servicenow

Define platform management practices

What's in this Success Insight

This Success Insight is an introduction to ServiceNow® platform management. It explains how to define policies for managing and maintaining your Now Platform so you can maximize its agility and minimize upgrade times. This Success Insight answers these key questions:

1. What is ServiceNow platform management? Why is it important?
2. What concepts and practices do I need to consider when defining ServiceNow platform management?
3. How do I define policies that support specific the platform management needs at my organization?

Key insights

- Good ServiceNow platform management practices define platform access protocol, upgrade and patching processes, performance monitoring practices, and platform security management.
- Start by defining a minimum viable set of policies to start with instead of trying to deliver a full, mature approach all at once.

1. What is ServiceNow platform management? Why is it important?

ServiceNow platform management defines the practices, policies, and standards for how to grant access to, upgrade, patch, secure, and maintain the Now Platform. It also defines the policies that allow your organization to optimize for performance.

Effective ServiceNow platform management helps maintain the foundational platform configuration, and it supports many business objectives, including:

- Reducing the level of effort required for maintenance activities

- Improving end users' experience
- Providing a framework your organization can follow for efficient and effective upgrades
- Making it easier to see the benefits of new features fast

Platform management policies are a key outcome of establishing solid ServiceNow technical governance and should be developed and/or approved by your technical governance board.

2. What should I consider when defining ServiceNow platform management?

Your ServiceNow platform management approach should define policies for platform access, upgrade management, platform patching, performance monitoring and readiness, and platform security management. Let's look at each of these separately.

Platform access

Your platform access policy defines the request process to obtain access to the Now Platform and the applications and data in the platform. Effective policies make the platform easier to manage and help secure it by controlling who has access.

Your platform access policies should consider:

a. **Access levels –** Define who has what level of access to specific parts of the platform and which instances

b. **Now Support (formerly HI) access –** Defines who has access to the Now Support customer support instance

c. **Temporary access –** Defines how people can get temporary access to the platform to fulfill a specific job

Read the sections below to learn more about each of these areas.

a. Access levels

ServiceNow manages access to the platform, applications, and data according to roles. Users are assigned roles that grant them to access to the data and functionality required for their role. Controlling your distribution of these roles is absolutely necessary to maintain the correct level of security (often set by security teams) and to reduce the risk of service interruption or failure.

Start by defining policies that document how you'll manage the access levels within the platform. When you define your access policies, ask these questions:

- Which users should have access to the instance?
- What level of access should users have within the instance?
- What is the process for requesting access?
- What training and/or certification do users need to have access at each level?
- Who is responsible for approving access?

Be sure you define these policies for each of your ServiceNow instances, not for your ServiceNow program as a whole, because you'll want to manage access differently based on each type of instance you have. For example, access is most strictly managed for production instances.

Take a look at the policies you've defined for instance management so you can keep the true purpose of each instance in mind when you create access policies. It's also important that platform owners work closely with product owners when defining these policies so they understand the needs of each solution deployed on the platform.

Practitioner insight

Access in ServiceNow is best managed by assigning roles to groups, and then managing the people within the group. Appoint a group manager and delegate group membership (or permissions) management to them to keep membership accurate. Managing permissions this way gives you assurance that your users have the right roles when they need them, and that those roles are removed when they're no longer necessary. You can automate and track approvals and access easily in the platform—just create catalog items to request adding or removing members from a group.

Practitioner insight

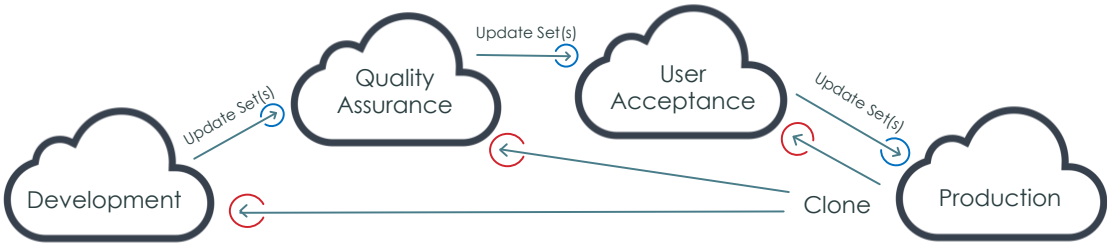
Define platform access policies early so you don't assign admin rights to too many users over time. This problem can require burdensome access control auditing to fix later on. Defining access policies early is especially important in a production instance—only grant a handful of users admin access. Use local accounts for admin access in a production environment in case the SSO authentication fails.

Be cautious when you decide who to grant high-privilege roles, such as system admin (**admin**) and security admin (**security_admin**), within each instance.

In a production instance, limit admin rights—the highest access—to fewer than five (ideally) people who are involved in troubleshooting and support. Make these admin accounts local so admins can access the instance even if SSO isn't working.

Review why someone would need a high-privilege role and if they'll be able to perform their daily functions without it. Don't grant higher-access roles than a person needs to fulfill their daily functions.

Also consider how access controls will impact your development's flow and efficiency. Refer to this example of a four-instance stack structure:



While all developers will usually have the **admin** role within the development instance, each organization needs to choose which of those developers will also have that same level of access in the QA instance. When you grant admin-level access in the QA instance, your development teams can migrate configuration and development work without involving other resources. But it also means that these modifications can freely migrate into the QA instance. The same philosophy holds true as you continue to move to user acceptance and finally, production.

Carefully consider how you'll assign admin access so you can reduce risk without hindering your development process. You might also need to modify your development process to comply with your access policies and provide a level of risk that's acceptable for your organization. Support from your partner or a ServiceNow platform architect is especially helpful when defining how this should work for you.

Practitioner insight

ServiceNow licenses are distributed through roles. Your platform owner should periodically review which users are assigned roles to make the most effective use of licensing. For example, look for users who are assigned roles and who haven't logged in for over 90 days, then decide if you should revoke the roles to reclaim licenses.

The Subscription Management application can also help you understand how your current subscriptions are used.

Practitioner insight

Only use impersonation for debugging purposes. Some customers deactivate impersonation features on production instances due to security and privacy concerns.

b. Now Support access

All customer instances are managed and supported by the Now Support instance. While security within this instance prevents users from seeing data from other customers, there are many actions you can request for your instances such as scheduling an upgrade or patch, or retiring an instance. Because of this, your organization should define policies regarding access to the Now Support system with these questions in mind:

- Who should have access to Now Support?
- What is the process for requesting access to Now Support?
- How often should we review the users with access to Now Support?

Practitioner insight

Anyone with access to Now Support will receive important notifications from ServiceNow. For example, they'll get messages about patch targets with advice to patch your instances as soon as possible.

Update and maintain the contacts listed in your company record so the right people get important program-related notifications.

For more information on managing company contacts, see Managing company contacts on Now Support.

c. Temporary admin access

Maintain strict control over your admin access to the production environment. While ServiceNow recommends keeping the number of users with admin rights to the production environment to five or fewer, there are often times when additional admin rights to

production need to be granted for a specific purpose. When this happens, it is best to grant admin rights temporarily to allow this work to be performed without providing long-term admin rights too frequently.

To accommodate this, define a process for how you'll grant temporary admin access in your platform access policy. This policy must specify who should be allowed to receive temporary access rights and what the requirements are to obtain them. It should also specify how temporary rights are requested and the length of time that temporary access is permitted (we recommend limiting temporary access to 24 hours max). Additionally, it is important to create a process to manage requests for temporary access and consistently provision and deprovision temporary access.

Upgrade management

Upgrade management practices define the process and policies your organization will use to upgrade efficiently and effectively. These practices make it easier for you to remain current with the latest family release.

We highly recommend that you upgrade with each new family release—if this isn't possible, be sure to upgrade at least once per year to maintain support. This practice helps your organization stay current, continue to receive support from ServiceNow, and take advantage of the new OOTB functionality provided with each new release.

Consider the areas in this table when you define your upgrade management policies:

Area	What you need to define
Process	• Who is responsible for reviewing release notes, planning for feature changes, and using new functionality? • What does the upgrade process flow look like? • Who should be involved in which phases of the upgrade? • When will each environment be upgraded? • What is the process to evaluate and/or remediate skipped items during the upgrade?
Approvals	• What approvals do we need before the upgrade? • What approvals do we need during the upgrade? • What approvals do we need after the upgrade?
Testing	• What testing do we need to perform before the upgrade? • What testing do we need to perform after the upgrade?
Scheduling	• What maintenance windows apply to upgrades? • What blackout windows apply to upgrades?
Communications	• What do we need to communicate before the upgrade? • What do we need to communicate during the upgrade? • What do we need to communicate after the upgrade?
Training	• What training do we need to provide to prepare users for the changes or features introduced during an upgrade? • How will we deliver training? • When does training occur within the upgrade cycle?
Support	• What is the support process to handle issues during upgrades? • When should we engage ServiceNow Support?

Practitioner insight

Approach upgrades as a project. Project management rigor can help you plan activities and timelines as needed so work is done correctly. It also helps you maintain accountability throughout the upgrade process.

Practitioner insight

Take time to review your upgrade management policies after each upgrade, and update them if necessary, so you can continuously improve.

Additional upgrades resources

- Upgrade Easily resources
- Perform ServiceNow upgrades quicker and more effectively
- Upgrade quickly and maintain platform health
- How do I perform ServiceNow Upgrades?

Platform patching

The ServiceNow Patching Program supports customers with consistent security, performance, and defect fixes. Each patch also remediates known security vulnerabilities. The Patching Program enables one full patch and two incremental security patches per quarter. To learn more about the program, watch the Patching Program Overview video and reading the ServiceNow Patching Program FAQs.

The effort to apply patches is much smaller than upgrading because patching doesn't introduce new functionality and doesn't affect system access. Consider the areas in this table when you write your platform patching policies.

Area	What needs to be defined
Process	• Who is responsible for reviewing patch release notes and planning for changes? • What does the patch process flow look like? • Who should be involved in which phases of the patch?
Approvals	Approvals aren't always necessary for patching. Determine if your organization's policies or compliance regulations require approvals for patching and then determine: • What approvals do we need before the patch? • What approvals do we need during the patch? • What approvals do we need after the patch?
Testing	Testing for patches is minimal compared to upgrades within the platform but you should still determine: • What testing do we need to perform before the patch? • What testing do we need to perform after the patch?
Scheduling	ServiceNow patches are scheduled automatically so it's important to understand the maintenance and blackout windows that apply so you can reschedule a patch if necessary. Consider: • What maintenances windows apply to patches? • What blackout windows apply to patches?
Communications	Communications for patching are typically less involved compared to upgrade communications but you still need to notify the user base of the activity. Consider: • What do I need to communicate before the patch? • What do I need to communicate during the patch? • What do I need to communicate after the patch?
Support	While it's unusual to experience issues during a patch, it's still important to define how to handle them if they occur. Consider: • What is the support process to handle issues during patching? • When should we engage ServiceNow Support?

Practitioner insight

Review your platform patching policies each quarter so you can continuously improve them.

Practitioner insight

Because patching happens frequently, consider only using automated testing to make the patching process more efficient.

Performance monitoring and readiness

Policies regarding performance monitoring and readiness describe the instance hygiene activities that administrators should perform on a routine basis to monitor and maintain the overall health of their ServiceNow instance(s). These activities should be identified by the frequency at which they are performed: daily, weekly, monthly, or quarterly.

When defining policies, consider including these activities and establish a process to handle discrepancies when you find them:

Activity	Recommended frequency
Review the system diagnostics homepage	Daily
Review the previous day's slow transactions	Daily
Review your scheduled jobs	Weekly
Check for repeated errors in the error log	Weekly
Look for excessive logging	Weekly
Find log files over 1GB	Weekly
Find slow-running jobs	Weekly
Find long-running jobs	Weekly
Monitor your table growth rate	Monthly
Clean your tables	Monthly
Review the Slow Queries log	Monthly
Check your instance for configurations that could impact upgrades	Quarterly

These activities and the procedures to perform them are listed in detail in the Fine-tune your ServiceNow platform with regular performance administration Success Playbook.

The table above list activities that apply to all instances. But based on the configuration of your instance(s) and the specific functionality in use, you might also consider defining policies and procedures to monitor:

- MID Servers
- ECC queue
- Mail connectivity and mailboxes
- Scheduled report executions
- Long-running reports
- Reports that haven't been run for over 90 days
- Discovery and Service Mapping jobs

Practitioner insight: Use HealthScan to keep a healthy instance

You can use the HealthScan platform to scan your instance(s) for best practice adherence in five categories: manageability, performance, security, upgradeability, and user experience. More specifically, HealthScan helps make sure you're following best practices for configuration and customization so you can avoid making common mistakes that impact your instance health. If you're actively engaged with ServiceNow Customer Outcomes, ask your representative if these services are available to you and determine the best frequency and timing to use them:

Score Card – The HealthScan Score Card is an automated scan that gives a high-level readout of instance health for each of the five categories as well the overall instance health.

Sprint Scan – The HealthScan Sprint Scan is an automated scan that you can use during an implementation. It's designed to run at the end of a sprint to make sure that any configurations you have align with ServiceNow best practices. Your implementation team can review the findings in detail and used them to improve your instance health.

Configuration Review – The HealthScan Configuration Review includes an automated scan similar the Sprint Scan but also includes a manual inspection of instance configuration and a detailed readout of your instance health.

Custom Scan – The HealthScan Custom Scan lets you scan a particular update set or application using specified definitions. This is useful during development cycles when you want to target the scan only to the areas where development is occurring.

Platform security management

Most organizations use ServiceNow environments to support mission-critical activities, so instance security is a high priority. In your platform management approach, include policies on platform security so users only have access to the data they need to execute their daily activities.

When defining platform security management policies, consider the areas in this table:

Area	What needs to be defined
Access control creation and updates	• What is the process for creating or updating access controls within the instance? • How are access control security requirements incorporated into development? • What testing do we need to perform when we create or modify access controls? • What approvals do we need to make changes to access controls?
User management	• What is the process for deactivating users? • How are users created and assigned to groups?
Role management	• How frequently should we review role membership? • How should we assign roles to groups? How often should we review them? • Who should approve any new roles we create?
Group management	• Who will manage user membership to a group? Should we delegate this to group managers or manage it centrally? • How frequently should we review group membership?
Auditing/monitoring	• What audits do we need to perform? • How frequently should we perform audits? • Are we planning to implement any monitoring capabilities? • How will we identify and review security events?
Administrator accounts	• What are the naming standards for administrator accounts? • Do we need dedicated accounts to grant users administrative access?

Practitioner insight: Stay secure with Instance Security Center

Instance Security Center is a plugin you can implement to provide a location for monitoring instance compliance with security controls, event management, and security settings. This plugin is enabled by default in all new instances but you may need to activate it on older instances. The Instance Security Center can provide platform administrators with:

- **Daily compliance score –** Provides a percentage score representation of the instance security based on compliance with the security hardening settings guidance
- **Hardening –** Allows admins to view and adjust security configuration properties that are impacting the compliance score
- **Session management –** Provides a location to view and manage all user logins and information about the logged-in user
- **Security notifications –** Notifications appear when security events take place in the instance and admins can view detailed information for each event

For more details visit Instance Security Center within the ServiceNow Docs site.

For more information on specific security settings visit Instance Security Hardening Settings within the ServiceNow Docs site.

2. Who should be involved in defining ServiceNow platform management?

Your ServiceNow platform owner and ServiceNow technical governance board should oversee the definition of effective platform management practices. This board is ultimately accountable for making certain the platform management policies are drafted and approved. But this board will likely need to get support from other groups and/or roles to define platform management policies.

Consider involving these roles when you define your ServiceNow platform management if they're not already participants on your technical governance board.

Role	Description
Enterprise architect	The enterprise architect creates one single language between people, processes, and technology that lets your organization share and enrich data across business functions seamlessly. The EA could be consulted when you define platform management policies and should at least be informed of this work.
Platform owner	The platform owner is typically accountable for managing the creation of all platform management policies.
Platform architect	The platform architect is typically responsible for the creation of platform management policies while consulting members of the organization, including enterprise architects, security administrators, and development leads/SMEs.
Security administrator	Security administrators are consulted during the creation of platform management policies to safeguard that the instances are protected according to organizational security policies and guidelines. You may also need to consult with security to so that patch and upgrade changes won't risk security issues.
Development leads/SMEs	Consult development leads/SMEs when you define the platform management policies because the output of these activities will affect the development flow and process.
IT operations lead(s)	Consult operations leads when you define platform management policies to identify which management activities are feasible and how they'll be done on a recurring basis. This is especially important for ServiceNow platform monitoring policies.

If your organization doesn't have a ServiceNow technical governance board, see our resource on getting started with ServiceNow governance.

3. What's the starter, or minimum viable approach, to ServiceNow platform management?

Ideally, your ServiceNow platform management will define platform access protocol, upgrade and patching processes, performance monitoring practices, *and* platform security management.

That's a lot to get right from the start. We recommend starting with a minimum viable policy that defines the most important standards and controls for your specific needs first instead of trying to define everything all at once.

Take these steps to get started:

1. Connect with your ServiceNow platform owner and, if established, your ServiceNow technical governance board. They should be accountable for managing the development of ServiceNow management policies at your organization.
2. Work with your platform owner to select one to three of the policy components listed in section 2 (for example, "upgrade management") that you think are the most urgent and important to enact at your organization. In our experience, at least platform access and upgrade management practices are most important to include in a minimum viable policy.
3. Consult with your technical governance board to approve of the components you selected. If necessary, invite any subject matter experts to help your technical governance board consider what your needs are for initial ServiceNow platform management.
4. Build out specific policy standards for your selected components.
5. Expand on your minimum viable approach to include standards for the remaining components in section 3.

4. How should I define specific ServiceNow platform management policies?

While this Success Insight covers what to consider when you define ServiceNow platform management, you need to define the specific policies and standards required for your organization, specifically. Account for any special needs required by:

- **Industry –** Companies operating in highly regulated industries (government, finance, and healthcare, for example) will likely require management practices and policies that more strictly enforce platform standards and controls.
- **Existing enterprise governance and/or platform management standards at your organization –** Many organizations already have defined practices for how to manage and maintain IT platforms. Your ServiceNow platform management practices need to align with (and usually be subordinate to) an existing, enterprise-wide policy at your organization.
- **IT architecture –** Your IT architecture may impact how you need to manage the Now Platform. Specific policies should account for how your IT environments are designed. This is especially true if ServiceNow is highly integrated with other systems.

When possible, we recommend working with your partner or with ServiceNow platform architects to define specific ServiceNow platform management practices and policies that will work for your organization. Reach out to your account manager to connect with ServiceNow architects to help with this.

Additional resources

- ServiceNow governance resources on the Customer Success Center
- Get started with ServiceNow governance
- Define ServiceNow technical governance policies
- Defining ServiceNow governance golden rules
- Define ServiceNow data governance
- Govern your ServiceNow environment

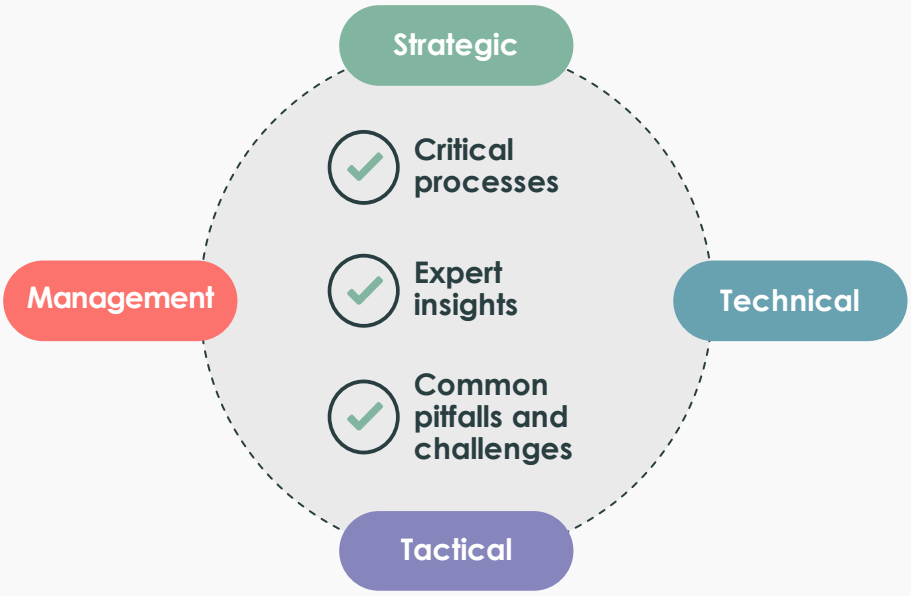
If you have any questions on this topic or you would like to be a contributor to future ServiceNow best practice content, please contact us at best.practices@servicenow.com.

servicenow

Customer Success Best Practices

ServiceNow's Best Practice Center of Excellence provides prescriptive, actionable advice to help you maximize the value of your ServiceNow investment.

Definitive guidance on a breadth of topics



Designed for:

- Executive sponsors
- Platform owners and teams
- Service and process owners

Created and vetted by experts

Best practice insights from customers, partners, and ServiceNow teams

Based on **thousands of successful implementations** across the globe

Distilled through a **rigorous process** to enhance your success

Proven to help you transform with confidence

- Practical
- Actionable
- Value-added
- Expert-validated

Get started today.

Visit Customer Success Center.

Contact your ServiceNow team for personalized assistance.