servicenow.

Define ServiceNow data governance

What's in this Success Insight

This introduction to ServiceNow data governance provides insight into how you can get started defining standards that govern how you manage and use data on the Now Platform®). It will help you answer the following key questions:

1. What is ServiceNow data governance? Why is it important? Who's involved?
2. What concepts and practices do I need to consider when defining ServiceNow data governance?
3. How do I define policies that support specific data governance needs at my organization?

Key insights

- There are eight different types of data that are created, stored, and/or processed on the Now Platform (your platform configuration data, for example). Your ServiceNow data governance should apply to all eight data types.
- Best-in-class ServiceNow data governance defines how data is owned, managed, structured, and secured.
- Your ServiceNow platform owner and technical governance board are accountable for defining ServiceNow data governance.
- You should start by defining a minimum viable set of policies and standards instead of trying to deliver a full, mature set of policies all at once.

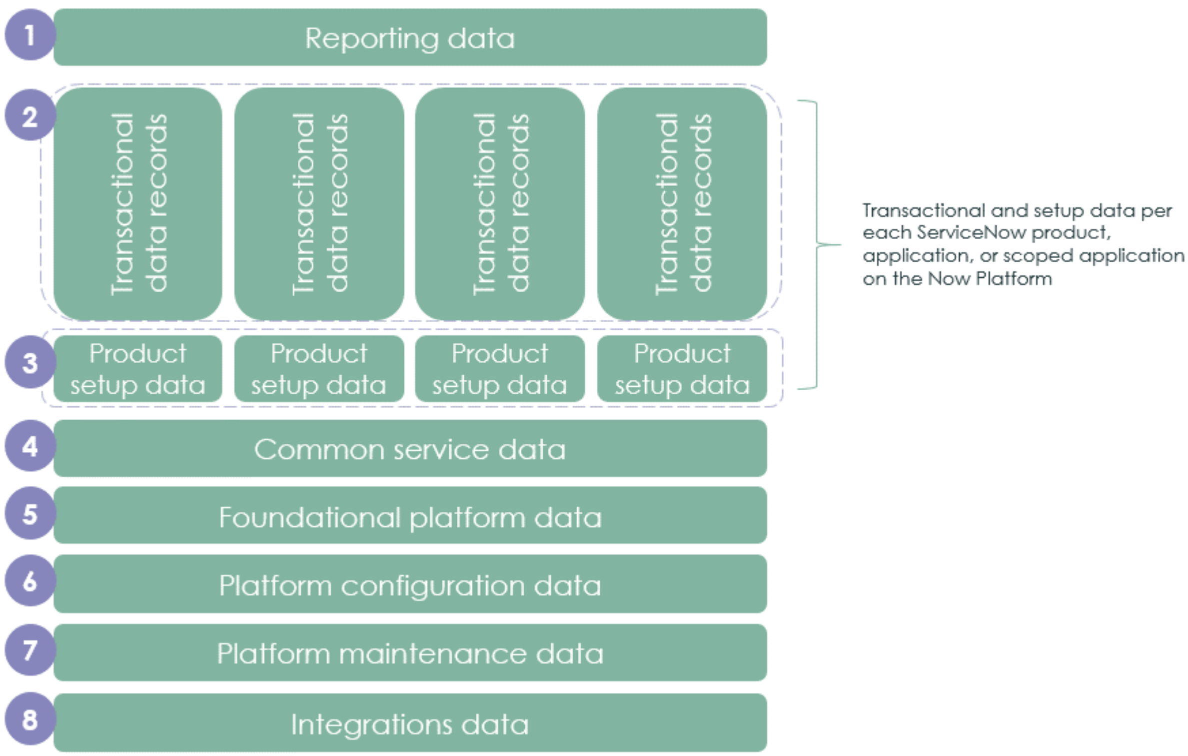
1. What is ServiceNow data governance? Why is it important?

ServiceNow data governance defines the standards and practices for owning and managing data assets created, stored, and/or processed on the Now Platform. It's a key part of ServiceNow technical governance, so be sure to develop and/or approve it in collaboration with your ServiceNow technical governance board.

ServiceNow data governance sets the foundational standards and controls needed to maintain high-quality data that your ServiceNow implementation can reliably and securely access and use. In doing so, ServiceNow data governance supports the maximum effective use and value of data for ServiceNow in your organization.

2. What data needs to be governed on the Now Platform?

Before defining ServiceNow data governance, it's important to understand the types of data typically involved when working on ServiceNow. There are eight different types of data that are created, stored, and/or processed on the Now Platform, including those shown in this graphic.



ServiceNow data governance should encompass all eight of these data types. But you shouldn't have to define separate policies for each type of data. For example, your data security policies should apply across all data types.

This chart outlines a definition for each type of data, examples of each type of data, and our recommendation for who should be the data owner for each type.

Data type	Definition	Example	Data owner
1. Reporting data	Performance data created to measure and track key performance indicators (KPIs)	• Performance Analytics metrics • Database views	• Product owner • Service owner • Security admin
2. Transactional data records	Data recorded from transactions within the platform	• Incidents • Cases • HR tasks • Scoped application records	Service owner
3. Product setup data	Data that's used by applications within the ServiceNow instance to configure functionality or behavior within the application	• Approval policies • Assignment rules • Group names and members • Integration requirements	Product owner
4. Common service data	Common service data across products and the Now Platform that can enable and support multiple configuration strategies	• Service model of a business application • CMDB configuration items	Business service owner(s)
5. Foundation platform data	Data that's used to depict the organizational structure	• Users • Groups • Locations • Business units • Companies	Business process stakeholders*
6. Platform configuration data	Data that's used to protect the integrity of the platform	• Authentication and authorization data • Domain separation • Encryption configuration and keys	• Platform administrator • Security admin
7. Platform maintenance data	Data that depicts the maintenance processes and data changes as part of platform administration	• Application logs • Transaction logs • Security logs • Event logs	• Platform administrator • Security admin
8. Integrations data	Data that is sourced or shared with other systems to enable platform capabilities	• Import set data • Staging table data	• Platform administrator • Product owner of the source system

* Foundational data ownership often sits outside the ServiceNow platform, e.g., HR owns users data, facilities own locations data, etc.

3. What should we consider when we define ServiceNow data governance?

Your ServiceNow data governance should define policies and standards for these listed practices.

Data ownership

ServiceNow data governance should define who owns any data that is created, stored, shared, or processed on the Now Platform.

Data owners are ultimately accountable for the state of the data. They must be able to make decisions that they can enforce throughout the organization via policy. They also need to work with the business and process owners to discern what data they need and how it will be consumed.

Your organization can appoint data ownership at an entity level (such as company records, user records, department records, configuration item (CI) classes, etc.) or at on an attribute level (such as state, assignment group, location, classification, etc.). ServiceNow recommends assigning ownership at the entity level because assigning at the attribute level could result in more maintenance work and complexity.

We recommend identifying owners for each of the eight data types on the Now Platform, as shown in the "data owner" column in the table in section 2.

Practitioner insight: Define data stewards in addition to data owners

Data stewards (sometimes referred to as data custodians) manage data according to set policies and standards on a daily basis. Stewards are generally operationally focused subject matter experts for the data entity or attributes. They can dramatically improve how well data is managed by both directly maintaining their data themselves and by consulting with others on how to best maintain their data.

Data management

To provide all ServiceNow platform stakeholders and users with high-quality data assets, data management is integral. We describe data management as the strategic practice of continually improving data quality, including its accuracy, integrity, relevance, and usefulness.

As part of ServiceNow data governance, define requirements for how you'll manage data on the Now Platform. As you do, consider these practices, at a minimum:

- **Data quality assessment and improvement process –** Define the process and standards for measuring and continuously improving your data quality. Measuring data quality can help your organization identify data errors for resolution and assess whether the data in your IT systems are fit to serve their intended purpose.

Start by assessing the current quality of the data your ServiceNow implementation uses and manages—is it accurate and complete? Then identify the metrics that will help you assess data quality over time and track the impact of any improvement efforts you make.

If your organization doesn't already have data quality processes in place, we recommend applying something like the DAMA Data Management Body of Knowledge's (DMBOK's) "data quality activities" to your ServiceNow data. This DAMA process includes steps to assess the quality of your data, identify and prioritize your improvement needs, and implement corrective actions.

ServiceNow also provides platform capabilities like dashboards to monitor data quality for specific uses cases.

Practitioner insight: Use dashboards to monitor data quality

ServiceNow provides out-of-the-box CMDB dashboards that display CMDB health reports and let you configure the CMDB health KPIs and metrics that CIs are evaluated for.

Similar custom dashboards can be configured to monitor other data quality use cases.

Practitioner insight: Configure validation checks and error messages to enforce data quality

Mandatory regulatory data quality use cases can be enforced by configuring validation checks and error messages while processing data. For example, you can set a business rule that checks whether key change attributes for changes to GxP- or SoX-relevant configurations are maintained. Keep in mind that enforcing data quality this way can negatively impact the user experience, so limit it to specific use cases.

Practitioner insight: Use your production instance as your single source of truth for data integrity

To maintain data integrity across instances (your sub production instances, for example), clone back from your production instance, which should be your single source of truth for data.

- **Audit –** Set expectations for how you'll audit your ServiceNow data to track changes and potentially identify issues. Here's an example audit cadence, which we recommend for auditing configuration management data.

Audit name	Audit scope	Frequency
Daily	Changes last 24 hrs.; authorized/unauthorized changes to the CMDB	Daily
Periodic	Business service audit verifying accurate CMDB information for a specific business service selected by the configuration manager or upon request from the business service owner	Quarterly
Major release	Data and data model changes introduced in a major release	On demand
Manual attribute data compliance	Verify data values for manual attributes such as CI owner, CI support groups etc.	Monthly
CI relationship	Verify the relationship between business service and nodes for a specific business service selected by the CFG manager or upon request from business service owner	Quarterly
Security logs	Verify no adverse platform configuration changes have occurred	Daily

- **Data lifecycle management practices –** Data lifecycle management is a process for managing data throughout its lifecycle on the Now Platform. Your data lifecycle management policies should contain governing principles about how to manage data at each stage of the data lifecycle: creation → storage → processing → reporting/machine learning → archiving/deleting.

servicenow

Practitioner insight: Be especially careful to define data retention and archiving standards so they support geographic-, industry-, and/or organization-specific retention requirements

You may need a policy requiring data owners to check data retention requirements before deleting any data. This policy could simply require that data owners answer no to questions like these before deleting any data:

- Does any regulatory or legal requirement mandate that this information is retained for a given period? If so, has it been retained for that period?
- Is the information in question critical for business operations?
- Would the information be considered a permanent document of any kind?
- Is the data considered proprietary intellectual property?
- Is the data required for fulfilling any business service level agreements (SLAs)?
- Does the data reflect current, legitimate, and useful business information or needs?

Tool tip! Explore the ServiceNow data archiving plug-in to automatically archive old data according to set criteria and/or business rules.

Practitioner insight: Classify data to enable quick retrieval for future use

Data retention preferences vary from organization to organization. Some organizations don't want data more than 6 months old and some are required to keep data for years. In many cases, this is influenced by industry regulations such as HIPPA.

No matter how long you must retain certain types of data at your organization, we recommend classifying your data to enable fast and easy retrieval for future use. Tagging data as confidential or legal can provide useful flags that help you retrieve data in the event of an audit. You can also classify data by how it is used—sales, financial, or employee data, for example.

Data architecture

ServiceNow data governance should consider data architecture needs by defining guidance and standards for how you structure data so applications can easily access and use it as needed. To do so, consider:

- **ServiceNow CMDB and Common Service Data Model adherence and standards –** Align your ServiceNow data governance with best practices for implementing and using the ServiceNow Configuration Management Database (CMDB) and Common Service Data Model (CSDM).

Here are a few helpful resources if you're not yet using ServiceNow CMDB or are unfamiliar with the ServiceNow Common Services Data Model (CSDM):

- CMDB and Discovery deployment
- Common Service Data Model (CSDM)
- Common Service Data Model (CSDM) 3.0 Fundamentals

Practitioner insight: Coordinate data synchronization carefully when data is shared/used by multiple ServiceNow applications

Data synchronization process and standards are especially important if the same data is being used by multiple applications on ServiceNow—for example, if you're using the same data for both the Application Portfolio Management and Information Technology Service Management (ITSM) applications. When this happens, make sure that the application service owners for each application coordinate with each other and with the platform owner to ensure proper data synchronization.

- **Integrations and data synchronization –** It's important to define standards for how you'll integrate ServiceNow with other systems when it's required to gain access to the data needed to do work on the platform. This includes data integrations standards that, for example, define how to use MID Servers, safeguard that the data fetched through integrations is clean, that integrations access data only as authorized and use it correctly, and that you know how to maintain a single source of truth for any data that's accessed.

  Also consider data synchronization standards that define how often you sync data, how you handle batching versus eBonding, and when core data copying is appropriate.

  See our checklist for information on how to implement integrations with ServiceNow.

- **Standards for how to manage database views and core/shared tables –** You should have a defined process for how to make architectural changes to core platform tables, especially as adoption grows on the platform.

Data security

Your ServiceNow data governance should set standards for how you will secure the data created, stored and/or accessed on the Now Platform. Defining how you will manage things like encryption, access, and personally identifiable information (PII) will reduce the risk of a breach and ensure you accommodate all enterprise-wide security protocols. This is key to maintaining access to the data your implementation relies on to deliver value.

To properly secure data, you should consider:

- **Encryption –** Identify encryption requirements at your organization and define how you plan to abide by them on ServiceNow.

- **Data access controls –** Consider how you will authorize access to data on the ServiceNow Platform. You also need to plan for how you audit access to track changes to permissions and access.

- **Securing personal data –** If you are creating, storing, and/or accessing personally identifiable information (PII), how will you protect this data? You must secure PII at least to the same standards set by enterprise information security protocol. This is especially important in highly regulated industries, such as healthcare and finance.

- **Securing asset data –** ServiceNow accesses a vast amount of information about your technology systems and assets. Unauthorized access to this data exposes your IT environment to potentially hostile actors. How will you secure this data on ServiceNow, in accordance with standards set by your IT information security team?

- **Product specific data security considerations –** In addition to data security considerations that apply to how you govern data security on the platform overall, there are also data security needs and concerns that are specific to individual products (e.g., data security needs that apply to ITSM). You can find a full description of these needs in our document on Understanding Your Data.

Practitioner insight: Don't forget about data sovereignty!

Data is subject to the:

- Laws in the country where the data is physically stored
- Jurisdiction the data subject belongs to (GDPR, for example).

ServiceNow hosts data in data center (DC) pairs—both members are either within the same jurisdiction or one that's mutually compatible, so even when data is transferred from one DC to another, the data's sovereignty is preserved.

Storing data and hosting it are *not* the same. ServiceNow only *hosts* customer data. In other words, ServiceNow provides a box and secures (hosts) it—customers decide what they put (store) in the box and who can access it.

Use these resources to learn more about securing data on the Now Platform:

- Safeguarding your data
- Securing the Now Platform

- ServiceNow security best practice guide
- Data access controls: A look at ServiceNow's access to customer data
- Product documentation: Instance Security Center

4. Who should be involved in defining ServiceNow data governance?

Your ServiceNow platform owner and ServiceNow technical governance board should be responsible for defining all technical governance and policies related to ServiceNow, including data governance.

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

Consider involving these roles in defining your ServiceNow data governance policy if they aren't already on your technical governance board.

Role	Description
Platform owner	The ServiceNow platform owner is ultimately accountable for creating ServiceNow data governance policies for the instance and safeguarding their alignment with any enterprise-wide data governance in place. Larger organizations may also have a chief data officer (CDO) who's accountable for overall enterprise data governance. If your organization has a CDO (or similar role), the platform owner is also accountable for getting the CDO to approve of proposed ServiceNow data governance, policies, and standards. The platform owner should collaborate with the ServiceNow executive sponsor to get this approval.
Enterprise architect	The enterprise architect creates one single language between people, processes, and technology that allows seamless sharing and data enrichment across IT Functions.
Platform architect/ data architect	The platform architect is typically responsible for creating specific data governance standards and policies in consultation with the organization's security administrators, data owners, process owners, and CMDB manager. Large organizations may also have separate data architect roles, as defined in The Open Group Architecture Framework (TOGAF).
CMDB manager	CMDB managers are responsible for maintaining the CMDB and all configuration data.
Security administrator	Security administrators are consulted during data governance policy creation so data is certain to be protected according to organizational security policies and guidelines.
Audit/risk expert	Fill this role with an audit/risk subject matter expert at your organization who can validate compliance and provide recommendations for storing and securing data.
Business process stakeholders	A business process stakeholder owns the source data for a particular, non-ServiceNow system and is responsible for the data quality of that system.

5. What's the starter, minimum viable approach to ServiceNow data governance?

Ideally, ServiceNow data governance should define data ownership, management processes, structure standards, *and* security protocols. But that's a lot to get right from the start. So we recommend starting with a minimum viable approach 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 developing ServiceNow data governance at your organization.
2. Work with your platform owner to select one or two of the policy components listed in section 3 that you think are the most urgent and important to enact at your organization, such as data security or data management. In our experience, data ownership and data security are most commonly included in a minimum viable approach.
3. Consult with your technical governance board to approve of the components you selected. If needed, invite any data subject matter experts to help your technical governance board consider what's needed in an initial ServiceNow data governance policy.
4. Build out specific policy standards for your selected components.
5. When your minimum viable approach is established and adding value, expand on your approach to include standards for the remaining components in section 3. Don't wait until you've perfected the standards for any one component before you expand. Instead, build a minimum set of standards across all necessary components—data ownership, management, architecture, security—then refine and mature your full approach over time.

6. How should I define specific ServiceNow data governance policies?

While this Success Insight covers considerations when defining ServiceNow data governance, each organization needs to define the specific policies and standards it requires. Account for any special needs required by:

- **Industry –** Companies operating in more highly regulated industries (like finance and healthcare) will likely require policies that enforce greater control over how data is used and secured in your organization.
- **Existing enterprise governance and/or data standards at your organization –** Many organizations already have defined data standards and policies, at least for data security. Your ServiceNow data governance needs 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 design a data governance policy that will work for your ServiceNow implementation. Specific data governance policies should account how your IT environments are designed. This is especially true if ServiceNow is highly integrated with other systems.

When possible, work with your partner or ServiceNow platform architects to define specific ServiceNow data governance policies that will work for your organization. Reach out to your account manager to connect with ServiceNow architects who can help you 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

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

Strategic

Management

Technical

Tactical

- Critical processes
- Expert insights
- Common pitfalls and challenges

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.