Gartner®

Find the Right Information Governance Model for Your Organization

Introduction

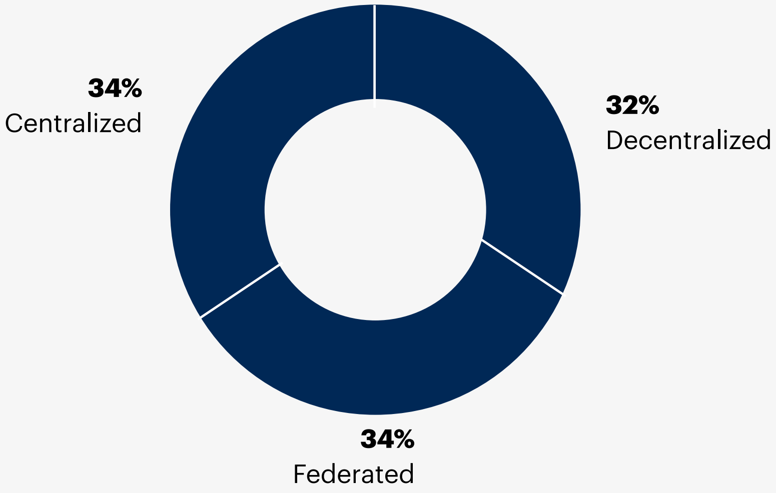
Privacy leaders must choose the right organizational model for information governance to meet their programs' goals. Use this research to assess whether a decentralized, federated or centralized model is the best fit for your needs.

Almost two-thirds of compliance, legal, and privacy leaders (63%) agree that information governance is an urgent priority in 2022, yet only 6% are satisfied with their organizations' progress.[1] One of the first questions privacy leaders ask when developing an information governance program is, "How should we structure ourselves?"

While there is no one right answer to this question, different organizational models are better-suited to different business contexts. Gartner's 2021 Legal and Compliance Information Governance Survey revealed that organizations operate under one of three organizational models for information governance (see Figure 1):

- **Decentralized** — Functions or business units independently undertake information governance efforts, with ad hoc collaboration as necessary.
- **Federated** — Functions or business units mostly implement information governance independently, but they have formal mechanisms for promoting strategic alignment and some operational coordination. These mechanisms usually take the form of a cross-functional governance steering committee or council.
- **Centralized** — An independent information governance function, or dedicated team within another function, primarily owns information governance. (Though a crossfunctional steering committee or governing council may also be present.)

Figure 1: Three Organizational Models of Information Governance



n = 59 legal, compliance and privacy leaders
Q: Which of these options best describes how information governance is managed at your organization. (If respondents chose either "We have an independent function that manages information governance activities" or "We have a team, or group of stakeholders, that sits within a function (e.g., privacy or information security) and administers the framework," we counted them as having a centralized organizational model.If respondents chose "There is no central function; each function independently executes information governance efforts" or "We do not have a mechanism for overseeing and administering our information governance framework," we counted them as having a decentralized model.
If respondents chose "We have a formal cross-functional steering committee," we counted them as having a federated model.)
Source: 2021 Gartner Legal and Compliance Information Governance Survey

To select the best governance model for their organizations, privacy leaders must consider the pros and cons of each.

Overview

Key Findings

- Organizations can choose a decentralized, federated or centralized organizational model for information governance. Each model has unique benefits and drawbacks that make it appropriate for different organizational needs.
- The decentralized model devolves decision making to the business level, the centralized model localizes decision making within a single function or team, and the federated model centralizes strategic aspects of governance while devolving more tactical decisions to the business level.
- All models exhibit similar program goals and key players, though organizations have moved from a focus on policy definition to a focus on implementation.

Recommendations

Privacy leaders seeking the best-fit information governance model should:

- Analyze the types and volume of sensitive data their organizations process, the level of desired standardization, and the level of flexibility and agility their organizations require to identify the most appropriate governance model.
- Take a fit-for-business-purpose approach to information governance by tying governance objectives directly to urgent business problems or opportunities.
- Include multiple functional or business unit perspectives, balance central guidance with local implementation, and clarify roles and responsibilities to ensure information governance success.

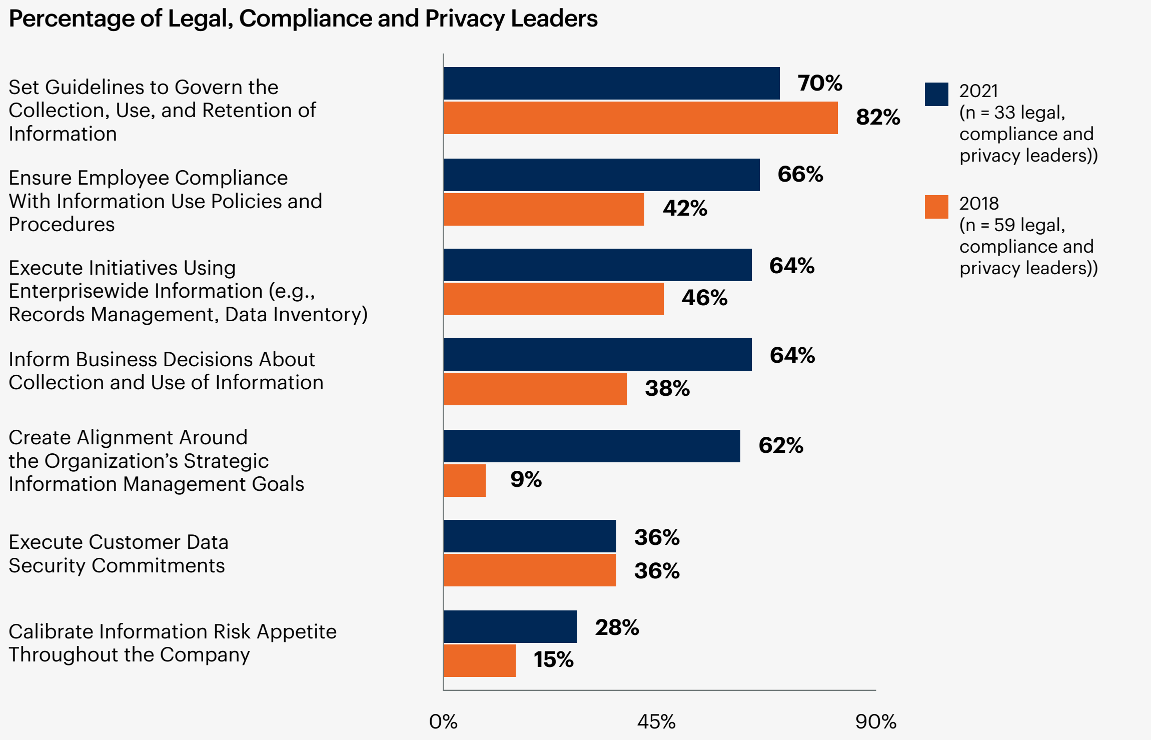
Analysis

Understand the Common Attributes for All Models

Gartner's 2021 Legal and Compliance Information Governance Survey showed clear differences between decentralized, federated and centralized governance models. Despite these differences, however, all models exhibit some common characteristics. These include:

- **Key players** — Regardless of governance model, legal, privacy and compliance tend to own policy-related activities (e.g., regulatory tracking, maintenance of information retention and deletion policies, creation of data use policies) and information governance training. IT and information security own information life cycle management activities (e.g., information classification, data mapping, inventorying).
- **Similar goals** — Assurance goals, such as increased compliance with regulations (used by 80% of organizations) and protection against reputational harm (64% of organizations), were common among all governance models. Seventy-eight percent of organizations also set goals for improved efficiency of information management, regardless of model. And 64% of organizations set goals for greater data transparency, better utilization of information to enhance business value and improvements in data quality, respectively.
- **Increasing maturity** — While organizations were mainly at the guidance-setting stage in 2018, most information governance programs have since taken at least some steps toward implementing their programs. In 2021, more than 50% of organizations listed ensuring compliance, executing initiatives using enterprisewide information, informing business decisions about the collection and use of data, and creating greater strategic alignment among their focuses (see Figure 2).

Figure 2: Focus of Information Governance Efforts in 2021 Compared to 2018



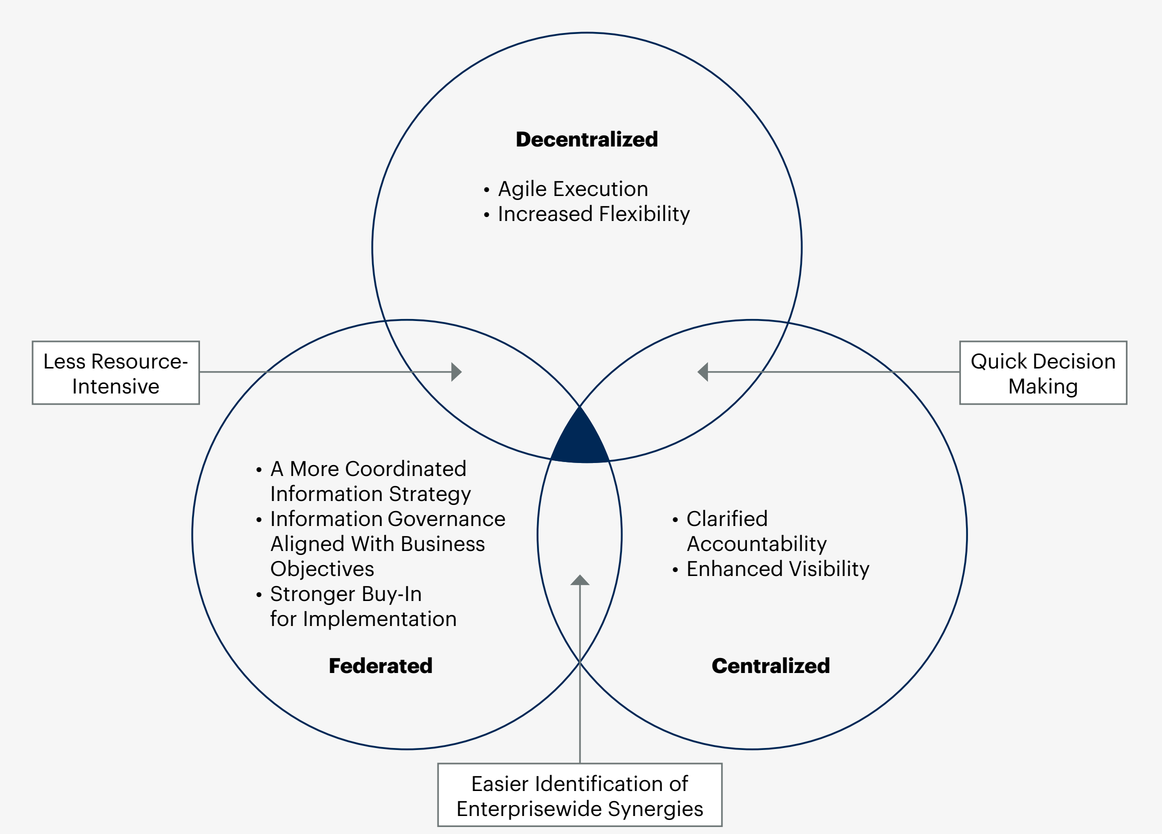
Q: [2018] What is the goal of your organization's information governance framework? [2021] What are the operational goals of your organization's information governance efforts in 2021?
Source: 2021 Gartner Legal and Compliance Information Governance Survey; 2018 Gartner Information Governance Survey
762982_C

- **Accountability challenges** — Only 8% of organizations indicated that the roles and responsibilities for governance activities were clearly defined, while only 10% agreed that owners of information governance activities were held accountable for outcomes. [2] Users of all models experienced poor accountability, but for different reasons. Multiple stakeholders with overlapping mandates and multiple layers of management inhibit users of the federated and centralized models, while poor oversight limits accountability for broader, organizational goals among those using the decentralized model. In all models, overlapping ownership of activities by different functions exacerbates confusion over who owns what, and further limits accountability. [3] Various business leaders are often happy to participate in information governance; however, few leaders outside a centralized information governance team want to assume accountability for enterprisewide governance outcomes given the scale and difficulty of the task.[4]

Choose the Model That Fits Your Needs

Decentralized, federated and centralized governance approaches each have their advantages and disadvantages (see Figure 3). No model is "best"; privacy leaders must take these organizational models' attributes into consideration when deciding which to choose.

Figure 3: Benefits of Each Organizational Model of Governance


Decentralized
• Agile Execution
• Increased Flexibility
Less Resource-Intensive
Quick Decision Making
• A More Coordinated Information Strategy
• Information Governance Aligned With Business Objectives
• Stronger Buy-In for Implementation
Federated
• Clarified Accountability
• Enhanced Visibility
Centralized
Easier Identification of Enterprisewide Synergies

Source: Gartner

Option 1: The Decentralized Model

In this model, most decisions about information use and management (both strategic and operational) are left to functions or business units, and coordination on roles, responsibilities, policy or strategy is limited and/or episodic. The decentralized model tends to represent the lowest level of maturity, and many organizations transition to the federated or centralized models as their programs progress.

The decentralized model underperforms relative to the federated or centralized models. Organizations using the decentralized model were more than two times as likely as those with the federated or centralized models to report dissatisfaction with their organizations' information governance progress. [5] They were also less successful overall at achieving their stated information governance goals. [6] However, the lower cost of this model and a need for business flexibility may outweigh these drawbacks, making this model a better choice for some.

Types of Organizations Adopting This Model

This model is best-suited for organizations working with a lower volume of personal or sensitive data, or where all sensitive data is collected and managed by one function (e.g., HR). Companies for which the regulation of function- or business-unit-specific data varies widely may also choose this model. Companies that are most likely to choose this model include:

- Thirty-eight percent of B2B companies and 25% of B2C companies adopt this model of governance.[1]
- Industries that are less dependent on personal data, such as manufacturing, energy, technology hardware and equipment, and materials.

Advantages of the Decentralized Model

- **Less resource-intensive:** The decentralized model usually does not require dedicated governance FTEs. As a result, it is a better choice for smaller organizations or those with limited personal or sensitive information assets. Similarly, the federated model, in which senior executives form a steering committee while the functions or business units handle tactical implementation, may also be an option for costsensitive organizations.
- **Agile execution:** Since decisions about information governance are made at the function or business unit level in the decentralized model, projects require fewer approval stages, and business partners are free to streamline and tailor processes to meet their needs. The decentralized model is also more responsive to employee input, and processes are easier to change when they are cumbersome because they are closer to the business level. As a result, organizations using the decentralized model were half as likely to report that information governance caused significant business drag as compared to the centralized model.[7]
- **Increased flexibility:** The decentralized model offers greater flexibility on policies because most decisions are left to function or business unit leaders. This is most useful when certain data types are subject to specialized regulations or most sensitive information is located within one function (such as HR) or part of the business.

Disadvantages of the Decentralized Model

- **Limited visibility and oversight increases risk:** Absent an owner, group or function that's responsible for companywide information governance, systemic issues (problems related to a specific type of information occurring wherever that information is used throughout the organization) are harder to identify. [8] This translates into potentially uneven guidelines, lax enforcement and higher compliance risk.
- **Organizational priorities are difficult to advance:** In the decentralized model, there is no single champion for information governance, nor are there significant resources or bandwidth dedicated exclusively to enterprisewide information governance goals. Organizations with this model are unable to cope with systemic issues because they cannot identify enterprisewide opportunities, get senior leadership buy-in or muster sufficient resources to address them.
- **Inability to coordinate activities leads to inefficiencies:** In the decentralized model, each business unit or function executes information governance activities at their discretion and without coordination. This creates potential for duplicative activities and gaps in implementation or enforcement.

Option 2: The Federated Model

The federated model adopts a cross-functional steering committee or council to manage enterprisewide information governance. Legal, compliance, privacy, information security, IT, records and information management, enterprise risk management, and data and analytics leaders are common participants, and high-level decisions are usually made by consensus or vote.

Steering committee mandates include formulating enterprisewide policies, advising on enterprisewide business decisions and strategy, managing enterprisewide information governance projects, resolving disputes, and surfacing concerns or different perspectives among stakeholders. In this model, steering committees tackle strategy (e.g., devising an information strategy for the organization, creating enterprisewide guidelines for data use), while the business leads tactical implementation (e.g., applying those standards to function- or business-unit-specific processes, training employees on those standards).

The federated model often acts as a "step up" in maturity from the decentralized model, and organizations usually adopt this model as they are first formalizing their programs.

Types of Organizations Adopting This Model

- B2C midsize enterprises, particularly in industries that manage high volumes of personal data (e.g., healthcare, insurance, financial services)
- B2Gs and public sector organizations (Sixty percent of the B2G organizations participating in our survey adopt this model, compared to 10% adopting centralized and 30% adopting decentralized.)
- Organizations where a variety of functions or business units collect and manage personal or sensitive data
- Organizations that would like to create more standardized information governance but do not have the resources for a dedicated information governance function or team
- Organizations with a strong committee culture or preexisting cross-functional committees that are equipped to take on an information governance role

Advantages of the Federated Model

- **Easier identification of enterprisewide synergies:** The federated and centralized models provide a forum that allows functional or business unit leaders to identify similar goals or redundant processes, and streamline or combine efforts to reduce duplicative work.
- **A more coordinated information strategy:** Committee structures provide a forum for function or business leaders to discuss the organizations' major information-related decisions and trade-offs, and to forge consensus on strategy and goals.
- **Information governance aligned with business objectives:** The federated model enables organizations to connect information governance work to the objectives and mandates of relevant functions or business units. This leads business leaders to prioritize information governance efforts over other demands on time and effort.
- **Stronger buy-in for implementation:** The federated model gives stakeholders a voice in overall governance strategy and provides a forum for them to share any business goals or barriers that may conflict with that strategy. This results in more realistic policies that won't fall flat upon implementation and an overall information governance strategy that balances function- and business-unit-level as well as enterprisewide goals.

Disadvantages of the Federated Model

- **Slow decision making:** With consensus decision making, achieving buy-in and agreeing on policy and strategic direction takes time. This is particularly true when business stakeholders have different mandates, goals and risk appetites. Poor role definition within the committee compounds this problem, prolonging unproductive debate and forcing final decisions.
- **Confusion about decision rights:** Authority to make decisions or settle disputes often remains unclear in the federated model. Moreover, committee structures may be layered on top of other bodies with overlapping mandates, such as privacy steering committees. As a result, robust discussion and agreement at the strategic level can have little practical effect because actors are not sure who is responsible for implementation. A charter with clearly delineated decision rights, a senior executive sponsor or an otherwise clear dispute resolution mechanism will help, as will meeting with stakeholders of related committees to identify and resolve areas of overlap.
- **Uneven training and awareness:** Organizations with the federated model report training and awareness as one their most significant challenges. When strategy is formed at the committee level and implementation is left to the business, those tasked with creating awareness and training may not see how the strategy applies to their teams. Even with training, employees may not understand how to adapt complex organizational guidance (which is often the product of compromise) to their individual situations. Putting data stewards or liaisons in charge of training can help bridge this gap. Their combined information governance and function-specific knowledge helps translate enterprise strategy or organizational policy into actionable guidance.

Option 3: The Centralized Model

Centralized information governance streamlines decision making and standardizes information governance policy and implementation. This model can take the form of either independent information governance functions or dedicated teams that sit within existing functions, such as legal or IT, or business units.

Many progressive organizations supplement independent information governance functions or teams with cross-functional steering committees to set strategic direction and working groups that help identify potential issues and drive action throughout the business. Others supplement their teams with data stewards or groups embedded in business units. In these hybrid models, central teams identify and resolve systemic issues, drive strategic alignment, provide oversight and standardize some elements of implementation. Embedded teams are usually tasked with executing policies or processes, driving awareness and surfacing issues in their parts of the business.

This model is a good fit for companies with high volumes of sensitive data and complex organizations that require a dedicated team to implement information governance.

Types of Organizations Adopting This Model

- Fifty-six percent of enterprises with $10 billion or more in yearly revenue adopt this model.
- Forty-five percent of B2C companies adopt this model.
- Forty-eight percent of publicly traded companies adopt this model.

Advantages of the Centralized Model

- **Clarified accountability:** With one function or team clearly responsible for information governance activities, little question remains about where responsibilities lie and who is responsible for success.
- **Quick decision making:** Centralized teams have fewer decision makers, clear lines of authority and clear mandates, and they are more closely knit. This limits unproductive debate and makes it easier to prioritize efforts and make trade-offs. More decentralized organizational models exhibit somewhat similar traits, though with limited effectiveness, as poor cross-functional visibility often means decisions are made with incomplete information.
- **Enhanced visibility:** Visibility into data use throughout the organization was listed as a top barrier to success by fewer organizations using the centralized model compared to those using the federated or decentralized models. [9] This is because dedicated governance teams have the time and resources to implement companywide platforms for data inventorying and mapping, define metrics and monitor compliance with guidance.

Disadvantages of the Centralized Model

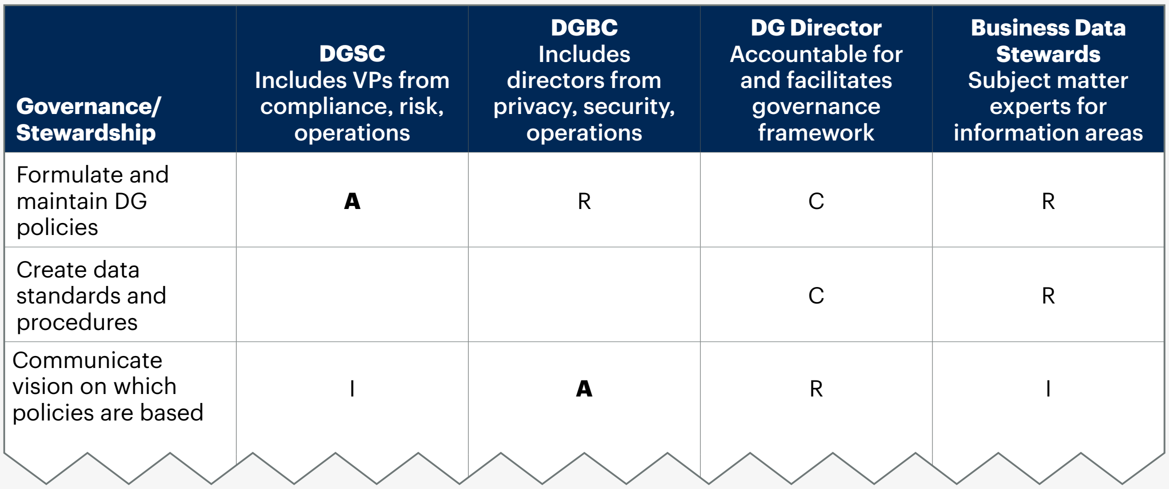
- **Risk of overcentralization:** Standards and guidance created by a centralized team may be inappropriate for specific business-level processes or run counter to function or business unit goals. The centralized model makes it difficult to solicit functional knowledge about processes and objectives that make for more tailored data use guidance and easier adoption.
- **Muddled division of labor:** Many organizations adopt the centralized model as their information governance efforts mature. While transitioning to this model, the new information governance team may be responsible for tasks that were once handled at the business level (i.e., functions or business units) or the committee level. Clear communication and delineation of how mandates and task ownership has changed will reduce confusion and redundant efforts.
- **Higher time and resource requirements:** Starting a whole new function dedicated to information governance is a big undertaking. Getting corporate approval, defining a mandate and hiring for dedicated roles are costly and time-consuming. It may be difficult to secure resourcing given myriad competing priorities. Furthermore, as implementing a program takes over a year, the organization's goals may have changed, and the policies and guidance they were tasked with creating may be out of date by the time that is done.

Build Flexibility and Clarity Into Your Information Governance Efforts

Regardless of which organizational model they choose, privacy leaders should adopt a flexible execution model and clarify roles and responsibilities to drive success. To do this, privacy leaders must:

- **Balance centralized guidance and local implementation:** While central oversight and guidance from a committee, team or function is valuable to information governance efforts, it's unlikely to be effective if it is not sensitive to business-level needs and goals. Make sure your chosen model of information governance has a way to implement initiatives at the business or function level. Consider using existing privacy or compliance liaisons, building a data steward network or creating working groups within the business to translate data standards into useful, relevant guidance.
- Ensure all necessary perspectives are represented. Make sure you build in opportunities to gather ongoing input from:
  - Executive decision makers and those responsible for implementing information governance (e.g., managers, project leaders, potentially rank-and-file employees)
  - Functions or business units with variable risk appetites
  - Functions or business units that control or collect high volumes of personal data
  - Functions that can represent the voice of the customer
  - Owners of data-intensive processes that cut across different parts of the business
- Clearly define roles. For the federated and centralized models, it is essential to define the decisions and tasks owned at the function or business unit level versus those owned at the enterprise level. Even with the centralized model, coordinating at the function or business unit level to devise a division of labor helps eliminate confusion, speed implementation and minimize redundant work. Develop a responsible, accountable, consulted and informed (RACI) chart that defines outcomes each group is accountable for, the role they play in achieving those outcomes and what implementation of these roles looks like in practice (see Figure 4).

Figure 4: Information Governance RACI Chart



Governance/ Stewardship	**DGSC** Includes VPs from compliance, risk, operations	**DGBC** Includes directors from privacy, security, operations	**DG Director** Accountable for and facilitates governance framework	**Business Data Stewards** Subject matter experts for information areas
Formulate and maintain DG policies	**A**	R	C	R
Create data standards and procedures			C	R
Communicate vision on which policies are based	I	**A**	R	I

Source: Adapted from Horizon Blue Cross Blue Shield of New Jersey

Evidence

Evidence for this piece was gathered from the 2021 Gartner Legal and Compliance Information Governance Survey, the 2018 Gartner Information Governance Survey and discussions with clients about their information governance efforts.

Gartner conducted the 2021 Legal and Compliance Information Governance survey among 59 compliance, legal and privacy leaders across a variety of industries, business types (i.e., B2C, B2B, B2G and public sector) and enterprise sizes to better understand how organizations structure their information governance efforts, how they distribute roles and responsibilities for information governance activities, and the level of maturity and formalization of their programs. The survey was conducted from October through November 2021.

Endnotes

[1] 2021 Gartner Legal and Compliance Information Governance Survey

[2] Survey question was, "On a scale of 1 to 7, where 1 is 'strongly disagree' and 7 is 'strongly agree,' to what extent do you agree with the following statements: 'Roles for key information governance activities are well-defined throughout the organization' and 'Owners of key elements of information governance programs are held accountable for positive or negative outcomes.'" While there were differences between models, users of no one organizational model agreed with either of these statements more than 20% of the time.

[3] We asked respondents to choose the owner of 17 activities from the following list: legal, privacy, human resources, data and analytics, IT, information security, finance, records and information management, compliance, internal audit, marketing, research and development, quality, enterprise risk management, project management office and business unit managers. We also included options for "multiple task owners," "other" and "My organization does not execute this activity." In all but one case, the most common answer was "multiple owners." Respondents chose this anywhere from roughly onequarter to almost half the time, depending on the activity.

[4] Accountability is usually built into centralized models, since there is a single team or function whose sole job is to lead information governance efforts. Therefore, unsurprisingly, respondents using the centralized model indicated that information governance leaders had more accountability than leaders in organizations using the federated or decentralized models. The differences between users of the decentralized and federated models, however, were marginal. While organizations often move from the decentralized to the federated model to clarify ownership, it sometimes has the opposite effect. Switching to the federated model creates additional layers of management and new tasks and responsibilities (for example, creating function-specific data use guidance), often confusing decision rights and responsibilities for legacy, siloed owners.

[5] We asked, "To what extent are you satisfied with your organization's information governance efforts?" Twenty-two percent of respondents using the decentralized model, 7% of respondents using the federated model and only 7% of respondents using the centralized model were dissatisfied or extremely dissatisfied.

Endnotes (Continued)

[6] Thirty-eight percent of respondents using the decentralized model reported success in achieving compliance, compared to 55% of respondents using the federated or centralized models. Only 11% of those using the decentralized model reported better utilization of information to create value for the company, compared to 28% for the other models. Only 15% of respondents using the decentralized model reported improvements in the quality of information used for decisions, compared to 28% for the other models.

[7] We asked, “To what extent does your organization’s information governance slow down progress on business partners’ projects or objectives?” Twelve percent of respondents using the decentralized model reported that it slowed progress to a large, very large or extremely large extent, compared to 27% of those using the centralized model.

[8] Sixty-three percent of decentralized organizations chose a lack of comprehensive understanding of how information is collected, used and managed across the organization as a top-three barrier to success. This was the most common answer for decentralized organizations, followed by competing priorities at the organizational level limiting the time and effort necessary to implement governance (at 47%), and then lack of coordination on policies and procedures (at 42%).

[9] Forty percent of organizations using the centralized model selected “we don’t have a comprehensive understanding of how information is collected, used and managed across the organization” as a top-three barrier to information governance success. This is compared to sixty percent of organizations using the federated model and 63% of organizations using the decentralized model.

Actionable, objective insight

Position your legal and compliance organization for success. Explore these additional complimentary resources and tools:

Research

Third-Party Risk Management Governance and Technology Investments

Understand top insights and trends for third-party risk management (TPRM).

Download Report

Research

2022 Legal Compliance Risk Hot Spots Report

Upgrade your legal and compliance risk management strategies.

Download Report

Webinar

Maximize Third-Party Risk Management With Aligned Assurance

Discover best practices for monitoring third-party risk.

Watch Now

Research

Deliver an Effective Training on Data Privacy

Educate employees to ensure compliance with policies and government regulations.

Download Presentation

Already a client?
Get access to even more resources in your client portal. Log In

Connect With Us

Get actionable, objective insight to deliver on your mission-critical priorities. Our expert guidance and tools enable faster, smarter decisions and stronger performance. Contact us to become a client:

U.S.: 1 855 811 7593

International: +44 (0) 3330 607 044

Become a Client

Learn more about Gartner for Legal, Risk & Compliance
gartner.com/en/legal-compliance

Stay connected to the latest insights in

Gartner®