# Integrated/Centralized **Versus** Federated Insider Risk Management

*By: Frank L. Greitzer, Chief Behavior Scientist Cogility Software*

**Abstract:** Insider threats pose a significant and evolving challenge for organizations, often involving complex behavioral and technical indicators that span multiple domains. Organizations that set up insider risk management (IRM) programs must choose between alternative program governance architectures, which can range from **decentralized** IRM models, where functional areas operate independently and data governance responsibilities are distributed across different business units or departments, to **centralized** models that have a central authority or team (hub) that oversees and enforces policies and standards across the entire enterprise. Between these two extremes, the federated data governance model combines elements of both, with a central governing body providing guidance and oversight while individual components maintain some degree of autonomy. Drawing on industry best-practices and governmental guidelines, we argue that a unified, centralized, enterprise-wide hub model—integrating data from all domains and consistently applying holistic, whole-person analysis—offers superior detection of nuanced risk patterns, consistent policy enforcement, and efficient resource use.

## Introduction

Insider threats remain one of the most complex and costly challenges in modern organizations, often involving subtle behavioral indicators and technical signals that span multiple domains (Cappelli et al., 2012). Traditional approaches to Insider Risk Management (IRM) frequently operate in silos (Chambers, 2025), with separate teams addressing risks within their own functional areas—such as IT security, HR, fraud, and compliance. While this data governance approach offers autonomy and domain-specific expertise, it often fails to capture the "big picture," leaving blind spots that sophisticated insiders can exploit.

This paper argues that an integrated, **centralized** IRM approach provides a superior framework for detecting and mitigating insider threats. By aggregating data across all functional areas and applying holistic, whole-person analysis, centralized programs enable early detection of complex risk patterns, consistent policy enforcement, and efficient resource allocation. Drawing on industry best practices and governmental guidelines, we compare the strengths and limitations of varying data and program governance models, demonstrating why a unified, integrated approach is essential for organizations seeking to proactively manage insider risk in today's interconnected threat landscape.

## Comparing Models

In this section we describe and compare alternative program and data governance models. The goal is to implement a data management and decision-making approach that promotes data integrity, informed decisions, and accountability. There are three main models that organizations can adopt: centralized, decentralized, and federated (Symons, 2005). Each has its own structure, benefits, and risks (see Fig. 1): the best choice is a function of the organization's mission and priorities.

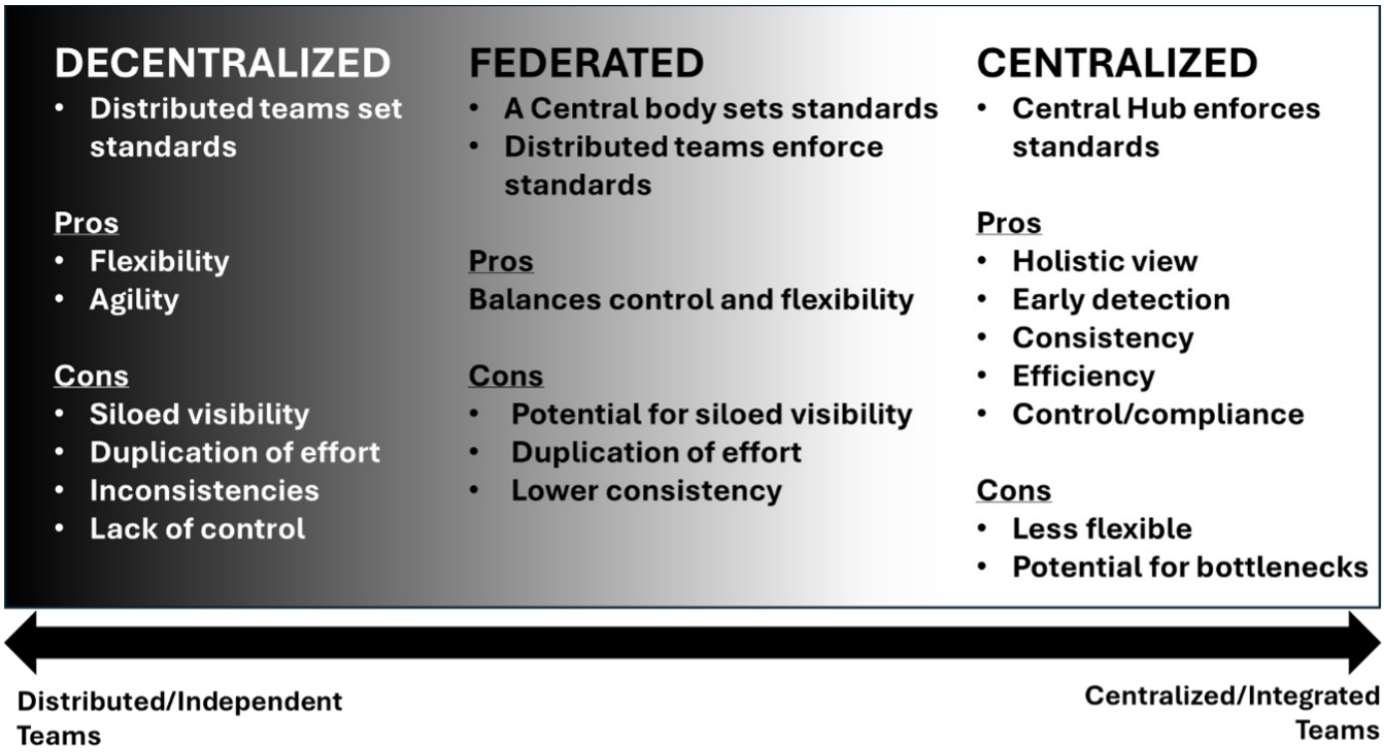


*Figure 1. Comparing program governance models*

### *Centralized Program*

In a **centralized** IRM program, the core IRM team serves as the central hub, aggregating data and signals from all sources—HR, Fraud, Security, Cyber, Legal, Compliance, etc. The hub performs integrated analysis and escalation, applying a "whole-person" approach to dynamically score individuals across multiple threat types (physical harm, IP theft, financial fraud, sabotage, etc.). Functional teams continue to gather information and act as subject-matter experts in their respective domains, but the **centralized** approach provides a holistic view of employee activity, enabling the detection of complex threats that may span multiple functional areas.

The following features of the **centralized** model should be considered when examining its efficacy as an IRM architecture:

- **Holistic View:** A **centralized** system consolidates data from various sources (e.g., IT systems, HR records, physical access logs) into a single oversight platform. This allows analysts to connect seemingly unrelated events across different domains (fraud, IP theft, physical security) to identify a complete picture of risk. By correlating disparate signals—such as a database access request (IT) following a negative performance review (HR) and an unusual wire transfer (Finance)—integrated systems identify complex threats that independent silos may miss.
- **Early Detection:** By integrating data, a **centralized** approach can often detect preparatory activities that might otherwise appear benign when viewed in isolation within separate functional areas. Mature analytic approaches leverage AI to provide predictive, whole-person risk assessments, moving beyond reactive technical alerts to proactive risk mitigation. For example, an employee researching online competitor information (source: network/IT data) while also working late (source: physical access data) and expressing dissatisfaction on internal forums (source: HR/communications data) presents a clearer risk pattern in an integrated system.



 

- **Consistent Policy Enforcement:** A single, central program fosters a consistent and uniform application of risk policies and procedures across the entire organization, reducing gaps and vulnerabilities that might arise from differing interpretations in separate departments.
- **Efficient Resource Allocation:** Centralization eliminates redundant efforts across functional areas, leading to more efficient use of resources, budget, and specialized personnel.
- **Better Compliance and Reporting:** Integration simplifies the process of demonstrating compliance with various regulations that often require a comprehensive view of risk, such as those related to data privacy and financial reporting.

▶ **Bottom Line:** While **centralized** program governance is sometimes criticized for potential processing bottlenecks, in the INFOSEC and IRM domains, these theoretical risks are outweighed by the practical advantages of integrated information flow, improved data sharing, and consistent application of policies and risk management practices.

### *Decentralized Program*

In a **decentralized** IRM program, there is no central hub; decision-making authority and data management responsibilities are distributed across functional areas (Fraud, Security, Cyber, etc.). Each team evaluates risks within its own scope using shared information. This model provides a more localized, independent approach to data governance and policy implementation.

The following features of the **decentralized** model should be considered when examining its efficacy as an IRM architecture:

- **Siloed Visibility:** In a **decentralized** model, risk analysis is done independently within functional areas (e.g., Fraud, Theft, IT Security), with local teams maintaining control over their domain-specific data. This allows different independent teams to define and implement individual policies and analytic practices that are not consistent across functional areas. In addition to producing inconsistent outcomes, this model encourages the development of information silos with local teams maintaining control over their domain-specific data.
- **Blind Spots:** While local teams may have a more nuanced understanding of their specific responsibilities, which potentially reduces false positives within that function, the lack of coordination and information sharing across functional areas can create “blind spots” at the intersection of different domains, making it easy for sophisticated insider threats to exploit gaps between departments (i.e., increasing false negatives). Thus, analysts may miss the “big picture” because they cannot see behavioral patterns emerging across other departments.
- **Duplication of Effort:** Multiple teams may independently investigate the same employee or activity from their specific perspective, leading to inefficient and redundant work.
- **Inconsistent Response:** The lack of central coordination can result in inconsistent or conflicting responses to insider incidents, potentially complicating investigations and legal actions.
- **Potential for Gaps:** Policies and detection mechanisms may not be uniformly applied, leaving vulnerabilities where insider activity could go undetected if it falls outside the narrow scope of a single functional area’s defined risks.
- **“Who Watches the Watchers” Dilemma:** The decentralized model creates an intractable IRM challenge for implementing controls and oversight of the analysts who are responsible for insider risk assessment, ensuring that security professionals themselves do not abuse their privileged access to sensitive information including PII. Unchecked power in security presents a massive risk. More centralized systems to monitor “the watchers” are critical for achieving robust governance concepts like Zero Trust.

▶ **Bottom Line:** A **decentralized** IRM model leads to fragmented visibility, as each functional area controls its own data and applies its own policies, creating inconsistent practices and isolated silos. This separation limits cross domain awareness, producing blind spots, duplicated investigations, and uneven or conflicting responses to insider threats.



 

### *Federated Program*

In **Federated** organizational structures are often described as hybrid models since they contain both centralized and decentralized components (Symons, 2005). There may be wide variation in the level of integration of federated programs, depending on how close they resemble a decentralized versus a centralized architecture (i.e., how far to the left or right in the representation of Fig.1 that the program operates). In other words, there is a balance in allocation of different functional areas in either central or distributed fashion. Ideally, key centralized components will include those that determine overall strategies, missions, and values (policies), as well as core technologies, IT infrastructure, and legal functions that ensure compliance. A model that assigns these functions to a central hub will be considered to more closely reflect the centralized architecture. A federated model that does not establish a central hub will allocate the implementation of policies/ procedures within the individual functional areas (Fraud, Security, Cyber, etc.). In that case, alignment occurs through governance and integration: Each team evaluates risks within its own scope using shared information. A hybrid federated architecture that combines a centralized policy-setting hub with decentralized execution is illustrated in Fig. 2 (after lifebit blog, 2025).

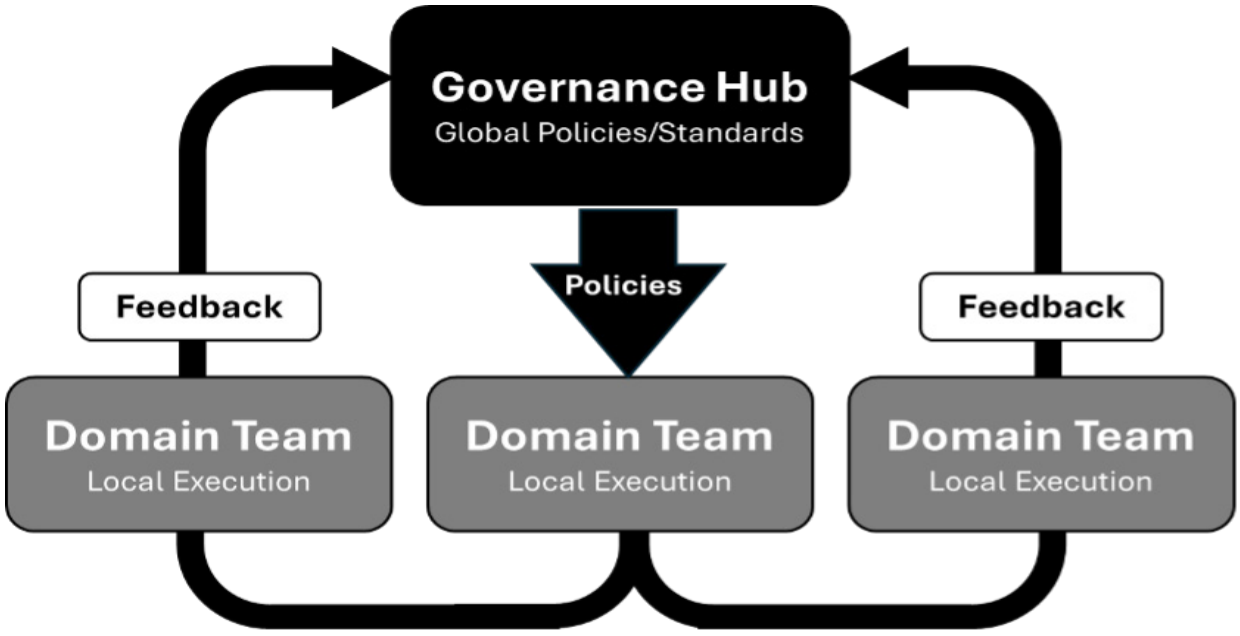


*Figure 2. Federated program architecture balancing centralized and decentralized functions*

Because the **federated** model has both centralized and distributed functions, its pros and cons represent a balanced combination of those associated with centralized and decentralized architectures. The following features of the **federated** model should be considered when examining its efficacy as an IRM architecture:

- **Siloed Visibility:** In a **federated** model, risk analysis is done independently within functional areas (e.g., Fraud, Theft, IT Security), with local teams maintaining control over their domain-specific data. As in the case of the **decentralized** model, the lack of coordination and information sharing (alignment) across these functional areas can create "blind spots" at the intersection of different domains. As noted previously, this means that analysts may miss behavioral patterns emerging across other functional areas, which can increase false negatives.
- **Complexity:** Coordinating multiple teams across IRM functions may be difficult without the integration provided by a central hub. Effective collaboration and information sharing mechanisms are crucial for successful implementation of this model.

- **Inconsistent Response:** Ensuring consistent practices and standards across the distributed functional area can be difficult; the lack of central coordination can result in inconsistent or conflicting responses to insider incidents, potentially complicating investigations and legal actions.
- **Duplication of Effort:** Multiple teams may independently investigate the same employee or activity from their specific perspective, leading to inefficient and redundant work.
- **Potential for Gaps:** Policies and detection mechanisms may not be uniformly applied, leaving vulnerabilities where insider activity could go undetected if it falls outside the narrow scope of a single functional area's defined risks.
- **"Who Watches the Watchers" Dilemma:** As in the **decentralized** model, the **federated** model may lack the ability to implement effective controls and oversight of the analysts who are responsible for insider risk assessment. More centralized governance systems to monitor "the watchers" are critical for achieving robust and secure performance in today's Zero Trust INFOSEC environments.

▶ **Bottom Line:** Although a **federated model** that centralizes data processing and analysis while delegating risk-assessment decisions can mitigate some information-flow bottlenecks, it frequently continues to face coordination and alignment challenges across functional areas. In such environments, the IRM team may have limited visibility into siloed functions such as cyber defense, personnel security, information security, and HR.

### *Discussion*

**Centralized** governance of IRM programs provides superior organizational outcomes because it enhances enterprise-wide visibility, enforces consistent control baselines, and enables more efficient use of scarce security expertise. Research on integrated security models demonstrates that unifying security functions improves information sharing and reduces silo-driven blind spots, thereby strengthening overall risk awareness and responsiveness (CISA, 2022). NIST's risk management guidance similarly emphasizes the need for organization-level governance structures to ensure coherent risk treatment and alignment with mission objectives, noting that fragmented or inconsistent approaches weaken risk posture (NIST, 2011). Industry analysis further finds that **centralized** governance increases efficiency by reducing redundancy, enabling cost-effective use of shared tools and talent, and providing leadership with clearer oversight and accountability—advantages that distributed models struggle to replicate (CSO Online, 2008).

#### How U.S. Government Departments Structure Their IRM Programs

Cogility Software currently supports two U.S. government agency/department IRM programs. In each case, these enterprises have centralized IRM hubs comprising a group of interdisciplinary insider risk analysts who perform holistic, predictive analytic (proactive) insider risk analyses. This enables the IRM programs to efficiently utilize scarce expertise across diverse domains (e.g., IT cybersecurity, behavioral science, legal) within a central hub, delivering consistent analytic risk assessments that are distributed to management who dispense appropriate mitigation or incident responses at the local sites.

Although critics argue that centralized structures may introduce decision bottlenecks, the literature shows that well designed centralized programs mitigate this risk through standardized processes, clear authority lines, and cross-functional coordination mechanisms that improve rather than impede incident response (CISA, 2022; CSO Online, 2008).

The effectiveness of IRM is increasingly defined by the ability to integrate technical signals with human behavioral context (Greitzer, 2019). The ability to analyze data across all functional areas is crucial for identifying the nuanced behavioral patterns that signal insider risk. Therefore, many industry frameworks and governmental best practices, such as those provided by the National Insider Threat Program (NITTF) and the Cybersecurity & Infrastructure Security Agency (CISA), advocate for a holistic approach to effectively mitigate insider threats. This is best achieved in a more **centralized** organizational structure.

Collectively, these findings support the conclusion that centralized governance yields a more consistent, efficient, and strategically aligned risk management posture.



 

## Summary and Conclusions

Insider threats represent a multifaceted challenge that demands a comprehensive and coordinated response. This paper examined a range of options for IRM program architectures from **decentralized** IRM models, where functional areas operate independently and data governance responsibilities are distributed across different business units or departments, to **centralized** models that have a central authority or team (hub) that oversees and enforces policies and standards across the entire enterprise; and including the hybrid **federated** model, which emphasizes autonomy within functional areas and allows for decentralized IRM procedures and analytic processes.

Considerations of **centralized** versus **decentralized** or **federated** program management requires accounting for impacts on efficiency, control, and responsiveness across an enterprise. The optimal structure is largely dictated by an organization's core mission and risk profile. For **decentralized** models (and potentially also for **federated** models) domain-specific expertise may be highly fragmented. While this offers a degree of agility, it may suffer from siloed visibility, inconsistent policy enforcement, and duplicated efforts—factors that create exploitable gaps for sophisticated insiders.

IT/business functions often favor a **federated** model, as it balances organizational efficiency with business unit autonomy and agility. The **federated** IT structure allows for decentralized decision-making, ensuring that the IT function closest to the business unit can respond quickly to specific needs, while still maintaining some overarching governance or shared services at the corporate level (e.g., Symons, 2005). While a **federated** approach may offer some departmental autonomy, an integrated/**centralized** approach is superior for INFOSEC organizations due to the nature of risk management and the need for consistent, enterprise-wide defense, including the need for effective systems that "watch the watchers." In INFOSEC, a single weak link can compromise the entire organization. The ability to analyze data across all functional areas is crucial for identifying the nuanced behavioral patterns that signal insider risk.

A **centralized** IRM model provides a holistic view of risk by aggregating signals from all functional areas and applying whole-person analysis. This integrated approach enables early detection of complex threat patterns, ensures consistent application of security policies, and optimizes resource allocation. Furthermore, **centralized** governance aligns with industry best practices and governmental guidelines, reinforcing its suitability for organizations seeking to proactively mitigate insider risk with coordinated responses to threats.

Ultimately, the ability to correlate technical indicators with behavioral context across the enterprise is critical for effective insider threat management. For organizations operating in today's interconnected and high-stakes environment, adopting a centralized IRM framework is not merely advantageous—it is essential for safeguarding assets, maintaining compliance, and preserving organizational trust.

## References


Agle, A. (2008). Information security governance: centralized vs. distributed. CSO Online. September 3, 2008. https://www.csoonline.com/article/522348/strategic-planning-erm-information-security-governance-centralized-vs-distributed.html

Cappelli, D., Moore, A., & Trzeciak, R. (2012). The CERT Guide to Insider Threats. Addison-Wesley.

Chambers, R. (2025). Break Down Silos for Visibility Into Enterprise Risk. MIT Sloan Management Review, 66(3), 11-13. https://www.proquest.com/openview/712c8ce1540150925ed75e2ef7fb2f51/1?pq-origsite=gscholar&cbl=26142

CISA (2022). Security Convergence: Achieving Integrated Security -- An Interagency Security Committee Best Practice. U.S. Department of Homeland Security, Cybersecurity and Infrastructure Security Agency, Interagency Security Committee. https://www.cisa.gov/sites/default/files/publications/Security%2520Convergence%2520-%2520Achieving%2520Integrated%2520Security%25202022%2520Edition.final_.pdf

Greitzer, FL. (2019). Insider Threat: It's the HUMAN, Stupid! Proceedings of the Northwest Cybersecurity Symposium, April 8-10, 2019. Article No. 4, pgs 1-8. ACM ISBN 978-1-4503-6614-4/19/04. https://doi.org/10.1145/3332448.3332458

lifebit (2025). Federated Governance: The Blueprint for Data Democracy. Lifebit blog, Sept 16, 2025. https://lifebit.ai/blog/federated-governance-complete-guide/

NIST (2011). Managing Information Security Risk: Organization, Mission, and Information System View. National Institute of Standards and Technology Special Publication 800-39. https://nvlpubs.nist.gov/nistpubs/Legacy/SP/nistspecialpublication800-39.pdf

Ravva, K. (2025). Comparative analysis of centralized vs. decentralized governance models for AI-BI in multi-cloud enterprises. Journal of Computer Science and Technology Studies, 7(6), 873-879. DOI: 10.32996/jcsts https://al-kindipublishers.org/index.php/jcsts/article/download/10102/8801

Symons, C. (2005). IT Governance Framework. Forrester Research. https://www.academia.edu/download/31849633/IT_Governance_Framework.pdf


Cogility's **Cogynt** Decision Intelligence platform is uniquely suited to support advanced, whole-person, proactive Insider Risk Management programs.

For more infomation, visit:
www.cogility.com

COGILITY


15495 Sand Canyon Ave.#150
Irvine, CA. 92618
sales@cogility.com
+1 949.398.0015