



## Data governance for Aerospace and Defense (A&D)

**Navigating costly compliance while safeguarding your data**



# Data classification in Aerospace & Defense

**A strategic asset versus a compliance liability**

Data classification in Aerospace & Defense: A strategic asset versus a compliance liability

In the Aerospace & Defense (A&D) industry, effective data classification can open doors to enhance operational efficiency and strategic decision-making. Enhancing data sharing can lead to fresh business insights and improved management of inventory, workforce planning, procurement, supply chain risk, and relationship management—crucial aspects in this sector. Let’s discuss:

- The potential benefits of data classification, specific to the A&D industry
- Guidance on beginning to understand your data within this industry’s context
- Overview of data types and repositories in A&D and how they impact the approach
- Challenges of data classification in the A&D sector
- How to establish and deploy a data classification program in this industry

Empower yourself to identify leading data classification practices in the A&D industry and explore ways to develop a data classification strategy that could be pivotal in achieving many of the goals of classification.

What is data classification?

Data classification is the process of categorizing information, based on its sensitivity, so that the suitable level of protection may be applied. An organization’s data classification standards and policies should define the categories, appropriate levels of protection, and prioritization of information required to reduce risk.

Why is this an important topic?

It enables the definition of risk-based controls to help prevent the loss or misuse of company information and IT assets. Company-wide data classification can be an enabler for many other initiatives:

- **Interoperability:** Exchange and interpret data across different systems and applications easier

Cybersecurity Maturity Model Certification (CMMC)

Identify sensitive data that should be protected and meet NIST 800-171 / CMMC requirements

**Digital twin:** Categorize replicas and structure vast amounts of data

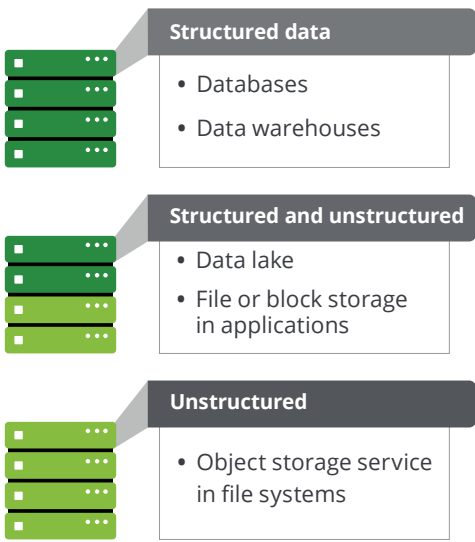
**Smart factory:** Organize data to drive decision-making, Operations and allocation of resources

**Data protection:** Apply the appropriate protection measures by identifying the data type and location

**Compliance:** Meet DFARS requirements by knowing what data you have and where it is stored

Data types and challenges

For many organizations, their data may fall heavily into one side of structured or unstructured repositories. Leveraging classification tools can help your organization classify its structured and unstructured data, but the types of storage and challenges for classification are different.



### Common challenges by data type

- Obtaining **application/data inventory** for effective implementation. Each application within legacy systems will need to be configured separately.
- Supporting the scanners with appropriate **human intervention**. Even the leading tools will require intervention by skilled personnel with a deep understanding of both the data and the industry.
- Understanding the data. Engineers cannot **identify the data** and the business will not **recognize the data structure**.
- Providing quality of **free-form text fields**. Organizations may need to clean their unstructured datasets to avoid skewing classification.
- Monitoring a **variety of data** and reviewing **false positives** from tools. Sensitive data types include CUI, FCI, ITAR, EAR, and other Export Controlled data.
- **Training users** properly is essential to an effective program. Recognize not all users will require the same level of training.
- Handling **limitations to file types**. Document management systems can be leveraged to overcome limitations to classifying CAD files and other unstructured data
- Managing **limitations to storage platforms**. Scaling across the organization in a consistent manner is central here.

Proper data governance is fundamental. A tool or solution can expand the reach of the classified data, but *everyone* in the organization is responsible for understanding what kind of data they are handling and their responsibilities for classification.



NOW: Begin by building your foundation	NEXT: Design and test in your environment	LATER: Deploy and begin to use data classification to help protect your enterprise
<ul style="list-style-type: none"> <li>• <b>Define clear and measurable objectives:</b> Collaborate with various functional stakeholders to determine critical and common goals for classifying data. Approach with ease instead of taking on too much too fast.</li> <li>• <b>Compose a data classification policy:</b> Administer enterprise-wide adoption through a policy that explains the importance and value of each applicable user's participation. The policy should be digestible for users, withstand the test of time, and align with regulatory requirements such as DFARS 252.204-7012, 7019, 7020 and 7021.</li> <li>• <b>Establish data classification schema/guidelines:</b> Define the classification categories and sub-categories specific to your organization, train users, and provide a universal reference on classification labels starting with your highest risk classifications such as Export Controlled (ITAR/EAR) and CUI.</li> <li>• <b>Integrate with data governance:</b> Incorporate data classification objectives into your existing data governance program strategies or start a new one. Frequently review and consider the types of data being handled and their requirements.</li> </ul>	<ul style="list-style-type: none"> <li>• <b>Conduct workshops with stakeholders to understand use cases:</b> Create use cases including the following information: department/function/unclassified program, business process, data elements/data types, and business process owners.</li> <li>• <b>Evaluate current toolset (if applicable) and/or perform vendor analysis:</b> Develop requirements based on identified use cases to evaluate whether the toolsets address technical and functional requirements.</li> <li>• <b>Develop technical architecture and design implementation plan:</b> Conduct workshops with the technical stakeholders and program owners to discuss solution architecture and design approach. Design implementation plan including Data Classification schema and user directory integration.</li> <li>• <b>Design the proof of concept (if applicable):</b> Define the scope and objective of the POC. Develop governance and operating models around scope, priorities, roles and responsibilities, metrics, and policies and procedures.</li> <li>• <b>Develop training and communications plan:</b> Develop training and communication plan, which may include the following: direct communications (e.g., emails, online trainings), indirect communications (e.g., intranet), organizational change management activities, management support and reinforcement.</li> <li>• <b>Conduct the proof of concept (if applicable):</b> Perform solution installation, configuration, and integrations. Develop operating procedures, test cases, and policies/rulesets.</li> </ul>	<ul style="list-style-type: none"> <li>• <b>Redesign the tool, resources and operations based on POC feedback:</b> Enhance technical architecture, training and communications toolkits, and operational procedures/policies with feedback from the POC.</li> <li>• <b>Develop and execute enterprise deployment plan:</b> Create a deployment plan that may include communications, enablement, and waves. Document technology change management plan and obtain "Go Live" authorization.</li> <li>• <b>Provide operational support:</b> Manage related questions and/or comments centrally (e.g., integrate with existing helpdesk/service desk processes). Update frequently asked questions documentation, as-needed.</li> <li>• <b>Enable protection by integrating controls (NIST 800-171/CMMC):</b> Automate controls to protect data beyond defined data elements and reduce manual protection efforts for both end users and security. For example, discover sensitive data locations based on data classification, and automatically block/encrypt sensitive data.</li> </ul>

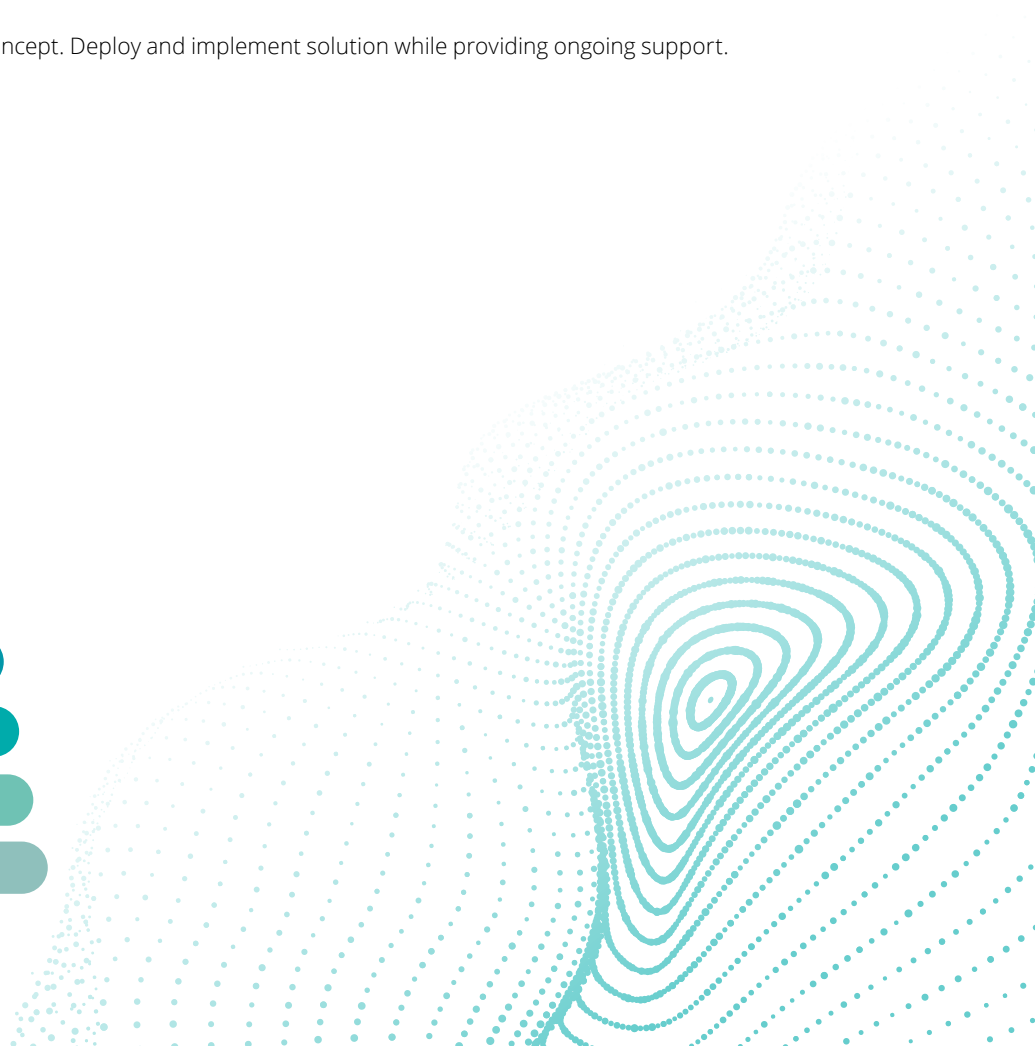
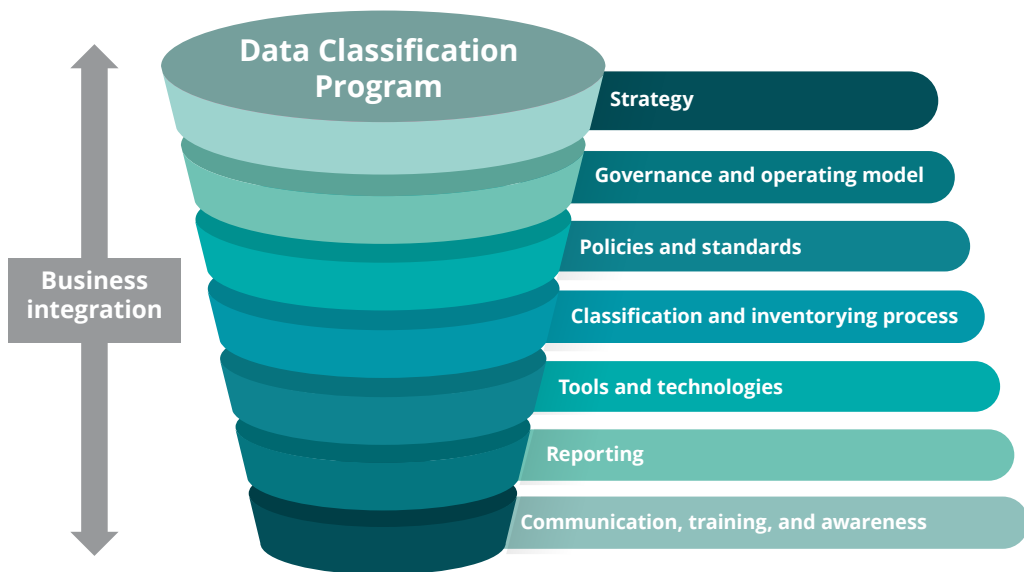
### Takeaways

- **What is data classification?** The process of categorizing information, based on its sensitivity, so that the suitable level of protection may be applied.
- **What are common data classification challenges?** Alignment of people is a prevalent challenge when it comes to data classification. Proper Data Governance is vital to the effectiveness of a data classification program.
- **What should you do now?** Define and prioritize your organizations objectives. Compose data classification policies and handling guidelines. Integrate with your data governance program and understand key regulations and contractual flow-downs.
- **What should you do next?** Evaluate data classification toolsets to identify appropriate solution. Design and implement a proof of concept with the selected solution.
- **What should you do later?** Design a deployment plan based on feedback from the proof of concept. Deploy and implement solution while providing ongoing support. Integrate with additional controls to enable enhanced data protection.

### Engage with Deloitte

#### How Deloitte can help

Deloitte can help clients design, build, and operate Data Classification and Data Governance programs wherever they may be in their cyber journey.



### The Deloitte difference



**We are data risk driven.** Data classification is a foundational component of Deloitte's data protection framework which uses industry-leading governance and technology capabilities to effectively protect sensitive data to drive business value.



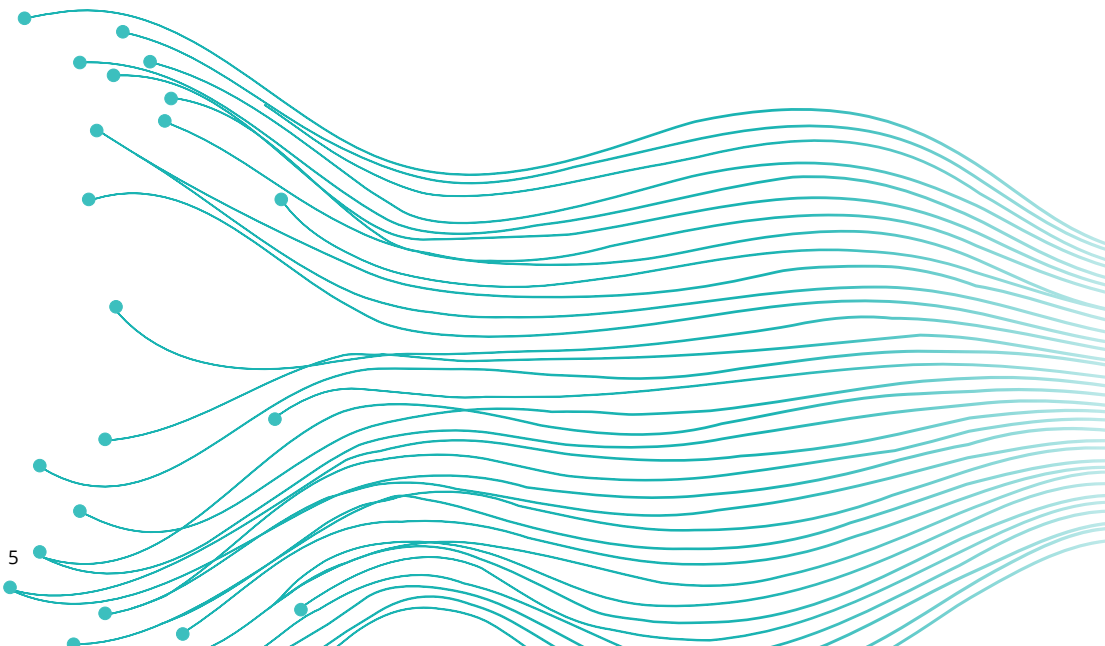
**Differentiators** include our value-based data risk management approach, dedicated managed services, strong relationships with leading vendors, and Data Protection Lab.



**Deloitte's extensive knowledge** provides valuable insights, customized approach, and an understanding of diverse threats. Our Cyber & Strategic Risk offerings include *Application Security, Crisis, Resilience, & Brand, Data & Privacy, Detect & Respond, Identity, Infrastructure, Cloud, & Emerging Tech, and Strategy & Extended Enterprise*. Our broad experience enhances problem-solving, regulatory compliance, and offers a broad cybersecurity approach.



**We help enterprise and government clients** identify and categorize their data based on business criticality and sensitivity. As a result, we enable our clients to raise awareness of the business impact of unauthorized disclosure or modification of data and identify and prioritize data that requires additional controls and safeguards.



### Contact us



**Jeff Lucy**  
Managing Director  
Risk & Financial Advisory  
Deloitte & Touche LLP  
[jlucy@deloitte.com](mailto:jlucy@deloitte.com)



**Brian Wolfe**  
Managing Director  
Risk & Financial Advisory  
Deloitte & Touche LLP  
[bwolfe@deloitte.com](mailto:bwolfe@deloitte.com)



**Eric Dahlgren**  
Senior Manager  
Risk & Financial Advisory  
Deloitte & Touche LLP  
[edahlgren@deloitte.com](mailto:edahlgren@deloitte.com)



**Colleen Freeman**  
Manager  
Risk & Financial Advisory  
Deloitte & Touche LLP  
[cfreeman@deloitte.com](mailto:cfreeman@deloitte.com)



## Data Discovery in Aerospace & Defense

**Advance decision-making, improve efficiency, and drive growth**



In the Aerospace & Defense industry, the rapid expansion of data is leading to escalating challenges in data management. To tackle these challenges, we recommend implementing a Data Discovery process to help pinpoint data and provide invaluable insights and actionable perspectives. A Data Discovery program is a crucial element of data privacy, protection, and governance in the highly regulated and complex environment of the Aerospace & Defense (A&D) industry. Let's talk about:

- The benefits of Data Discovery specific to the Aerospace & Defense sector
- The challenges of Data Discovery based on the specific data types in the industry
- The process to establish and deploy a Data Discovery program within an Aerospace & Defense context

See your growth take flight: We'll outline top-tier Data Discovery practices and uncover methods to construct a Data Discovery strategy that could play a pivotal role in achieving numerous data management objectives within the Aerospace & Defense industry.

### What is Data Discovery?

*Data Discovery* is the user-driven process of identifying patterns or specific terms/objects in a dataset to gain insights. The process involves scanning and making sense of data using data profiling, data cleansing, and advanced reporting services and solutions.

*Data Scanning* is the technical process of analyzing large datasets across an organization to understand the environment and data quality. The process includes scanning metadata, understanding data structures, identifying patterns, establishing connections, and data lineage.

### Why this is an important topic

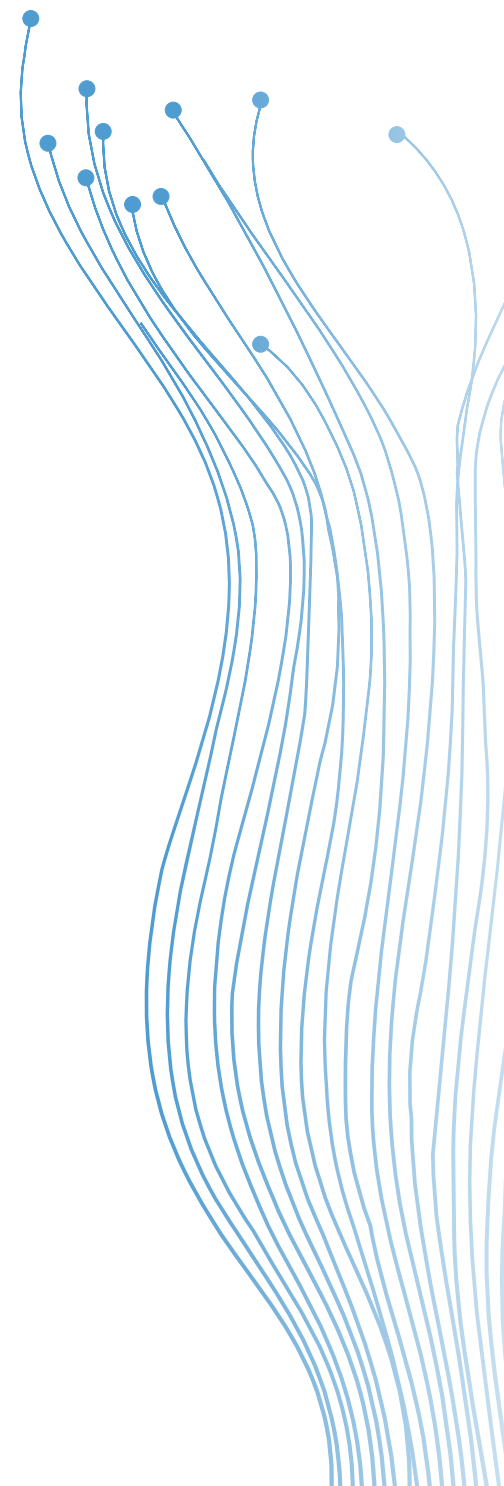
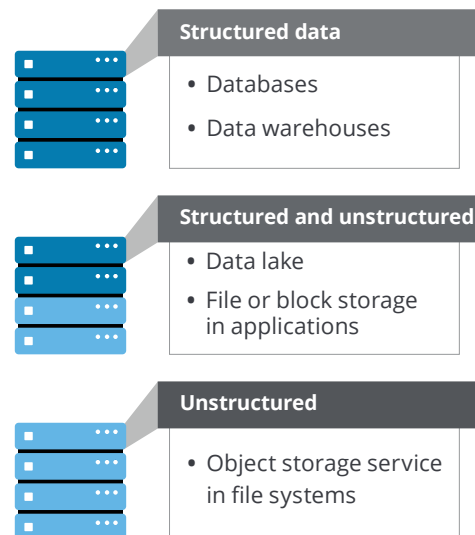
Data Discovery is crucial for a broad data management strategy and can be an enabler for many other initiatives:

- **Data quality management:** Identify and resolve data quality issues by designing and enabling rules

- **Metadata management:** Label, classify, and search data based on metadata
- **Enterprise data management:** Identify, evaluate, and collate potential critical data and map data locations
- **Advanced analytics:** Attain deeper insights into relevant data, especially unstructured data
- **Data governance:** Manage data throughout its life cycle by overseeing data ownership
- **Data compliance:** Meet regulatory mandates (Defense Federal Acquisition Regulation Supplement (DFARS) 252.204-7012, 7019, 7020, and 7021) with strengthened data security

### Data types and challenges

Scanning structured data and unstructured data have their own particular set of challenges. Organizations should determine what data types they want to prioritize. While there are solutions that offer scanning for both data types, Data Discovery capabilities may not be as insightful as a tool that focuses on scanning primarily structured or unstructured data.



### Common challenges by data type

- Scanning **high volumes** of structured, unstructured, geospatial, and sensitive data that organizations typically store can be **time-consuming and resource-intensive**.
- **Preserving the security** of sensitive information can require a broad set of different coordinated tools (e.g., encryption, attribute-based access controls), in accordance with DFARS.
- **Identifying and extracting relevant information** from a variety of sensitive data types, such as Controlled Unclassified Information (CUI), Federal Contracting Information (FCI), and Export Controlled data (ITAR/EAR).
- Determining which data can be stored in different types of repositories, such as Government Cloud and On-Prem, and managing access based on factors like employer, citizenship, and offshore.
- **Generative Artificial Intelligence (GenAI)** tools are still being evaluated for this industry. As adoption increases, it will enable users to create more documents faster than ever, compounding the challenges of scanning everything.
- Understanding the **complex relationships** between tables and fields for prioritizing National Institute of Standards and Technology (NIST) 800-171/Cybersecurity Maturity Model Certification (CMMC) controls while enabling the business to do what it needs.

For an effective Data Discovery program, it's important to consider your organization's data landscape, vision, and objectives when evaluating and selecting a tool.

**NOW: Begin by building your foundation**

- **Determine the maturity of your organization's current state**
  - Evaluate the present state of the organization's capabilities, processes, and systems. Understand how mature or developed these aspects are by using a model to identify the current level of maturity and areas to improve.
- **Develop and socialize a road map for the approach**
  - Create a strategic plan that defines the goals or desired outcomes and includes the major steps or milestones needed to reach them. Outline the scope, identify the resources needed (time, money, or staff), and set clear objectives or goals for the project. Socialize the road map by sharing and explaining this plan to relevant stakeholders to attain their understanding and support for the approach. The complexity of environments with co-mingled regulatory and non-regulatory data may present a challenge.
- **Define use cases, scope, resources, and objectives to develop the project plan**
  - Define the specific scenarios or situations in which a proposed system or project might be used (use cases). Use cases should be built for the processing, storage, and transmission of regulatory data in environments where non-regulatory data also may exist.

**NEXT: Design and test in your environment**

- **Acquire and implement the desired technical solution(s)**
  - Identify, purchase, and procure the technology or software tools required to collect, process, and analyze data in the Data Discovery process (e.g., data mining tools, databases, data visualization).
  - Remediate vulnerabilities or issues discovered during data scanning. It could involve deleting unneeded sensitive data, moving data to more secure locations, or implementing additional security controls.
- **Refine the technical design and process**
  - Fine-tune the technical design and process flow of the solution. Test the solution or application to confirm that the solution works as intended and addresses the selected requirements. Address issues identified during testing and modify as needed.
  - Keep data sovereignty and citizenship status requirements in mind while refining technical designs
- **Build and document the Data Discovery process for future utilization**
  - Create a detailed, step-by-step guide to the Data Discovery process. Document the tools used, methods for collecting and analyzing data, and the process for interpreting and presenting the results.
  - Develop a Data Discovery process with these fundamental steps: 1) Identify the relevant data; 2) develop a data conversion and migration strategy; 3) classify the data; 4) define the business requirement; 5) execute discovery; and 6) create the content architecture (flow and gaps).

**LATER: Expand Data Discovery to protect your enterprise**

- **Monitor processes as part of the larger data governance strategy**
  - Observe and track data to promote quality, security, and compliance with relevant regulations. Continuously correct inaccuracies, identify security breaches, and track data usage across the organization.
- **Establish and document a transition plan for the technical solution**
  - Create a structured approach for moving the implemented technical solution from its current state to its desired future state. Detail how this change will be managed, the steps involved, and the timeline. Share the transition plan with the stakeholders to socialize the process and their roles in it.
- **Expand the Data Discovery program to other business areas by onboarding and training new resources**
  - Extend the scope of the Data Discovery initiative to encompass more of the organization. Train new team members on the Data Discovery processes and tools to improve data handling and decision-making across the organization.
- **Identify automation opportunities for Data Discovery**
  - As discovery tools continue to incorporate Machine Learning (ML) models, they may aid in metadata management by improving the automation of labeling and classifying data, making it easier to search and analyze data. They can also play a role in data quality management by identifying anomalies or errors and suggesting corrections based on learned data patterns. However, data sovereignty and citizenship status requirements play a crucial role in which tools may be used.


## Takeaways

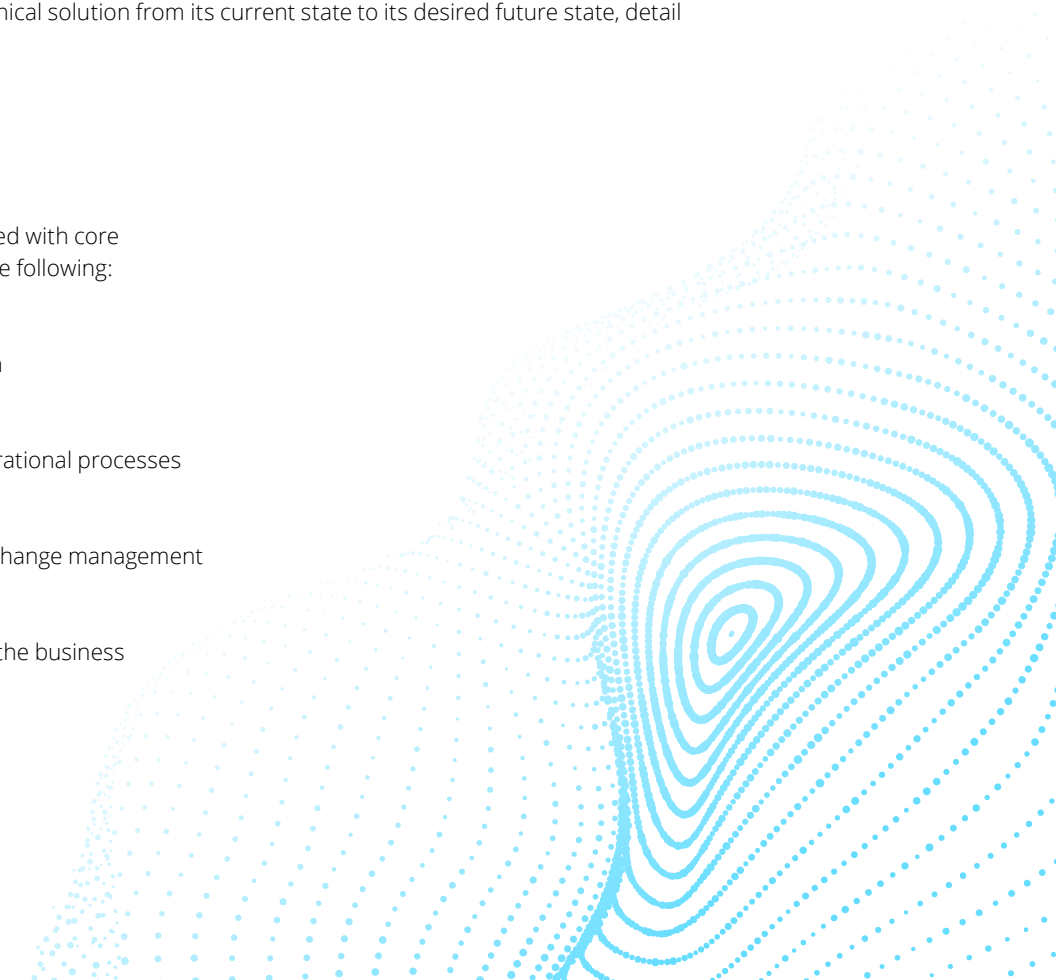
- **What is Data Discovery?** Data Discovery is the user-driven process of scanning and identifying patterns or specific terms/objects in a dataset to gain insights.
- **What are common Data Discovery challenges?** Both structured and unstructured data scanning can pose challenges. Organizations should determine which types of data they want to focus on scanning first, especially in co-mingled data environments and multi-cloud (Gov-Cloud versus Commercial Cloud) landscapes.
- **What should you do now?** Create a strategic plan that defines the goals or desired outcomes, includes the major steps needed to reach them, and defines the specific situations in which a proposed system or project might be used (use cases).
- **What should you do next?** Acquire and implement the technical solution(s) for the Data Discovery effort. Fine-tune the solution's technical design and process flow by testing the solution or application with the correct unclassified program teams.
- **What should you do later?** Create a structured approach for moving the implemented technical solution from its current state to its desired future state, detail change management, the steps involved, and the timeline.

## Engage with Deloitte

### How Deloitte can help

Deloitte can help clients design, build, and operate progressive Data Discovery programs aligned with core business objectives. Relevant activities to maturing a program include, but are not limited to the following:

- |  |  |
|--|--|
|  Assess current state and define scope    |  Test and refine the solution                  |
|  Establish requirements and road map     |  Design and document operational processes    |
|  Define use cases and identify resources |  Assist with organizational change management |
|  Implement and configure solution        |  Expand operations across the business        |





## The Deloitte difference



**We are data risk driven.** Data Discovery is built into Deloitte's Data Protection & Governance framework, which provides various other services that enable organizations to understand their data throughout its life cycle, and the controls in place to protect data.



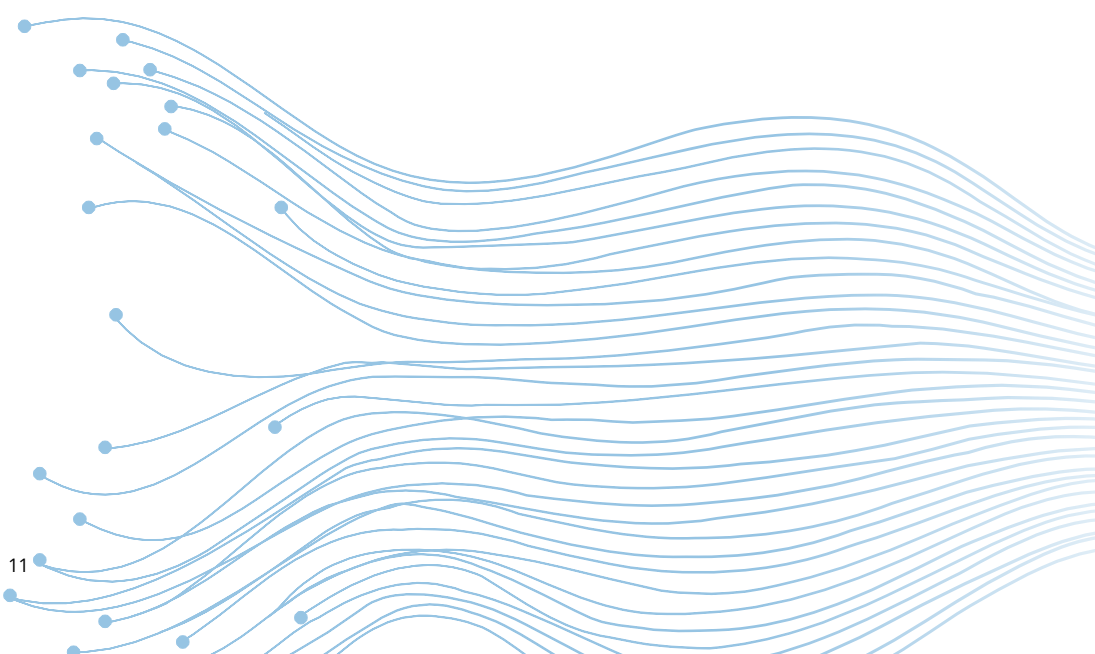
**Differentiators** include our value-based data risk management approach, dedicated managed services, strong relationships with leading vendors, and Data Protection Lab.



**Deloitte's extensive knowledge** provides valuable insights, a customized approach, and an understanding of diverse threats. Our Cyber & Strategic Risk offerings include *Application Security, Crisis, Resilience, & Brand, Data & Privacy, Detect & Respond, Identity, Infrastructure, Cloud, & Emerging Tech, and Strategy & Extended Enterprise*. Our broad experience enhances problem-solving, and regulatory compliance, and offers a broad cybersecurity approach.



**We help enterprise and government clients** increase visibility and knowledge of their data, usage, and risks. As well as identify their sensitive data types and where they are located across their environments.



## Contact us



**Jeff Lucy**  
Managing Director  
Risk & Financial Advisory  
Deloitte & Touche LLP  
[jlucy@deloitte.com](mailto:jlucy@deloitte.com)



**Brandon Abjanich**  
Manager  
Risk & Financial Advisory  
Deloitte & Touche LLP  
[babjanich@deloitte.com](mailto:babjanich@deloitte.com)



**Eric Dahlgren**  
Senior Manager  
Risk & Financial Advisory  
Deloitte & Touche LLP  
[edahlgren@deloitte.com](mailto:edahlgren@deloitte.com)



**Colleen Freeman**  
Manager  
Risk & Financial Advisory  
Deloitte & Touche LLP  
[cfreeman@deloitte.com](mailto:cfreeman@deloitte.com)





Soaring to new heights:  
Tagging and labeling in Aerospace & Defense  
**A launchpad to enhance precision, boost security, and propel innovation**

Data tagging and labeling forms a crucial part of a broad cybersecurity strategy for organizations in the Aerospace & Defense (A&D) industry. It plays a significant role in data management, security, and regulatory compliance that's specific to this sector. In this chapter, we'll discuss:

- Methods used to classify and prioritize data
- Consistent and specific tagging benefits
- Promoting participation and organizational change
- Advantages of automation

Here are top-tier data tagging and labeling practices for A&D, as well as methods to construct a data tagging and labeling strategy and to achieve numerous data management objectives.

### What is data tagging and labeling?

Data tagging and labeling plays a crucial role in cybersecurity. This process involves applying identifiers or metadata (tags or labels) to various types of cyber-related data, which are then used to classify, organize, track, prioritize, and protect data based on its sensitivity, importance, and the level of security required. These tags or labels might include details like the type of data (personal information, financial data, etc.), classification level (public, internal, confidential, restricted, etc.), source (cloud or on-prem), or other attributes that help in manage and/or protect the data.

### Why is this an important topic?

Data tagging and labeling enables efficient search, organization, and analysis and promotes appropriate data handling regarding security, privacy, and compliance requirements.

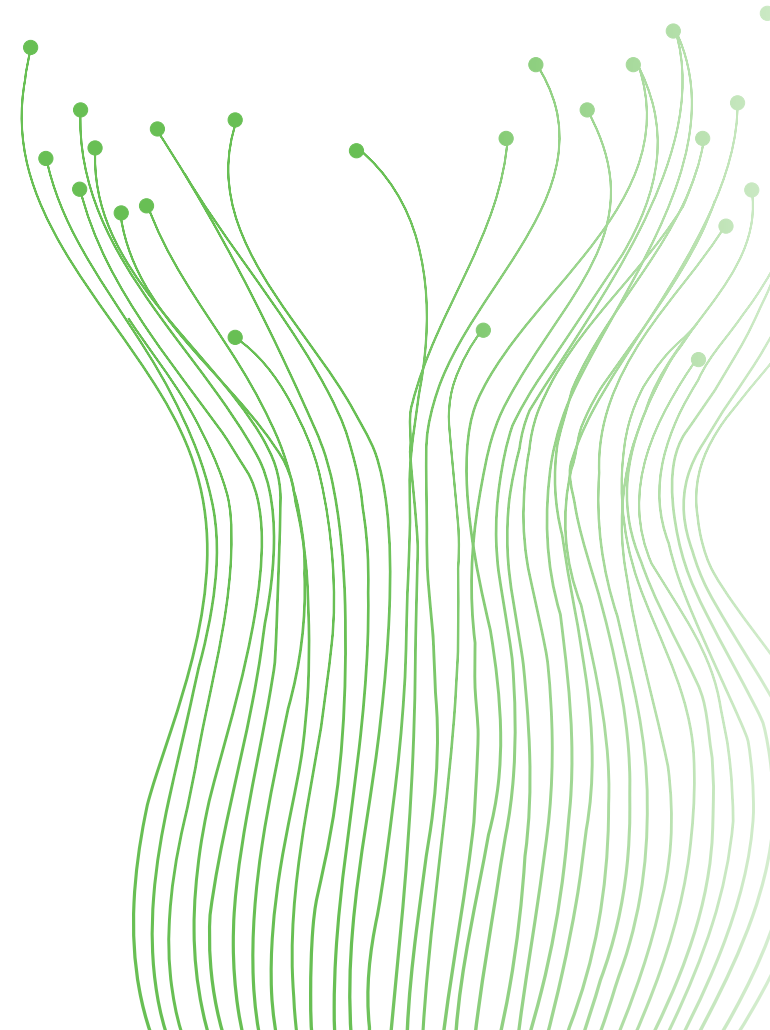
- **Foundational capability for analytics discoverability:** Tagging and labeling can aid in the categorization and organization of data, making it easier to find and use data for analytical purposes.

- **Improved data quality and consistency:**

Tagging and labeling data can help maintain quality and consistency by enabling easy identification, classification, and management of data, which in turn supports proper and reliable analytics and decision-making.

- **Advanced protection controls:** These controls may be implemented via tagging and labeling, i.e., access to certain fields could be blocked or restricted based on the data type, enhancing the security of sensitive information.

- **Compliance with regulations:** Given the growing importance of data privacy and protection regulations, data tagging and labeling can help achieve compliance by appropriately categorizing, protecting, and using data in accordance with legal requirements, including Cybersecurity Maturity Model Certification (CMMC) Controlled Unclassified Information (CUI), International Traffic in Arms Regulations (ITAR) and General Data Protection Regulation (GDPR)



### Data types and challenges: The differences in approaches

- In structured data classification, the process starts at the application level and then moves to the table/field level. Labeling is completed in a separate data inventory, supplied manually or by data discovery tools.
- Structured data tends to involve information technology and other data professionals who own the data or manage the inventory, who may be more likely to be familiar with the data's purpose or the underlying technology.
- Unstructured data typically requires manual classification and role-based access controls. This is due to the lack of a predefined model or format for certain file types. Common business file types store classification in metadata fields. Other file types, like computer-aided design (CAD) files or source code, are more typically managed by classifying within the repository, with labels also applicable to user-controlled repositories.
- Tagging unstructured data involves user training so that everyone who handles documents or sends emails in the organization understands the sensitivity level of the data, regardless of their knowledge and experience with data risks or technology.

### Solution for common challenges

- Implement a data governance and management system with data cataloging and role-based access controls to use the **data labels for tables and fields** to prioritize remediation, apply National Institute of Standards and Technology (NIST) 800-171/CMMC controls, and otherwise restrict access to required data only.
- Conduct broad **training and awareness programs** to educate users about the importance of effective data tagging, its impact on data management and analysis, and leading practices for tagging data carefully and consistently.
- Implement an advanced data classification tool that can help **identify and extract relevant information** from a variety of sensitive data types, i.e., Controlled Unclassified Information (CUI), Federal Contract Information (FCI), International Traffic in Arms Regulations (ITAR), Export Administration Regulations (EAR), and other Export Controlled data.
- **Automate the data tagging and labeling process** with algorithms, starting with a careful review of their effectiveness on a subset of the data, then apply the policies to large volumes of data, cataloging and refining it along the way.

For an effective data tagging program, clear guidelines must be established, and requisite training must be provided to help result in consistent and careful application of tags across the organization.



**NOW: Begin by building your foundation**

- **Determine the maturity of your organization's current state**
  - Evaluate the present state of the organization's capabilities, processes, and systems. Understand how mature or developed these aspects are by using a model to identify the current level of maturity and areas to improve.
- **Develop and socialize a road map for approach**
  - Create a strategic plan that defines the goals or desired outcomes and includes the major steps or milestones needed to reach them. Outline the scope, identify the resources needed (time, money, or staff), and set clear objectives or goals for the project. Socialize the road map by sharing and explaining this plan to relevant stakeholders to gain support for the approach.
- **Determine a prioritization approach**
  - The broad approach to data tagging and labeling starts by classifying across many applications—offering a basic comprehension of the data landscape but not getting into details like application tables/fields or specific user files.
  - The deep approach involves prioritizing the tagging and labeling of vital or frequently used data, requiring more focused resources but yielding valuable, targeted insights, which can be used for other reasons, like granular access controls.
- **Define use cases, scope, resources, and objectives to develop the project plan**
  - Outline specific scenarios or situations where a proposed system or project might be used (use cases).
  - Develop a standardized data tagging and labeling process that is consistently used across many data types. This can improve accuracy, may help with efficient data retrieval, and might support compliance with data protection regulations.

**NEXT: Design and test in your environment**

- **Acquire and implement the desired technical solution(s)**
  - Identify, purchase, and procure the applicable technology or software tools to collect, process, and analyze data in the data tagging and labeling process (e.g., data annotation, automated, collaborative tools).
  - Determine the sensitivity and importance of various data types and prioritize them based on their risk level. This helps apply appropriate security measures to protect critical or sensitive data.
- **Build and document data tagging and labeling for implementation**
  - Develop a data tagging and labeling strategy, which includes determining the categories or tags to be used and establishing guidelines for when and how to apply these tags for a tailored rollout in stages.
  - Creating detailed documentation that provides step-by-step instructions on implementing the data tagging and labeling strategy to assist with consistent application across the organization and provide a reference point for training and troubleshooting. Develop reference training materials for users.
- **Refine the design and monitor implementation**
  - Regularly track and read the implementation process to adjust the data tagging and labeling strategy as required to assist with consistent and effective application and address issues or challenges that may arise during the process.

**LATER: Expand data tagging and labeling to protect your enterprise**

- **Protect data and monitor processes as part of a larger data governance strategy**
  - Observe and track data to promote quality, security, and compliance with relevant regulations. Continuously correct inaccuracies, identify trends, and track data usage across the organization.

## Takeaways

- **What is data tagging and labeling?** Data tagging and labeling plays a crucial role in cybersecurity. This process involves applying identifiers or metadata (tags or labels) to various types of cyber-related data, which are then used to classify, organize, track, prioritize, and protect data based on its sensitivity, importance, and the level of security required.
- **What are common Data Tagging & Labeling challenges?** Poor quality data may lead to inaccurate tags and labels, which might impact data analysis and decision-making. Resistance to change throughout the organization can create challenges.
- **What should you do now?** Create a strategic plan that defines the goals or desired outcomes (and includes the major steps or milestones needed to reach them). Also, determine the specific scenarios or situations where a proposed system or project might be used (use cases).
- **What should you do next?** Acquire and implement the technical solution(s) for the data tagging and labeling effort. Fine-tune the technical design and process flow of the solution by testing the solution or application; develop training materials for users; and plan for implementation by considering anticipated hurdles.
- **What should you do later?** Determine and approach for prioritization. Protect data and monitor processes as part of a larger data governance strategy.

## Engage with Deloitte

### How Deloitte can help

Deloitte can help clients design, build, and operate progressive data tagging and labeling programs aligned with core business objectives. Relevant activities to maturing a program include, but are not limited to, the following:



Assess current state and define scope



Test and refine the solution



Establish requirements and road map



Design and document operational processes



Define use cases and identify resources



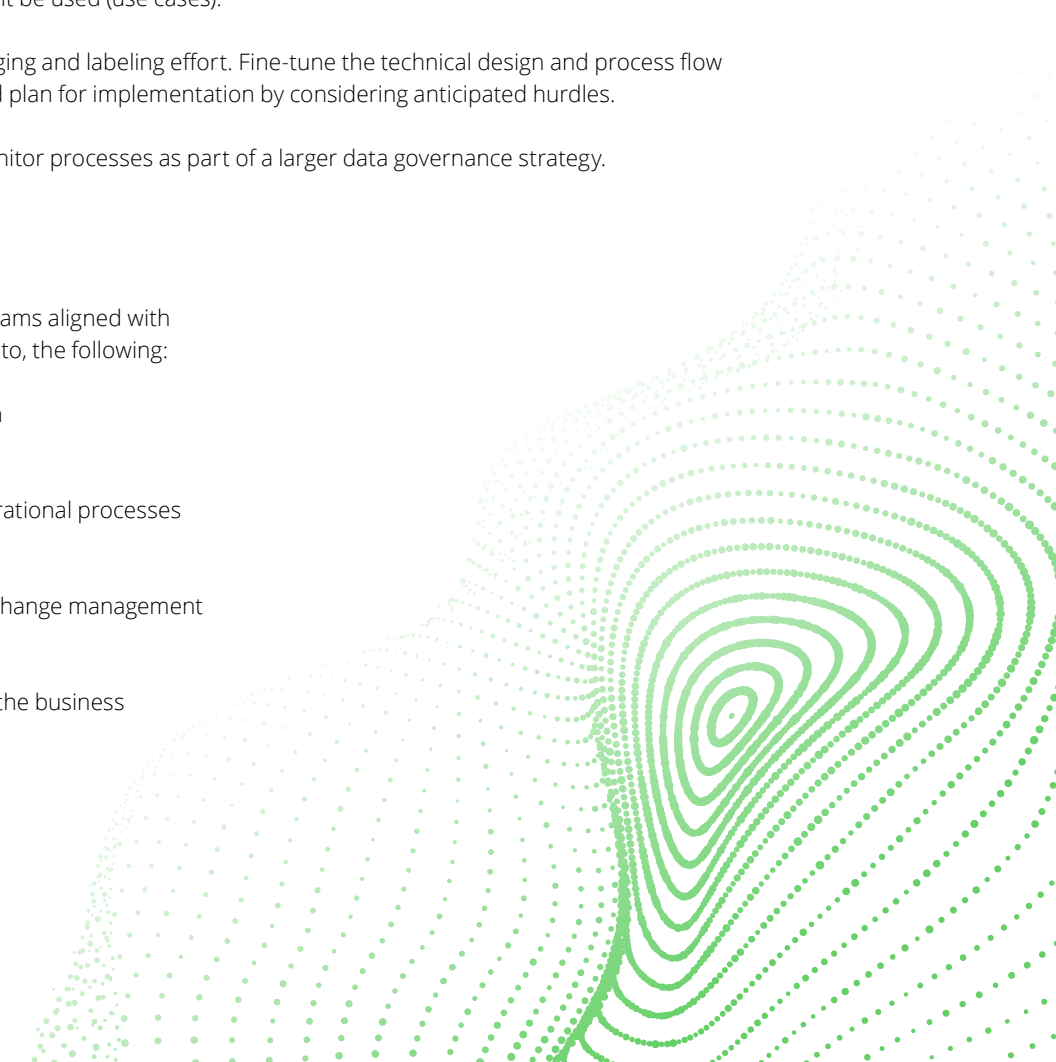
Assist with organizational change management



Implement and configure solution



Expand operations across the business



## The Deloitte difference



**We are data risk driven.** Data tagging and labeling is built into Deloitte's data protection and governance framework, which provides other services that can enable organizations to understand their data throughout its life cycle, including the controls in place to protect data.



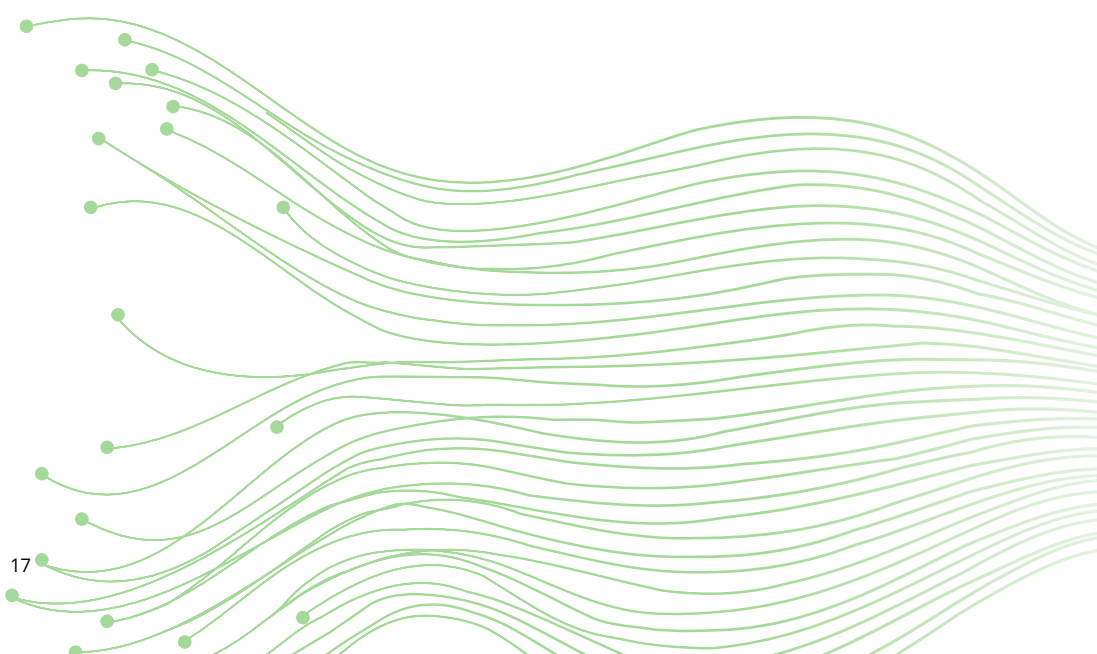
**Differentiators** include our value-based data risk management approach, dedicated managed services, strong relationships with leading vendors, and Data Protection Lab



**Deloitte's extensive knowledge** provides valuable insights, customized approach, and an understanding of diverse threats. Our Cyber & Strategic Risk offerings include Application Security, Crisis, Resilience & Brand, Data & Privacy, Detect & Respond, Identity, Infrastructure, Cloud, & Emerging Tech, and Strategy & Extended Enterprise. Our broad experience enhances problem-solving regulatory compliance and offers a broad cybersecurity approach.



**We help enterprise and government clients** increase visibility and knowledge of their data, usage, and risks, as well as identify sensitive data types and where they are located across their environments.



## Contact us



**Jeff Lucy**  
Managing Director  
Risk & Financial Advisory  
Deloitte & Touche LLP  
[jlucy@deloitte.com](mailto:jlucy@deloitte.com)



**Brandon Abjanich**  
Manager  
Risk & Financial Advisory  
Deloitte & Touche LLP  
[babjanich@deloitte.com](mailto:babjanich@deloitte.com)



**Eric Dahlgren**  
Senior Manager  
Risk & Financial Advisory  
Deloitte & Touche LLP  
[edahlgren@deloitte.com](mailto:edahlgren@deloitte.com)



**Colleen Freeman**  
Manager  
Risk & Financial Advisory  
Deloitte & Touche LLP  
[cfreeman@deloitte.com](mailto:cfreeman@deloitte.com)





Protect and monitor in Aerospace & Defense:  
Enhancing precision, boosting security, and propelling innovation



In the Aerospace & Defense (A&D) industry, protection and monitoring practices are critical components of a broad cybersecurity strategy. These practices are essential for data management, security, and regulatory compliance. In this release, we'll discuss the importance of:

- Identifying and prioritizing data
- Providing consistent monitoring
- Promoting a data protection culture
- Leveraging automation for protection

This information should help guide you to outlining top-tier protection and monitoring data governance practices for A&D, aligned with a larger data governance strategy.

### What is protect and monitor?

Protection and monitoring refers to the strategies and practices implemented to safeguard the security, privacy, and integrity of data. This involves implementing measures to prevent unauthorized access, use, disclosure, disruption, modification, inspection, recording, or destruction of information. Protection and monitoring also involves regularly tracking and reviewing how data is accessed or used to detect irregularities or breaches.

### Why do we think this is an important topic?

Protection and monitoring in data governance is crucial as it safeguards the security, privacy, and compliance of data. It allows for efficient tracking and oversight of data, facilitating appropriate handling of information, thereby reducing risks and enhancing regulatory compliance.

• **Regulatory compliance:** Many industries are subject to regulations regarding data protection and privacy. Consistent data monitoring and protection promote compliance with these rules, avoiding potential penalties. As regulatory requirements increase, provable program maturity is needed to be eligible to compete for contracts. Cybersecurity Maturity Model

Certification (CMMC), International Traffic in Arms Regulations (ITAR), and the Export Administration Regulation (EAR) are examples of this in the A&D industry.

- **Trust and reputation:** Businesses that effectively protect and monitor their data build trust with customers, partners, and stakeholders. This can enhance their reputation as a secure and reliable entity and provide a competitive advantage in contract bids.
- **Decision-making and business operations:** Reliable data is essential for informed decision-making and smooth business operations. Protecting data from corruption or loss and monitoring for accuracy and consistency help maintain data quality. This is crucial in meeting your Defense Federal Acquisition Regulation Supplement (DFARS 7012) requirements for the Department of Defense (DoD).
- **Financial impact:** Data breaches could result in significant financial losses due to penalties, recovery costs, and lost business. Effective data protection and monitoring can help mitigate these risks and prevent further penalties for late disclosure.



## Data types and goals

The A&D industry handles various types of data, like classified military information and controlled but unclassified data, including technical specifications, operational data, personnel records, and financial data—which are of significant sensitivity. The primary goal of data governance in this sector is to protect data by maintaining the confidentiality, integrity, and availability of data. This involves understanding and prioritizing sensitive data, establishing stringent access controls to prevent unauthorized access, use, or disclosure, and monitoring the data against disruption, modification, or destruction, whether inadvertently or maliciously.

Monitoring plays a critical role in the data governance framework. Regular scrutiny of data usage, access, and alterations helps identify and mitigate potential risks (e.g., data breaches or misuse, especially for prioritized sensitive data.) Monitoring also helps maintain compliance with various regulatory standards, which is essential in the A&D industry, and helps maintain stakeholder trust. Furthermore, it provides valuable insights that can enhance operational efficiency and inform strategic decision-making. As digital technologies continue to permeate the A&D industry, the scope of monitoring extends to managing the quality and life cycle of data, underpinning its accuracy, consistency, and relevance over time.

## Common challenges for protect and monitor

Updated requirements for programs like CMMC put higher pressure on provable maturity of controls.

- Current technical export control requirements for programs like ITAR and EAR potentially reduce flexibility for offshore resource mixes and cost reduction mechanisms.
  - Dealing with high volumes of data and alerts can make it difficult to identify genuine threats or issues. This could lead to important signals being missed or overlooked.
  - Highly sensitive data should be accessible to those who need it for decision-making or other purposes, but this accessibility can create security risks.
  - Data schemas may change over time, requiring updates to tagging and labeling practices to comply with security standards and regulations.
  - Protecting data from insider threats originating within the organization, whether intentional or accidental, requires understanding who truly needs access to data and diligent monitoring of how they handle it. This can be achieved through post-access controls like Data Loss Prevention (DLP) or correlating activity with threat feeds and User and Entity Behavior Analytics (UEBA).
- Unconventional data, such as satellite images, radar data, or free textual reports, can be challenging to protect and monitor due to its complexity and the lack of standard formats.
  - Managing the life cycle of unstructured data, from creation to disposal, in a cost-effective manner while enabling continuous protection can be challenging.
  - Identifying and implementing effective metrics for data protection and classification can present a significant challenge based on the complexity of managing sensitive data under stringent regulatory requirements. This underscores the need for establishing a framework that defines essential metrics tailored to an organization's specific circumstances. Some examples include:
    - **Data classification:** Percentage of data classified by sensitivity level, distribution of sensitive data across endpoints, cloud, and on-premises locations, and groups responsible for the classification of different types of sensitive data.
    - **Access controls and reviews:** Frequency of access reviews conducted, incidents of unauthorized access attempts, and violations of organizational access policies.
    - **Data Loss Prevention (DLP):** Number of DLP incidents, incident response time, percentage of data protected by DLP measures, and the amount and distribution of sensitive data types shared externally.

**NOW: Begin by building your foundation**

- **Assess the current state of your organization's security measures**
  - Evaluate the existing state of the organization's security capabilities, procedures, and systems. Use a model to comprehend the maturity level of these elements, identify the current security posture, and discover potential areas of improvement.
- **Identify use cases, scope, resources, and objectives to formulate the security project plan**
  - Define the specific scenarios or situations in which a proposed security system or project might be used (use cases).
  - Develop a uniform process for security practices that is consistently implemented across various data types. This can enhance accuracy, facilitate efficient data retrieval, and aid compliance with data protection regulations.
- **Formulate and disseminate a security road map**
  - Design a strategic road map that encompasses the security goals or anticipated outcomes and the stages or milestones required to achieve them. Detail the scope, ascertain the required resources (time, funds, or personnel), and establish distinct objectives for the security project. Increase awareness of the road map by circulating and elucidating this plan to various relevant stakeholders to secure their comprehension and backing for the approach.

**NEXT: Design and test in your environment**

- **Procure and deploy the required security solutions**
  - Identify, purchase, and implement security technology or software tools required for the monitor and protect process (e.g., data encryption, automated alerting of data movement, collaborative tools).
  - Evaluate the sensitivity and significance of different data types and prioritize them based on their risk level, which will aid in the application of appropriate protective measures for critical or sensitive data.
- **Establish and document a security strategy for secure implementation**
  - Formulate a strategy, decide on the security measures to be used, setting up guidelines for applying these measures, and plan a phased rollout.
  - Generate broad documentation that offers a step-by-step guide on implementing the strategy, promoting uniform application across the organization, and serving as a training and troubleshooting reference. Develop training materials for users that emphasize security-leading practices.
- **Fine-tune the design to oversee secure implementation**
  - Regularly monitor the implementation process to make required adjustments for secure and effective application.
  - Address security issues or challenges that may arise during the process promptly and effectively.

**LATER: Expand your protection and monitoring programs to secure your enterprise**

- **Formulate and document a transition plan for the security solution**
  - Design a systematic approach to transition the implemented security solution from its present state to its intended future state.
  - Outline the change management process, steps involved, and timeline.
  - Disseminate the transition plan amongst stakeholders to familiarize them with the process and their respective roles.
- **Extend the security program to other business sectors and cloud infrastructure through the onboarding and training of new personnel**
  - Broaden the protection and monitoring programs to include more areas of the organization, reinforcing data security across sectors. Educate new staff members on the security procedures and tools to enhance secure data handling and decision-making across the organization.









### Takeaways

- **What is protect and monitor?** Protection and monitoring refer to the strategies and practices implemented to provide for the security, privacy, and integrity of data. This involves implementing measures to prevent unauthorized access, use, disclosure, disruption, modification, inspection, recording or destruction of information.
- **What are common protect and monitor challenges?** The main challenges include managing the vast volume and quality of data, keeping pace with technological changes, complying with diverse data protection laws, balancing data accessibility with security, and mitigating human error risks.
- **What should you do now?** Assess the current state of your organization’s security measures, disseminate a security road map, and identify use cases, scope, resources, and objectives to formulate the security project plan.
- **What should you do next?** Procure and deploy the required security solutions, establish a security strategy for secure implementation, and fine-tune the design to oversee secure implementation.
- **What should you do later?** Oversee processes as part of the more broad data security strategy, document a transition plan for the security solution, fine tune the design to oversee secure implementation.

### Engage with Deloitte

#### How Deloitte can help

Deloitte can help clients design, build, and operate progressive protection and monitoring programs aligned with core business objectives. Relevant activities to maturing a program include, but are not limited to, the following:

- |  |  |
|--|--|
|  Assess current state and define scope   |  Test and refine the solution                 |
|  Establish requirements and road map     |  Design and document operational processes    |
|  Define use cases and identify resources |  Assist with organizational change management |
|  Implement and configure solution        |  Expand operations across the business        |

For effective protect and monitor programs, it is crucial to establish clear guidelines and provide sufficient training to support the consistent and diligent application of protective measures across the organization.

## The Deloitte difference



**We are data risk-driven.** Protection and monitoring is built into Deloitte's Data Protection & Governance framework, which provides various other services that help organizations understand their data throughout its life cycle, and the controls in place to protect data.



**Differentiators** include our value-based data risk management approach, dedicated managed services, strong relationships with leading vendors, and Data Protection Lab.



**Deloitte's extensive knowledge** provides valuable insights, customized approach, and an understanding of diverse threats. Our Cyber & Strategic Risk offerings include Application Security, Crisis, Resilience, & Brand, Data & Privacy, Detect & Respond, Identity, Infrastructure, Cloud, & Emerging Tech, and Strategy & Extended Enterprise. Our broad experience enhances problem-solving, regulatory compliance, and offers a broad cybersecurity approach.



**We help enterprise and government clients** increase visibility and knowledge of their data, usage, and risks. As well as identify their sensitive data types and where they are located across their environments.

## Contact us



### Jeff Lucy

Managing Director  
Risk & Financial Advisory  
Deloitte & Touche LLP  
[jlucy@deloitte.com](mailto:jlucy@deloitte.com)



### Brandon Abjanich

Manager  
Risk & Financial Advisory  
Deloitte & Touche LLP  
[babjanich@deloitte.com](mailto:babjanich@deloitte.com)



### Eric Dahlgren


Senior Manager  
Risk & Financial Advisory  
Deloitte & Touche LLP  
[edahlgren@deloitte.com](mailto:edahlgren@deloitte.com)



### Colleen Freeman

Manager  
Risk & Financial Advisory  
Deloitte & Touche LLP  
[cfreeman@deloitte.com](mailto:cfreeman@deloitte.com)





Cloud

Cloud in Aerospace & Defense:  
Enhancing precision, boosting security, and propelling innovation

In the Aerospace & Defense (A&D) industry, cloud practices are integral to a broad cybersecurity strategy, playing a pivotal role in data management, security, and regulatory compliance specific to this sector. This document outlines top-tier cloud data governance practices and methods to build a data governance strategy that will likely play a crucial role in achieving various data management objectives within A&D, such as:

- Centralized data access
- Enhanced tooling capabilities
- Standardized technology and data
- Integrated data platforms

### What is Cloud?

Cloud computing is a model for enabling convenient, on-demand network access to a shared pool of configurable computing resources. These resources could include networks, servers, storage, applications, and services. They can be rapidly provisioned and released with minimal management effort or service provider interaction.

### Why do we think this is an important topic?

Cloud is crucial for data governance as it enables centralized data management, giving business users access to high-quality data while reducing the effort to remediate data issues across the enterprise. It provides a suite of tools for data storage, business intelligence, and visualizations. It also allows for standardization of technology and data capabilities, thereby enhancing the overall efficiency and effectiveness of data governance.

### Benefits:

- **Decision-making and business operations:** Reliable data is essential for informed decision-making and smooth business operations. Protecting data from corruption or loss and monitoring for accuracy and consistency help maintain data quality.

- **Advanced tooling capabilities:** Cloud computing provides a variety of tools for data storage, business intelligence, and visualizations. These enhanced capabilities offer broad solutions for managing and interpreting data.

- **Standardized technology:** Cloud computing allows for the standardization of technology and data capabilities. This provides consistency in technology and user experiences, enhancing the quality of data governance.

- **Integrated data platforms:** Cloud computing supports integrated platforms that offer new data capabilities. These platforms provide significant technical benefits compared to traditional legacy systems.

### Data types and goals

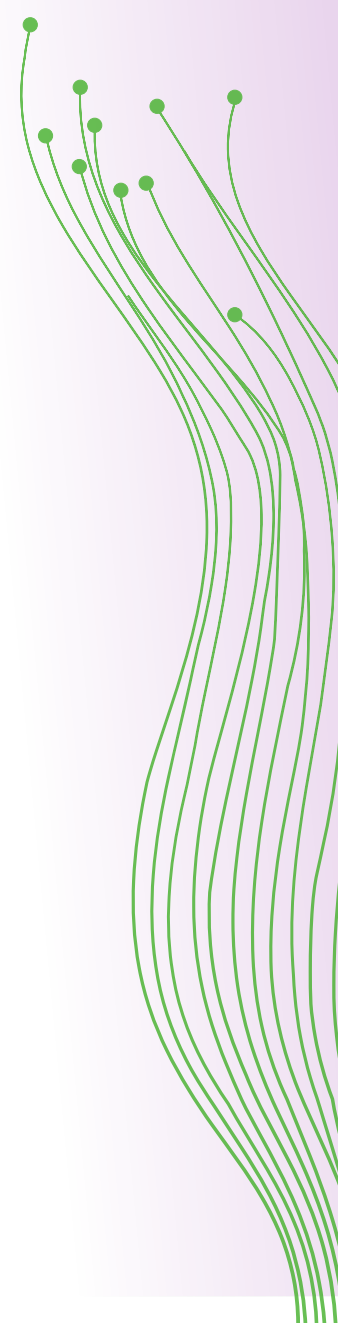
**Structured and unstructured data:** The A&D industry handles a wide variety of data types in its operations, ranging from structured data such as flight logs and maintenance records to unstructured data like satellite images and surveillance footage.

**Real-time data and Internet of Things (IoT):** With the advent of IoT and real-time data processing, there's also a significant amount of near real-time and real-time data produced by sensors and other devices. The data's nature, function, availability, and ownership can be diverse. For effective cloud-based data governance, it is essential to develop strategies that address these varied data types and manage them effectively, securely, and in compliance with industry-specific regulations.

### Secure and efficient data management:

The main goal of cloud implementation in data governance for A&D is to enable safe, efficient, and cost-effective data management. Cloud technology offers scalable and secure platforms that support interoperable data strategies, collaborative analysis, and services to expedite and scale research and development innovation with low latency.

**Advancing intelligence strategies:** For instance, an organization like the US Defense Information Systems Agency Joint AI Center is looking to advance its intelligence strategy with a shared cloud-native/edge platform across multiple mission areas. Thus, cloud implementation is aimed at harnessing big data, reducing data costs, creating more data analysis flexibility, and tapping into powerful artificial intelligence tools.



## Common challenges for cloud

- Managing and interpreting **unstructured data** like images, videos, and text files in the cloud can be challenging.
- Timely and accurate processing of **real-time data** in the cloud can be difficult.
- Protecting **sensitive data** like personally identifiable information (PII) and maintaining privacy in the cloud is a significant concern.
- Handling large **volumes of data** in the cloud can make it difficult to scale security and operational controls.
- Integrating and harmonizing data from **multiple sources** in a cloud environment can be complex.
- Migrating and transforming **legacy data** to be compatible with cloud technologies can be a daunting task.

## Enhanced cloud data governance strategy

### Cloud/data security posture management (CSPM/DSPM)

- **Continuous compliance monitoring:** Use CSPM/DSPM tools to continuously monitor cloud environments for compliance with security policies and standards. This helps the cloud infrastructure adhere to regulatory requirements and internal policies.
- **Automated remediation:** Implement automated remediation workflows to address security misconfigurations and vulnerabilities promptly. This reduces the risk of data breaches and enhances the overall security posture.

## Cloud access security broker (CASB)

- **CASB solutions:** Deploy CASB solutions to provide visibility and control over data and applications in the cloud. These solutions help monitor and manage cloud usage while protecting that data and controlling access.
- **Shadow IT detection:** Identify and manage unauthorized cloud applications and services used within the organization. This helps with mitigating risks associated with unapproved software and services.

## Data governance automation

- **Policy automation:** Use automation tools to enforce data governance policies consistently across cloud environments and, as a result, reduce the risk of human error.
- **Automated data lineage:** Implement tools to automatically track data lineage and allow for data traceability. This helps with understanding data flow and maintaining data integrity.

## Advanced identity and access management (IAM)

- **Zero trust architecture:** Implement a zero trust security model to provide methodical identity verification for every person and device trying to access resources. This minimizes the risk of unauthorized access.
- **Multi-factor authentication (MFA):** Enforce MFA across cloud platforms to enhance security, providing an additional layer of protection by requiring multiple forms of verification.

## Data quality management

- **Data quality frameworks:** Develop and implement frameworks to provide complete and consistent data. High-quality data is crucial for reliable analysis and decision-making.
- **Data stewardship programs:** Establish data stewardship programs to assign responsibility for data quality and governance. Data stewards play a significant role in maintaining data standards and resolving data-related issues.

## Advanced analytics and AI governance

- **AI and machine learning governance:** Establish governance frameworks for the ethical use of AI and machine learning in data analysis so that AI technologies are used responsibly and transparently.
- **Predictive analytics:** Use predictive analytics to forecast trends and make data-driven decisions. Predictive analytics can provide valuable insights and improve strategic planning.



## Recommendations for implementation

### NOW: Begin by building your foundation

- **Establish a cloud governance charter**
  - Formalize your cloud governance capability with guiding principles, stakeholders, roles, objectives, and voting procedures. It should also define the extent to which cloud governance will be incorporated into the existing governance approach.
- **Implement a concept of operations (CONOPS)**
  - Outline roles and functions of the governance and define how it will operate within the organization. It should include procedures such as cloud intake, multi-cloud guardrails, vendor sourcing, and resource tagging.
- **Create a cloud governance change management strategy**
  - Plan to bring stakeholder groups, communication channels, reporting structures, processes, training, and collaboration together to implement and execute cloud governance.

### NEXT: Design and test in your environment

- **Define and implement infrastructure**
  - Outline the specific cloud infrastructure that will underpin your data governance efforts.
  - Determine the appropriate databases, servers, and software tools required for your needs.
  - Implement accordingly, making sure it aligns with your governance policies and can adequately handle the type, volume, and complexity of the data you will be managing.
- **Develop data models**
  - Develop broad data models to guide how data is structured, stored, and accessed in your cloud environment, providing consistency and facilitating effective data management and analysis.
- **Perform testing of the cloud environment**
  - Perform careful functionality testing to help ensure elements work as expected, conduct performance testing to scrutinize if your setup can handle the required data loads, and do security testing to confirm that your data is adequately protected in the cloud.

### LATER: Expand cloud programs to secure your enterprise

- **Develop a financial operations strategy for cloud resources**
  - It involves creating a broad plan that includes budgeting for cloud resources, aligning human capital for managing these resources, and implementing tagging procedures for resource allocation and tracking.
  - A crucial part of this strategy is analyzing usage data to be cost-efficient and optimize resource utilization.
- **Align modernization goals and plans with training initiatives**
  - Modernization of the organization's systems and operations should be closely tied to training programs. These programs should be designed to provide your team with the required skills to implement, manage, and leverage new technologies effectively.
  - Evolve the team alongside the technology, enabling a smoother transition during modernization. Disseminate the transition plan amongst stakeholders to familiarize them with the process and their respective roles.
- **Extend the cloud program to other business sectors and product life cycle through the onboarding and training of new personnel**
  - Provide broad training on cloud technologies and their applications so that staff understand how to use the cloud effectively in their specific roles, thereby integrating cloud capabilities across various business sectors and throughout each stage of the product life cycle.









### Takeaways

- **What is cloud?** Cloud computing is a model for enabling convenient, on-demand network access to a shared pool of configurable computing resources. These resources could include networks, servers, storage, applications, and services. They can be rapidly provisioned and released with minimal management effort or service provider interaction.
- **What are common cloud challenges?** Managing, interpreting, and protecting unstructured, real-time, legacy, and sensitive data and handling large volumes of data from multiple sources.
- **What should you do now?** Establish a cloud governance charter to formalize governance capabilities, implement a concept of operations (CONOPS) to outline roles and functions, and create a cloud governance change management strategy to coordinate stakeholder groups, channels, structures, and processes for effective cloud governance execution.
- **What should you do next?** Define and implement specific cloud infrastructure tailored to your needs, develop broad data models for effective data management, and conduct functionality, performance, and security testing to operate securely in the cloud environment.
- **What should you do later?** Develop a financial operations strategy for efficient cloud resource management and usage, align modernization goals with training initiatives for effective technology transition, and extend the cloud program to business sectors and product life cycle stages through broad onboarding and training of personnel.

### Engage with Deloitte

#### How Deloitte can help

Deloitte can help clients design, build, and operate progressive cloud programs aligned with core business objectives. Relevant activities to maturing a program include, but are not limited to, the following:

- |  |  |
|--|--|
|  Assess current state and define scope   |  Test and refine the solution                 |
|  Establish requirements and road map     |  Design and document operational processes    |
|  Define use cases and identify resources |  Assist with organizational change management |
|  Implement and configure solution        |  Expand operations across the business        |

For effective implementation of cloud programs for data governance purposes, it is crucial to have consistent application of data protection measures across the organization, promoting diligent data management and security in the cloud environment.



### The Deloitte difference



**We are data risk driven.** Cloud is built into Deloitte's Data Protection & Governance framework, which provides various other services that enable organizations to understand their data throughout its life cycle, and the controls in place to protect data.



**Differentiators** include our value-based data risk management approach, dedicated managed services, strong relationships with leading vendors, and Data Protection Lab.



**Deloitte's extensive knowledge** provides valuable insights, customized approach, and an understanding of diverse threats. Our Cyber & Strategic Risk offerings include *Application Security, Crisis, Resilience, & Brand, Data & Privacy, Detect & Respond, Identity, Infrastructure, Cloud, & Emerging Tech, and Strategy & Extended Enterprise*. Our broad experience enhances problem-solving and regulatory compliance and offers a broad cybersecurity approach.



**We help enterprise and government clients** increase visibility and knowledge of their data, usage, and risks. As well as identify their sensitive data types and where they are located across their environments.

### Contact us



**Jeff Lucy**  
Managing Director  
Risk & Financial Advisory  
Deloitte & Touche LLP  
[jlucy@deloitte.com](mailto:jlucy@deloitte.com)




**Brandon Abjanich**  
Manager  
Risk & Financial Advisory  
Deloitte & Touche LLP  
[babjanich@deloitte.com](mailto:babjanich@deloitte.com)



**Eric Dahlgren**  
Senior Manager  
Risk & Financial Advisory  
Deloitte & Touche LLP  
[edahlgren@deloitte.com](mailto:edahlgren@deloitte.com)



**Colleen Freeman**  
Manager  
Risk & Financial Advisory  
Deloitte & Touche LLP  
[cfreeman@deloitte.com](mailto:cfreeman@deloitte.com)



● Product lifecycle management (PLM)

Product lifecycle management in Aerospace & Defense:  
**Enhancing precision, boosting security, and propelling innovation**

In the Aerospace & Defense (A&D) industry, the complexity and sensitivity of products necessitate broad management practices to enhance efficiency, security, and compliance. Product lifecycle management (PLM) practices are integral to an effective cybersecurity strategy, playing a pivotal role in data management, security, and regulatory compliance specific to A&D. By leveraging PLM, organizations can streamline operations, enhance collaboration, and maintain stringent security protocols throughout the product life cycle. Additionally, mechanisms to tag and label regulatory data at initiation within PLM may provide benefits in an organization's data protection journey. Initially tagging data at creation can simplify the protection process by reducing the rigorous effort of locating data in a co-mingled environment years later. Here are some notable aspects of PLM:

- **CMMC compliance and dissemination control of CUI data:** Helps enable CAD files and metadata to be tagged as CUI in order to meet CMMC requirements and increase security of files and metadata, including encryption, user authorization, restricted access and change control. Initiating tagging and labeling at the creation/initiation of data allows more control of the data prior to exiting the PLM boundary.
- **Unified view of product data:** Enhances accessibility and accuracy across the organization.
- **Complex design and collaboration management:** Improves the ability to manage complex product designs and collaboration processes effectively by integrating tools and workflows.
- **Standardization and error reduction:** Helps establish uniform standards for product data and technology, promoting consistency and reducing errors.
- **Enhanced data security controls:** Enables additional data security controls based on risks related to the products throughout their life cycle.

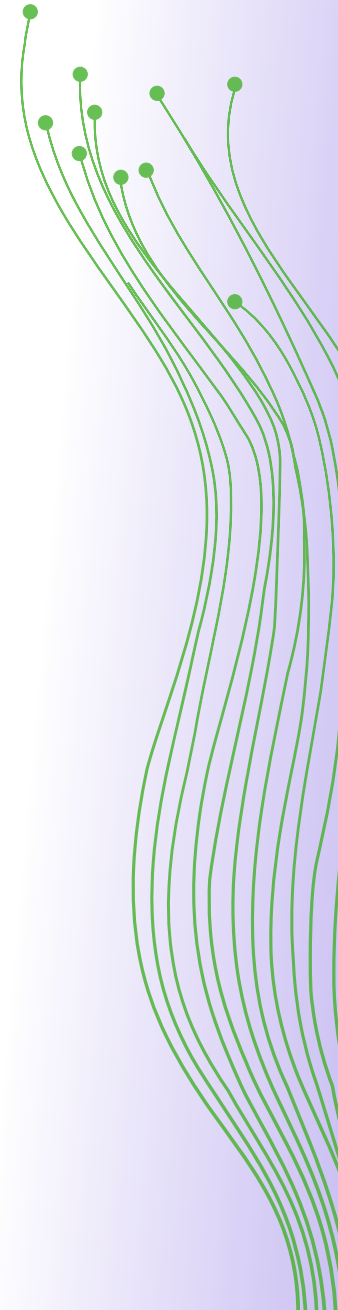
The following information should assist in developing top-tier PLM practices for the A&D industry. In addition, it could help you explore strategies to build an efficient PLM system, which could play a significant role in achieving various product management objectives within this sector.

### What is Product Lifecycle Management?

It is a systematic approach to managing the series of changes a product undergoes, from its inception and design to its retirement or disposal. This process integrates people, data, processes, and business systems to provide a product information backbone for organizations.

Our approach to implementing PLM in the A&D industry involves several components:

- **Assessment and planning:** Conducting a careful assessment of current PLM practices and defining a clear road map for implementation.
- **Integration of tools and workflows:** Leveraging various tools and workflows to enhance the management of complex product designs and collaboration processes.
- **Data management and security:** Establishing uniform standards for product data and technology, integrating multiple systems into a single platform, and implementing additional data security controls based on risks.
- **Governance and compliance:** Developing a governance structure that tracks data classification types, enhances security for unsupported file types, and supports compliance with industry-specific cybersecurity standards.



## Why do we think this is an important topic?

PLM is essential as it consolidates product data, streamlines operations, accelerates the design-to-market process and drives cost reduction while improving product quality. Furthermore, it aids regulatory compliance, facilitates informed decision-making, and confers a competitive advantage by promoting efficiency, innovation, and customer satisfaction.

- **Efficiency and speed:** Streamlines processes, reduces time-to-market, and aids in informed decision-making, allowing organizations to swiftly react to market changes.
- **Cost and quality control:** Identifies and addresses inefficiencies, leading to cost reduction and improved product quality by maintaining a single source of truth.
- **Regulatory compliance:** Enables identification, creation and maintenance of sensitive data such as CUI, IP, restricted and confidential data while maintaining security control, aids in meeting regulatory standards and maintaining compliance.
- **Competitive Advantage and Cost Reduction:** Establishes a competitive edge by fostering innovation, enhancing customer satisfaction, and establishing a single repository of product metadata and files. Reduction to risk of non-compliance and time spent on identifying and managing restricted and sensitive data in multiple applications.

## Data types and goals

- **Data types and their importance:** A&D deals with data types that mainly include design specifications, manufacturing processes, supply chain information, and regulatory compliance data. These data types encompass computer-aided design (CAD) models, blueprints, product specifications, materials data, supplier information, test results, quality assurance records, and maintenance and service logs. The proper management and integration of these diverse data types are crucial to the integrity, safety, and compliance of A&D products throughout their life cycle.

- **Cybersecurity and operational data:** Additionally, crucial data related to cybersecurity, such as threat intelligence, vulnerability assessments, incident reports, and security protocols, are also managed within the PLM system. Operational and usage data collected from aerospace systems during operation is also vital, as it is used for performance analysis and predictive maintenance, enhancing the safety and reliability of aerospace operations.
- **Manufacturing records and data sensitivity:** Furthermore, detailed records of manufacturing processes, which include methodologies, machine settings, and environmental conditions, are vital as they directly impact the integrity and functionality of aerospace components. It's important to note that the data within a PLM system in the A&D industry is highly sensitive, given the nature of the products and the stringent regulatory requirements.
- **Governance activities and data classification:** PLM is also leveraged for critical governance activities, which includes tracking data classification types for unsupported file types that are not compatible with standard classification tools designed for Microsoft Office files and integrating additional controls where broader data protection falls short.
- **Data access controls and regulatory compliance:** PLM can coordinate a broad range of governance activities, from decision-making to establishing a source of truth, each tailored to data risks and configuration challenges. This involves implementing data access controls, encryption methods, and security protocols to protect data from unauthorized access, breaches, or cyber-attacks. Another industry PLM objective is to maintain regulatory compliance with industry-specific cybersecurity standards, such as those outlined by the Department of Defense (DoD) in the United States.
- **Cybersecurity integration and revision control:** By tying directly into the product teams' workflows, PLM can integrate cybersecurity considerations into each stage of the product life cycle, from initial design to disposal. This means considering potential cybersecurity risks during

product design, incorporating security features during the manufacturing process, enabling secure maintenance and disposal practices, and using revision control for broad visibility of historical data. Revision control is a vital aspect of PLM that allows for tracing changes made to product data throughout its life cycle, thus promoting transparency and accountability.

- **Secure product life cycle:** Ultimately, the goal is to create a safe product life cycle, which is particularly crucial in the aerospace and defense industry, where products often have national security implications.

## Common challenges for PLM

- Global product development data is often **decentralized**, which is instead stored in separate PLM or Enterprise Resource Planning (ERP) systems.
- Rationalizing **discrepancies** across these systems is difficult due to poor or incomplete data and lack of digitized attribute data which decreases quality of data and introduces risk of non-compliance for restricted, sensitive and confidential data.
- Different product **data management** systems can limit component consolidation, making bill of materials (BOM) comparisons more complex and cross-product family analyses more burdensome.
- Traditional PLM search is not broad enough to make rapid, **data-driven decisions** and drive high levels of reuse.
- There is no **stable environment** for new product development or product discontinuation.
- **Planning** tends to be ineffective, communication is limited, and there is a lack of reaction-driven commercialization mechanisms.
- **Swift implementation** of replacement parts for end-of-life (EOL) scenarios.
- Identify **suitable parts or substitute alternates** and track these substitutes throughout their life cycle.



### NOW: Begin by building your foundation

- **Establish a PLM governance charter**
  - A PLM governance charter is a foundational component that defines the structure of PLM governance. It includes guiding principles, essential stakeholders, roles, objectives, and decision-making processes. This charter outlines how PLM governance integrates into the existing governance framework in the A&D industry.
- **Implement a concept of operations (CONOPS)**
  - The concept of operations (CONOPS) details the essential roles and functions of PLM governance within the organization. It includes procedures such as product intake, harmonization of different product data management systems, and resource allocation specific to product life cycle management.
- **Create a PLM governance change management strategy**
  - A PLM governance change management strategy is a broad plan that integrates stakeholder groups, communication channels, reporting structures, processes, training, and collaboration. This strategy helps ensure the effective execution of PLM governance in the A&D industry.
- **Establish data quality measurement and monitoring**
  - Data quality measurement and monitoring involve developing key performance indicators (KPIs) that reflect the goals of the PLM strategy. Regular monitoring and reporting on these KPIs using dashboards determines data quality and integrity throughout the product life cycle. This component facilitates continuous improvement and helps promptly identify issues or areas of concern.

### NEXT: Design and test in your environment

- **Develop a PLM system architecture**
  - A PLM system architecture is designed to support the organization's needs in the A&D industry. It facilitates the management of product data, processes, life cycle states, and integration with other enterprise systems.
- **Initiate prototype testing**
  - Prototype testing involves developing a prototype of the PLM system and testing it in a controlled environment. This component identifies potential issues or challenges before full deployment, enabling required adjustments.
- **Conduct user acceptance testing (UAT):**
  - UAT engages end-users in the testing process before fully implementing the PLM system. UAT provides valuable feedback about the system's functionality and usability from the perspective of daily users, checking that it addresses the demands and expectations of the A&D industry.

### LATER: Expand product life cycle management programs to secure your enterprise

- **Incorporate cloud-based PLM systems**
  - Cloud-based PLM systems offer scalability, flexibility, and accessibility and can enhance collaboration among different teams in the A&D industry.
- **Implement broad security measures:**
  - Security measures include data encryption, secure user authentication, and regular vulnerability assessments. These measures protect sensitive information and manage compliance with industry regulations.
- **Continuous monitoring and improvement**
  - Continuous monitoring and improvement involves establishing processes for ongoing monitoring and management of the cloud-based PLM system. This includes tracking system performance, user feedback, and evolving industry needs to continually improve and adapt the PLM strategy.











### Takeaways

- **What is PLM?** It is a systematic approach to managing the series of changes a product undergoes, from its inception and design to its retirement or disposal. This process integrates people, data, processes, and business systems to provide a product information backbone for organizations. Importantly, PLM also addresses the challenge of managing file types beyond common documents and securing data for products that traditional tools may not adequately cover.
- **What are common PLM challenges?** Global product development data is often decentralized in separate PLM or enterprise resource planning (ERP) systems, leading to difficulties in rationalizing discrepancies, limitations in component consolidation, ineffective planning, and inadequate communication. Many of these factors hamper rapid, data-driven decisions and reaction-driven commercialization mechanisms. Additionally, working diligently toward efficient security for diverse file types and data formats presents a significant challenge.
- **What should you do now?** Establish a PLM governance charter defining the structure, implement a concept of operations detailing roles and procedures for governance, and create a PLM governance change management strategy that integrates stakeholder groups, communication, processes, and training for effective PLM governance execution in the aerospace and defense industry. This should include strategies to handle your product design file types and enhance data security measures beyond traditional classification and access capabilities.
- **What should you do next?** Design a PLM system architecture that supports your organization’s needs, initiate prototype testing to identify potential issues, and conduct user acceptance testing to confirm that the system’s functionality and usability meet the demands and expectations of end-users in the aerospace and defense industry. Determine that the architecture includes provisions for managing unsupported file types and implementing core data security controls.
- **What should you do later?** Incorporate cloud-based PLM systems for scalability, flexibility, and enhanced collaboration, implement security measures, including data encryption and secure user authentication, and establish ongoing monitoring and improvement processes for high-quality system performance and adaptability in the aerospace and defense industry.

### Engage with Deloitte

#### How Deloitte can help

Deloitte can help clients design, build, and operate progressive PLM programs aligned with core business objectives. Relevant activities to maturing a program include, but are not limited to, the following:

- |  |  |
|--|--|
|  Assess current state and define scope   |  Test and refine the solution                 |
|  Establish requirements and road map     |  Design and document operational processes    |
|  Define use cases and identify resources |  Assist with organizational change management |
|  Implement and configure solution        |  Expand operations across the business        |

For effective implementation of Product Lifecycle Management (PLM) programs in the Aerospace and Defense industry, it is essential to consistently apply data protection measures, promote diligent data management, and take steps toward efficient security in the cyber environment.

## The Deloitte difference



**We are data risk-driven.** PLM is built into Deloitte's Data Protection & Governance framework, which provides various other services that enable organizations to understand their data throughout its life cycle, and the controls in place to protect data.



**Differentiators** include our value-based data risk management approach, dedicated managed services, strong relationships with leading vendors, and Data Protection Lab.



**Deloitte's extensive knowledge** provides valuable insights, customized approach, and an understanding of diverse threats. Our Cyber & Strategic Risk offerings include *Application Security, Crisis, Resilience, & Brand, Data & Privacy, Detect & Respond, Identity, Infrastructure, Cloud, & Emerging Tech, and Strategy & Extended Enterprise*. Our broad experience enhances problem-solving and regulatory compliance and offers a broad cybersecurity approach.



**We help enterprise and government clients** increase visibility and knowledge of their data, usage, and risks. As well as identify their sensitive data types and where they are located across their environments.

## Contact us



### Jeff Lucy

Managing Director  
Risk & Financial Advisory  
Deloitte & Touche LLP  
[jlucy@deloitte.com](mailto:jlucy@deloitte.com)



### Brandon Abjanich

Manager  
Risk & Financial Advisory  
Deloitte & Touche LLP  
[babjanich@deloitte.com](mailto:babjanich@deloitte.com)



### Eric Dahlgren

Senior Manager  
Risk & Financial Advisory  
Deloitte & Touche LLP  
[edahlgren@deloitte.com](mailto:edahlgren@deloitte.com)



### Colleen Freeman

Manager  
Risk & Financial Advisory  
Deloitte & Touche LLP  
[cfreeman@deloitte.com](mailto:cfreeman@deloitte.com)

As used in this document, "Deloitte" means Deloitte & Touche LLP, a subsidiary of Deloitte LLP. Please see [www.deloitte.com/us/about](http://www.deloitte.com/us/about) for a detailed description of our legal structure. Certain services may not be available to attest clients under the rules and regulations of public accounting.

This publication contains general information only and Deloitte is not, by means of this publication, rendering accounting, business, financial, investment, legal, tax, or other professional advice or services. This publication is not a substitute for such professional advice or services, nor should it be used as a basis for any decision or action that may affect your business. Before making any decision or taking any action that may affect your business, you should consult a qualified professional advisor. Deloitte shall not be responsible for any loss sustained by any person who relies on this publication.

Copyright © 2024 Deloitte Development LLC. All rights reserved.