locking out based on pre-set location information (e.g. unsecured Wi-Fi location)

Continued >>>

AC—Access Control (cont.)

Control No.	Control Description	PortalGuard Feature
AC-14	a. Identifies specific user actions that can be performed on the information system without identification or authentication	Users can be assigned to a specific group depending on job need, characteristic, etc.
AC-17	b. Establishes usage restrictions and implementation guidance for each allowed access method; c. Monitors for unauthorized remote access to the information system; d. Authorizes remote access to the information system prior to connection; and e. Enforces requirements for remote connections to the information system.	PortalGuard allows full customization based on job role, login location, and methodology via user defined risk factors.
AC-18	a. Establishes usage restrictions and implementation guidance for wireless access; b. Monitors for unauthorized wireless access to the information system; c. Authorizes wireless access to the information system prior to connection; and d. Enforces requirements for wireless connections to the information system.	Fully configurable by system administrator.

AU—Auditing & Reporting

Control No.	Control Description	PortalGuard Feature
AU-2	d. Determines, based on current threat information and ongoing assessment of risk, that the following events are to be audited within the information system.	PortalGuard has the ability to providing reporting detail on user location, type of connection (e.g. secure vs. public), number of failed attempts and user lockout.
AU-3	The information system produces audit records that contain sufficient information to, at a minimum, establish what type of event occurred, when (date and time) the event occurred, where the event occurred, the source of the event, the outcome (success or failure) of the event, and the identity of any user/subject associated with the event.	As outlined in Control AU2, PortalGuard offers full reporting and auditing capability by user, group, event, and location.
AU-4	The organization allocates audit record storage capacity and configures auditing to reduce the likelihood of such capacity being exceeded.	See Control AU2 & AU3 for details.

Continued >>>

AU—Auditing & Reporting (cont.)

Control No.	Control Description	PortalGuard Feature
AU-5	a. Alerts designated organizational officials in the event of an audit processing failure; and b. Takes the following additional actions: (e.g., shut down information system, overwrite oldest audit records, stop generating audit records)].	PortalGuard offers real time reporting features (e.g. email, text, report) of logins by user, # of attempts, locations, etc.
AU-7	The information system provides an audit reduction and report generation capability.	See Control AU2 & AU3 for details.
AU-8	The information system uses internal system clocks to generate time stamps for audit records.	All login attempts are time stamped with date, time, location and can be reported and summarized as user needs dictates.
AU-9	The information system protects audit information and audit tools from unauthorized access, modification, and deletion.	Report generation is limited to properly authorized users and is fully customizable.

CA—Security Assessment

Control No.	Control Description	PortalGuard Feature
CA-7	d. Reporting the security state of the information system to appropriate organizational officials	PortalGuard allows for customization to organizations needs based on Policy & Procedures

CM—Configuration Management

Control No.	Control Description	PortalGuard Feature
CM-2	The organization develops, documents, and maintains under configuration control, a current baseline configuration of the information system.	PortalGuard is able to provide detail information regarding current user status, group, and allowable access.
CM-4	The organization analyzes changes to the information system to determine potential security impacts prior to change implementation.	PortalGuard allows for full user customization based on user and/or user group privileges. System configuration and any subsequent changes are centrally controlled and auditable.
CM-5	The organization defines, documents, approves, and enforces physical and logical access restrictions associated with changes to the information system.	PortalGuard can be customized based on changing client needs.

Continued >>>

CM—Configuration Management (cont.)

Control No.	Control Description	PortalGuard Feature
CM-6	a. Establishes and documents mandatory configuration settings for information technology products employed within the information system using [c. Identifies, documents, and approves exceptions from the mandatory configuration settings for individual components within the information system based on explicit operational requirements; and d. Monitors and controls changes to the configuration settings in accordance with organizational policies and procedures.	As outlined in Control CM5 PortalGuard maintains a centrally administered configuration and settings are set system wide based on business needs and requirements. Changes occur in real-time and across the entire enterprise based on prescribed configuration settings. Any changes are documented and auditable.
CM-7	The organization configures the information system to provide only essential capabilities and specifically prohibits or restricts the use of the following functions, ports, protocols, and/or services:	User access if fully customizable with PortalGuard and can be controlled at the individual or user group level. PortalGuard also offers the ability to control access based on user logon location (e.g. secure vs. unsecure location).

IA—Identification & Authentication

Control No.	Control Description	PortalGuard Feature
IA-2	The information system uniquely identifies and authenticates organizational users (or processes acting on behalf of organizational users).	All users required to login and granted access based on user profile
IA-3	The information system uniquely identifies and authenticates [	PortalGuard is able to determine system type and location.
IA-5	The organization manages information system authenticators for users and devices by: a. Verifying, as part of the initial authenticator distribution, the identity of the individual and/or device receiving the authenticator; b. Establishing initial authenticator content for authenticators defined by the organization; c. Ensuring that authenticators have sufficient strength of mechanism for their intended use;	With it's integration with Active Directory PortalGuard is able to identify the unique user, able to determine their location and mode of login. PortalGuard requires all users to meet predetermined criteria before they are allowed to gain access to any systems.
IA-6	The information system obscures feedback of authentication information during the authentication process to protect the information from possible exploitation/use by unauthorized individuals.	PortalGuard offers a real time reporting dashboard that shows number of users logged in, location, length of login, number of login attempts and number of failed login attempts.

IR—Incident Reporting

Control No.	Control Description	PortalGuard Feature
IR-4	a. Implements an incident handling capability for security incidents that includes preparation, detection and analysis, containment, eradication, and recovery.	PortalGuard's reporting and dashboard features provide in depth reporting by user, group, time, location, and failed login attempts.
IR-5	The organization tracks and documents information system security incidents.	As outlined in IR-4, PortalGuard has the ability to report on ID, time, & location.
IR-6	a. Requires personnel to report suspected security incidents to the organizational incident response capability within [Assignment: organization-defined time-period]; and b. Reports security incident information to designated authorities.	See IR-4 & 5 for detail.

RA—Risk Assessment

Control No.	Control Description	PortalGuard Feature
RA-5	b. Employs vulnerability scanning tools and techniques that promote interoperability among tools and automate parts of the vulnerability management process by using standards for:	Password strength indicator helps understand potential vulnerabilities.

SC—System & Communication Protection

Control No.	Control Description	PortalGuard Feature
SC-7	b. Connects to external networks or information systems only through managed interfaces consisting of boundary protection devices arranged in accordance with an organizational security architecture.	PortalGuard has the ability to limit user access based on a number of parameters including geographic location, IP address and/or secure vs. public Wi-Fi.
SC-8	The information system protects the integrity of transmitted information.	See SC-7