Microsoft Data Governance Webinar

—

David Young

Portfolio

Slide 1 copy:

How to Implement a Successful Data Governance Strategy That Makes Your Organization More Secure

Date
Presenter name

Slide 1 script:

Welcome.

[Speaker introduces him/herself.]

I'm excited to talk with you today about the importance of implementing a data governance strategy for your organization, especially when it comes to your data security.

To start out with, we're going to go over some basic aspects of data governance and explore how

it intersects with your organization's data security concerns.

In the second part of this session, we'll dive into the details of how to successfully implement a data governance strategy. This will include a review of the major factors your organization should first consider, as well as some best practices and real-world examples.

Finally, we'll look at how Power BI can help promote sound data governance and make your organization more secure.

Let's begin!

Slide 2 copy:

What is data governance?

And why does it matter?

Slide 2 script:

Just to make sure everyone's on the same page, let's start with a basic definition of data governance:

It refers to the management of the availability, usability, integrity, and security of any data that is employed in an enterprise. In other words, it is an overall strategy that defines not only who gets to view, edit, and share data, but also how an organization's access to data can best be used to further its goals, as well as who is held accountable if there happens to be a security breach.

In this way, data governance is actually less about the *direct* management of data, and more about how data is accessed in accordance with other aspects and priorities of an organization. For instance, a data governance strategy that does not require an organization to store any data on its own servers may initially help out its bottom line, but could also go on to affect its marketing or sales department in challenging ways.

Which brings us to why data governance matters.

In short: We live in a data-driven culture. In many ways, we have more data than we even know what to do with. This means, in order make the best use of all that data, it is essential to put in place a strategy that takes into account the needs at every level, from corporate through IT and down to individual business units. This will help clarify roles, responsibilities, and decision-making, as well as foster effective collaboration. In turn, this will produce more informed business insights that will keep an organization ahead of its competition.

Slide 3 copy:

The intersection of data governance and security

[Verizon 2016 data breach report]

- Data doesn't leave
- Only relevant data
- Data is not altered

Slide 3 script:

Data governance also makes up an inseparable part of keeping an organization's data (and ultimately its profits and reputation) safe.

For instance, according to a 2016 Verizon report on data breaches, the vast majority (85 percent) of data threats actually begin *within* the organization itself. The reason for this is simple: Individuals unintentionally share or send data and reports to other individuals or entities that shouldn't have access to it. Quite often, employees aren't even aware of where they can or cannot send data in the first place – a factor that can further put an organization's overall security at risk.

Therefore, to shore up the security of your organization, it is essential that whatever data governance strategy you put in place does the following:

First, it should make sure that no confidential data is able to leave the organization. Employee salaries, sensitive sales numbers, trade secrets, and anything that could harm the organization if it fell into the wrong hands needs to be siloed away somewhere safe, where no one can unintentionally distribute it.

Second, departments should only be able to access data that is relevant to them. Unless there's a specific reason to do otherwise, keep data where it belongs. This not only limits the chances of a preventable security breach, but also can help keep individual departments focused on the data they should be looking at. Everything else is just noise.

Third, a good data governance strategy will also ensure that data sources and reports cannot be altered or corrupted. This means carefully considering who can edit data sources and why, and then putting firm controls in place to maintain the integrity of your data. The last thing you want is for someone who doesn't know what they are doing to make a small change that throws everything off.

Especially with the increasing prevalence of BYOD policies, it's important to keep these security measures in mind when designing your data governance strategy.

Slide 4 copy:

Effective data governance is not a one-time project.

Corporate, IT, and business managers must collaborate to:

- Locate and update data sources
- Come up with most effective uses of data
- Ensure stakeholders have access to data

- Prevent data breaches
- Monitor violation of data privacy rules

Slide 4 script:

However, even the most comprehensive and well-planned data governance strategy will fall short if it is not continuously maintained and enforced by all of its stakeholders. It cannot be a one-and-done activity.

With this in mind, executives, IT, and business managers and users must communicate with each other and work together to consistently keep track of where data is coming from and update their list of sources as new ones are added and old ones are removed.

They should also keep track of the rules, permissions, and other aspects of their data governance strategy to ensure data is being put toward its most effective use – and make changes whenever it is not. For instance, would it be more beneficial if individual business units could manipulate data sources themselves, rather than relying on reports? Are they able to draw useful insights from the data they do have? Questions such as these should spur an open and ongoing conversation.

Similarly, it's important to regularly evaluate whether everyone has access to the data they need as part of their role. This should be evaluated in careful relation to the organization's security concerns. While it is important not to leave an organization vulnerable to data theft or unintentional breaches, it is equally crucial that no protective rules put in place keep anyone from doing their job.

Of course, security needs to remain a primary concern, especially as an organization grows and changes over time. Policies and processes should be established and consistently enforced to ensure that data does not ever end up in the wrong hands. Likewise, access rules and permissions should be regularly reevaluated in order to ensure everyone has the data they need and nothing more.

Finally, as an organization evolves, it's important to check that no aspect of its data governance strategy is in violation of any data privacy rules

set forth by organizations such as HIPAA, the FTC, and PCI. This should be enforced through careful and consistent monitoring by an information security team. It can also be a good idea to educate all data stewards on these rules as well.

Slide 5 copy:

Implementing a data governance strategy

Slide 5 script:

Now that we have reviewed what good data governance and how it intersects with your organization's security concerns, let's look at the steps for implementing a successful data governance strategy.

Slide 6 copy:

The five basic steps:

Step 1: Define custodians of data and data sources

Slide 6 script:

Regardless of your organization's type, size, or complexity, the procedure for implementing a data governance strategy can be broken down into five basic steps:

One, define the custodians (or owners) of your data and data sources. This will involve developing policies that clearly specify who is responsible for the various aspects of your data, such as its level of accuracy and consistency, its accessibility across the organization, and how it is updated. As we will see later, depending on how many custodians your organization defines (whether the IT department controls all the data or responsibility is divided up among a variety of teams), this step will affect how the rest of your

data governance strategy is carried out.

Slide 7 copy:

Step 2: Define how data is stored, archived, backed up, and secured

Slide 7 script:

Two, put in place policies that define how your data is stored, archived, backed up, and secured. For instance, small organizations with limited data sources may be able to simply store their data on-site and authorize a limited number of computers and devices to access it. Larger organizations, however – especially those with staff in multiple locations – will have to adopt a more complex set of policies, often involving a mixture of on-premises and cloud storage, as well as security controls that take into account the various needs and responsibilities of data custodians.

Slide 8 copy:

Step 3: Define how data is accessed, edited, and shared

Slide 8 script:

Three, define how your data can be accessed, edited, and shared by all staff. Similar to step two – but with even wider implications since this goes beyond data custodians and affects all employees – your approach will ultimately depend on the unique needs of your organization. For instance, organizations that handle particularly sensitive data, such as those in the healthcare industry, will want to set policies that limit who can access that data. Likewise, organizations with diffuse structures and data sources should undertake a needs assessment to determine the most effective policies regarding how their employees can best make use of their data.

Limiting data access can enhance data security, but may come at the cost of organizational efficiency. On the other hand, while giving employees greater freedom to access and edit data could lead to more actionable insights, it could also put your organization at greater risk.

Slide 9 copy:

Step 4: Define ongoing procedures for ensuring compliance, security, and efficiency

Slide 9 script:

Four, define your organization's ongoing procedures for ensuring data security and guaranteeing compliance with data privacy regulations. As we mentioned, this step is tied up with how much access your organization gives its employees to its data, as well as your organization's type, size, complexity, and so on. However, it is important to emphasize that this step should focus on how your data's security can be protected on an *ongoing* basis, rather than just at the outset of implementing your data governance strategy. To do this, procedures should be defined for evaluating new data sources, reassessing access permissions and sharing procedures, and so on.

Slide 10 copy:

Step 5: Provide regular data governance training for all staff

Slide 10 script:

Finally, your organization needs to provide regular training for all staff regarding data governance policies and procedures, as well as security and data privacy best practices. This should be a regular part of onboarding new staff,

and ample documentation should be available for staff to reference on their own if they have any questions or concerns. Adequate data governance education can often be the best way to ensure a successful implementation that helps make your organization more efficient and secure.

Slide 11 copy:

Factors to consider before applying these steps:

- Organization size
- Structure
- Complexity
- Type of users
- Type of data used (and storage/privacy rules)

Slide 11 script:

Since each organization is different, the specific ways you end up applying these five basic steps will depend on a number of different variables. The most important factors to consider are these:

Your organization's size. A company with a dozen employees will have much different data governance needs than one with several thousand.

Your organization's structure. Does your business have one location, or is it spread around the globe? Is it broken up into numerous teams and departments, or does it have a more straightforward chain of command? All of this will affect the type of data governance strategy you choose.

Your organization's complexity. This relates to structure, but also to the unique data needs of your organization. For instance, are you collecting and analyzing data from many different sources? Do you have to take into account a wide array of different security needs and permissions? How many different ways do you need to share data and open it up to collaboration? All of this needs

to be considered.

The type of users in your organization. Is your data only used by limited number of power users who are familiar with data security issues? Or does your organization need to open up its data to a large number of users who may not be as familiar with data governance and security concepts? Each scenario may benefit from a different strategy.

The type of data you are using, as well as your organization's data storage and privacy rules. The more sensitive the data your organization uses, the greater the need for increased data security. Likewise, the way that data is stored and archived (whether on-premise, on the cloud, or some combination of the two) will affect the ways users can access and use it, too.

Slide 12 copy:

The three traditional approaches to data governance:

- Business-led self-service (bottom up)
- IT-managed (middle out)
- Corporate-led (top down)

Slide 12 script:

Now that we've covered the basic steps and variables, let's consider the three traditional approaches that organizations have used when implementing a data governance strategy. As we'll see, each comes with its own distinct advantages and disadvantages, and can usually be found in a certain type or size of organization. However, that does not preclude their use elsewhere.

Let's begin with business-led self-service, which is commonly described as a "bottom-up" style of data governance.

Slide 13 copy:

Business-led self-service (bottom-up)

In this approach, individual business units define ownership and management of data. It is most common with small organizations and those with simple data structures.

Advantages:

- Agility
- Creativity
- Freedom to innovate

Disadvantages:

- Less control over how data is used
- Greater possibility of data breaches

Slide 13 script:

Business-led self-service refers to a data governance strategy that leaves the ownership and management of data to the individual business units that use them. Unlike more centralized forms of data governance, this strategy usually involves a larger number of data stewards, each of whom determines the best policies and procedures for accessing, editing, and sharing their data (although they may still have to adhere to certain organization-wide rules regarding sensitive data). For this reason, business-led self-service is traditionally found in smaller organizations with fewer employees, as well as those with simple data structures and needs.

Its advantages are primarily the increased agility

it gives to organizations, the level of creativity it encourages, and the possibility that such freedom will inspire workers to uncover greater business insights and innovations. The idea is to cut out any gate-keepers between the data and those who are using and benefiting from it, so data can be put to its most effective use, and workers exploring data can develop ways of applying and benefiting from it that may not have otherwise been possible.

On the other side of the coin, there are disadvantages to such an approach. An organization relinquishes a certain amount of control over data when making it accessible to business units and employees. As such, without proper oversight, it can be more difficult to eliminate outdated or inaccurate sources of data, and add in verifiable new sources of data. This, in turn, may make an organization more vulnerable to data breaches and other security concerns.

Slide 14 copy:

IT-managed (middle-out)

In this approach, IT defines ownership of data, while business units control how it is reported. It’s most common with midsize and large organizations with more complex data infrastructures.

Advantages:

- Greater control over data sources
- Maintain creativity and freedom to innovate

Disadvantage:

- May require more oversight to ensure continued relevancy/usefulness of data

Slide 14 script:

IT-managed data governance, as its name implies, puts control of data into the hands of the IT department, whose job it is to properly vet new data sources, do quality control on old or inaccurate data sources, and enforce any and all security measures when it comes to data access, sharing, backup and storage. How they do all this is determined by a combination of corporate-level priorities, unique organizational security concerns, and the needs of the individual business units that are using their access to data to generate reports. Because this approach involves a dedicated IT department and gives a higher priority to security concerns, it is most commonly found in midsize and large organizations with more complex data infrastructures.

The chief advantage of such a system is its careful balance between security and freedom. Although it gives organizations greater control over their data sources than the business-led self-service approach, it still allows employees a certain amount of data-driven creative control and innovation. For instance, by continuously filtering all data sources through a dedicated IT department, an organization can more reliably (and often much more quickly) ensure their data is up to date. At the same time, the IT department can also communicate with business users using the data to make sure they are getting everything they need to remain efficient and innovative.

The disadvantage of an IT-managed system over a business-led self-service approach is simply that – to be successful – it requires much more consistent communication between the business units and the IT department. For example, if business units fail to properly inform IT of their data needs, or if IT does not act on their requests in a timely manner, they risk shutting the organization off from vital data sources, potentially affecting future growth.

Slide 15 copy:

Corporate-led (top-down)

In this approach, IT defines ownership of data, as directed by executive vision, and issues data-driven reports to business units. It's most common with large organizations with complex data infrastructures, especially those with more pronounced privacy concerns.

Advantages:

- Complete control over data sources
- Ability to drive what business units do with data insights
- Greater security

Disadvantage:

- Possible loss of innovation and additional insights that come with greater data freedom

Slide 15 script:

The most centrally organized of the three traditional approaches, a corporate-led data governance strategy is shaped at the top according to the priorities of an executive vision, which then gives full ownership of approved data sources to the IT department so that they can periodically release sanctioned reports to individual business units or to the wider

organization. This ensures the greatest possible control over not only what data sources are used, but also how that data is seen. Because of this, the corporate-led approach is most commonly seen in large organizations with complex data infrastructures, especially those that have more urgent privacy concerns, such as organizations in healthcare and government.

The advantages of this are most clearly seen in the increased control and security it gives organizations over their data, as well as how this control can translate into specific insights that executive-level leadership are looking for from the business units. Executive leaders who have a clear vision of how they want their organization to grow can use this approach to guide their employees in a highly specific direction, while ensuring that their organization's data remains under a tight set of controls. Because sharing and collaboration are mostly discouraged under this model, the risk of data breaches and other security issues is very low.

The biggest disadvantage to instituting such a high level of control is that it severely reduces the ability of business units to uncover insights and innovations from their data. By only sharing reports from a list of pre-approved data sources – and not allowing business units to make edits in accordance with their own needs – an organization can effectively push itself toward one goal, but at the cost of its own flexibility and adaptability.

Slide 16 copy:

Moving beyond a single model to a modern data governance approach

An intelligent solution that combines the best of all three worlds:

- Nimble, creative self-service culture
- Responsive and

comprehensive security

To do this:

- Identify data sources that require more oversight
- Determine which data sources business units can manage
- Design a frictionless strategy that lets units access what they need, then secures the rest

Slide 16 script:

Although one of the three traditional data governance strategies may serve the needs of some organizations, these days most will want to use a more nuanced strategy that combines the best aspects of all three. Let's take a look at how to develop a more modern approach to data governance.

The goal of any modern data governance approach should be to implement an intelligent solution that effectively emphasizes a creative business-led self-service culture – since this makes organizations more nimble and open to growth – while also taking into consideration any unique security needs.

However, to do this it is necessary that those at all levels – from the executive level through business managers, IT, and compliance officers – communicate and collaborate to customize a solution that aligns with larger organizational goals, day-to-day business unit needs, and overarching security concerns. This can be done by identifying which data sources require more control – whether over the entire organization (such as personal information) or from unit to unit (such as sales numbers) – and which data sources can be managed by business units and teams.

Most importantly, the data governance strategy that is developed from this conversation needs to be *frictionless*. This means no single unit or individual has to worry about setting security or

sharing measures for the data they can access. Instead, they will only be able to access the data and reports that they already need, then share it with whomever. Everything else will already be properly secured and protected against unintentional distribution. In effect, a truly modern data governance strategy will be both all-encompassing and invisible to the average user.

Slide 17 copy:

Example 1: An enterprise financial services company

- Business users can access a variety of data sources and use them to build reports
- Business users can share reports within the organization
- Pre-set data restrictions limit what others can see within those reports based on their permissions

Ideal for organizations:

- With a lot of data sources
- That value security
- Don’t have the need for intense data regulation

Slide 17 script:

Let’s take a look at an example of how a specific type of organization may implement a modern data governance approach.

Consider an enterprise financial services company that regularly collects and analyzes data from a

variety of different sources, much of it confidential but much of it also fairly standard. Their industry requires that they continuously innovate and adapt to consumer needs, but it also puts a high priority on keeping customer and organizational data safe and secure. Such a business needs a data governance approach that does the following:

After identifying which data sources cannot be disseminated outside (or perhaps even within) the company, business users have the freedom to access a variety of useful data sources that they can then analyze and use to build their own reports based on their unique needs. Afterwards, they can share those reports with authorized users within the organization to drive further collaboration.

However, if anyone attempts to share confidential information with an unauthorized individual or business unit – or even just with someone outside the company – pre-set restrictions will prevent them. If they are using business intelligence tools to generate and share these reports, they could even automatically remove restricted data based on the permissions of the user who is viewing it. This way, collaboration continues and security is maintained with as little extra effort as possible.

This sort of approach works best for organizations that use a lot of different data sources that may otherwise be too costly or time-consuming to centrally manage, as well as those that place a high value on their data security but don't otherwise have an intense need for data regulation.

Slide 18 copy:

Example 2: A midsize healthcare provider

- IT cordons off sensitive data and data sources, limiting access only to those with explicit permission
- Workers with permission can

share reports with larger audiences if they choose
- Other data and data sources can be accessed as needed by business users

Ideal for organizations:

- With highly sensitive or personal data
- At a higher risk of data breaches

Slide 18 script:

Let's also consider the example of a midsize healthcare provider, which obviously handles a great deal of sensitive personal data but is still looking for a more nimble data governance solution.

In their case, their IT department would locate and identify any data that cannot be accessed, viewed, or edited by a general audience, then cordon it off to all but those individuals (such as the executive leadership or specific unit managers) who warrant access. If these individuals so choose, however, they can generate reports based on this data and share it with a larger audience in order to garner additional insights and/or push the organization toward a specific goal.

Meanwhile, all other users can access data and data sources according to their specific needs, which should have already been determined after a careful assessment. Like in the previous example, if these workers attempt to share any protected data with an authorized user or unit, pre-set conditions will prevent them. This way, the security of the most sensitive data is prioritized, while all other data sources are managed more directly by individual units, which then have the freedom to analyze and edit them without having to worry about additional security concerns.

This type of approach is ideal for organizations (such as government and healthcare) that place a

high value on securing their data, but are still interested in fostering a culture of collaboration.

Slide 19 copy:

Steps to designing your own modern data governance approach:

- Identify which data and data sources need greater vs. less security
- Determine how much value you place on freedom and creativity to handle data
- Consider how the size and complexity of your organization affects the two previous factors
- Start small, then incrementally build your data governance strategy out as you assess the needs of your organization

Slide 19 script:

Just as each organization is different, each of their approaches to modern data governance should differ, too. The following checklist will help you develop a solution that maximizes the opportunities for creativity and collaboration while also keeping your data secure.

Slide 20 copy:

Identify which data and data

sources need greater vs. less security

Slide 20 script:

First, assess which data and data sources require a greater amount of security – and thus less access permissions – and which can be used by individual units or even the entire organization. Ideally, this should be done in conversation with a variety of stakeholders across the organization. For data reports, a quick rule of thumb is that if it is temporary or just for personal or team usage, then less governance may be required. However, if it is permanent or intended to serve a broad number of decision-makers, it likely would benefit from greater governance.

Slide 21 copy:

Determine how much value you place on freedom and creativity to handle data

Slide 21 script:

Second, carefully consider how much your organization values the freedom to access and edit data against how much it values controlling the security and effects of that data. Then ask yourself how the outcome of this consideration aligns with your organizational goals. What kind of culture do you want to create?

Slide 22 copy:

Consider how the size and complexity of your organization affects the two previous factors

Slide 22 script:

Third, consider how the size of your organization,

as well as its complexity (whether in structure or in the variety of data use), affects the two previous factors. Is it feasible to properly regulate the free use of data, or will that lead to too many potential security concerns? Alternately, does your organization's structure or industry make it necessary to give business users more control of their data?

Slide 23 copy:

Start small, then incrementally build your data governance strategy out as you assess the needs of your organization

Slide 23 script:

Finally, we recommend that – rather than trying to do everything at once – you start small with a data governance strategy, and then slowly build it out over time. For instance, begin with a single business unit or a selection of similar data sources, apply user permissions and security controls, and then study what works. It's normal not to get everything right out of the gate, so you may as well lower the stakes as you begin to implement the new strategy. When you've properly determined the needs of your organization and thoroughly tested your strategy, you can begin applying it elsewhere.

Slide 24 copy:

Power BI Pro and Premium

Your shortcut to a modern data governance strategy:

- Drives new insights into data through reports and analysis
- Promotes security through

more data oversight and monitoring
- Puts in place a flexible strategy that will stay relevant as you unfold it over the long term

Slide 24 script:

Now that we've reviewed the basics of data governance and security, including the general concepts and strategies behind implementing a successful solution, let's look at an actual tool your organization can begin using to jumpstart its data governance success.

Put simply, Power BI is the most advanced business intelligence solution available on the market. With it in their toolbox, even non-technical users can begin drawing more valuable insights from their data through a robust collection of reporting and analysis options, while corporate-level and IT users gain greater control over how data is used.

The result is a more secure and collaborative data governance strategy that will be able to grow and evolve with your organization over the long haul.

Slide 25 copy:

6 ways Power BI Pro and Premium promote good data governance:

Slide 25 script:

Here are some specific ways your organization can use Power BI to implement and promote a successful data governance and security strategy.

Slide 26 copy:

1. Can connect to a vast array of

different data sources

Slide 26 script:

#1: Power BI has been designed to seamlessly connect and communicate with a huge number of different data sources. You can plug it into your existing CRM solution, get data from your website analytics software, pull out regular reports from your email marketing service, and more. There are literally thousands of different ways to connect data to Power BI, and new content packs are constantly being added. It's the single best way to put all your data under one umbrella and draw quick, insightful conclusions from it.

Slide 27 copy:

2. Integrated with the Microsoft family of solutions

Slide 27 script:

#2: Unlike other business intelligence solutions, Power BI will automatically integrate with the Microsoft family of solutions. That means you don't have to worry about trying to configure some kind of third-party solution. Instead, you can quickly connect Power BI to your Azure Active Directory or other Microsoft tool, and start exploring your data right away.

Slide 28 copy:

3. Easy to create different roles and permissions

Slide 28 script:

#3: Integral to proper data governance, Power BI is incredibly flexible when it comes to setting up a variety of different roles and permissions. For instance, you can set permissions according to individual reports, user, data source, or some combination of all three. You can even set different permissions within the same report so

users with different access levels see only what they need to. (Remember our first modern data governance example?) In short: regardless of your organization's type, size, or complexity, Power BI will work for you.

Slide 29 copy:

4. Allows analytical sandboxes

Slide 29 script:

#4: Another cool feature, especially useful to those considering proper data governance, is Power BI's ability to create analytical sandboxes. These are special areas in which users can access and explore data without running the risk of compromising sources or committing an unintentional data breach. This is a great solution for those organizations still experimenting to target an optimal data governance strategy, as well as for those that may want to allow their users more freedom from time to time.

Slide 30 copy:

5. Leverages both on-premise and cloud solutions

Slide 30 script:

#5: The Power BI suite of programs also makes good use of both on-premise and cloud solutions. For example, Power BI Desktop is a free, feature-rich tool that you can use on your own computers to create detailed reports and analyses using its growing library of stunning interactive graphics. You can then send these over to Power BI Pro or Premium service on the cloud, where the rest of your coworkers can view and edit them, distribute them even further, and garner valuable insights wherever they happen to be.

Slide 31 copy:

6. It’s easy to use

Slide 31 script:

#6: Finally, Power BI is designed to be as intuitive to use as possible. This is a tool for everyone – not just experts. You can build custom graphs and charts in just minutes by plugging in an existing Excel spreadsheet or formula and using drag-and-drop graphics. You can set user roles and permissions, or connect Power BI to whatever third-party tool you rely on, all with just a few simple clicks. You can even ask natural-language questions within the program, and Power BI will automatically select the corresponding data and visualizations you need. These features and many others combine to make it an indispensable tool for all of your business intelligence needs.

Slide 32 copy:

With Power BI Pro and Premium, data freedom and creativity need no longer be in opposition to data security.

Thank you!

Slide 32 script:

It wasn’t too long ago when everyone thought data freedom and creativity had to come at the cost of data security.

Yet, by going through the steps we’ve outlined in this webinar and implementing a modern data governance and security solution, that is no longer the case.

A data governance strategy that provides both data security and data freedom at the same time can give you a competitive edge. And Power BI Pro and Premium can help you get there.

Thanks for listening!