5 Risks Embedded in Your Legacy "System"

The Case for Migration and What Successful Adoption of New Technology Can Mean for Your Agency

OPEXUS | casepoint

A Change is Needed

Up to 51 years old

In a study of 65 legacy systems within the federal government, the average age of those systems was between 8 and 51 years old.

$350 million to operate

Collectively, these 65 legacy systems took nearly $350 million to support with the proper resources (e.g., electricity, space requirements, staff).

Offices of Inspector General (OIG) must work diligently to eliminate fraud, waste, and abuse from agencies throughout the federal government. Unfortunately, legacy systems hinder the auditing and investigatory processes due to siloed data, a lack of standardized workflows, insufficient collaboration tools (if any), and a needlessly complex user experience.

And the longer that OIGs depend on their legacy systems, the farther behind they will fall in their mission. This is because outdated legacy systems lack the capabilities, functionality, and flexibility OIGs need to:

- Stay on top of increasing workloads that are outpacing hiring rates
- Adapt to quickly evolving regulatory requirements
- Reduce their operational costs and save limited budgets
- Reduce their operational costs and save limited budgets

While change can result in more effort in the short-term, the migration away from legacy systems is crucial for Inspector Generals (IGs) to optimize spending, maximize productivity, and ensure government fraud, waste, and abuse are rooted out as quickly as possible. Otherwise, their office will remain vulnerable to these **5 critical risks of working in a legacy audit system:**

Risk #1: Data Integrity and Accuracy

Reduced data integrity and accuracy are downstream effects of human errors. Legacy systems intrinsically have more human touchpoints than modernized and automated systems, yet they also lack enforceable rules for data entry. Team members may create version control problems by emailing an outdated spreadsheet. Two or more auditors may unknowingly perform the same task and submit different findings or compile different data. And with a legacy system's limited data validation, the issues these human errors and missteps create can slip through the cracks.

Meanwhile, modern systems can check data parameters to ensure information is being entered correctly, flag and eliminate duplicate data entries, and enable audit supervisors to efficiently manage, track, and share case details.

Risk #2: Data Privacy and Cybersecurity

Modern systems better safeguard data because legacy systems have more blindspots and vulnerabilities. When these systems are designed exclusively for government professionals, they are also more likely to be StateRAMP and FedRAMP certified, ensuring appropriate security safeguards are in place for information and processes that reside or occur in the cloud.

Conversely, legacy systems are likely to have issues such as outdated security protocols and inadequate user authentication steps (e.g., no multi-factor authentication). They also have sparse or irregular security updates, if at all.

Risk #3: Change Management and Training New Employees

Legacy systems have minimal to no training or onboarding documentation, requiring your top, most efficient team members to spend their time and energy helping train new hires instead of closing out cases.

Legacy systems are also rife with non-standard processes, which further contribute to an already steep learning curve.

Risk #4: Audit Trail and Accountability

Without a built-in audit trail, legacy systems make it impossible to know what steps were taken by a user and when. You need adequate logging capabilities to track user activity and maintain transparency over who has accessed certain data. On the other hand, modern systems can reconstruct past actions and identify the source of errors.

Risk #5: Process Mapping and Documentation

Many legacy systems have no effective way to standardize processes or ensure compliance with important standards such as GAO's Yellow Book Government Auditing Standards. Other complaints include missing documentation to guide new users through key system features and steps required to complete common tasks. As a result, resources such as time and manpower are wasted on tracking down redundant information or completing tasks in a highly inefficient manner.

If an IG is unable to enforce repeatable workflows via a modern system, auditors will undoubtedly resort to third-party tools and apps to complete their work. And they will create information blindspots, generate duplicate data, and perform the same tasks multiple times while doing so. Additionally, training and onboarding becomes harder due to a lack of a consistent processes and steps for new hires to learn.

Why the Transition from Legacy to Modern Is a Worthwhile Change

Less prone to glitches

> *We always had big problems with our hyperlinks, our cross indexing, things like that.... (Microsoft) Word within the software would triple or quadruple the hyperlinks and fudge up the reports. We also had reports that would crash when you had too many hyperlinks in them, whether they were native or non-native. We haven't experienced any problems since transitioning.*
>
> — Dominic Gagliardi, DOJ OIG

Improved workflows between in-office and remote teams

> *The old legacy system was helpful, but there certainly were limitations to how one could openly collaborate. Within the [new] system, it's just 100% collaborative.*
>
> — Gregory Pachua, DOJ OIG

A FedRAMP-certified system

> *Cybersecurity was our primary concern, [and] the old system was not necessarily completely secure. FedRAMP certification was the selling point for us.*
>
> — Ergene Lee, DOJ OIG

Learn more about the risks of legacy systems and the benefits of change.
Visit: www.OPEXUSTech.com