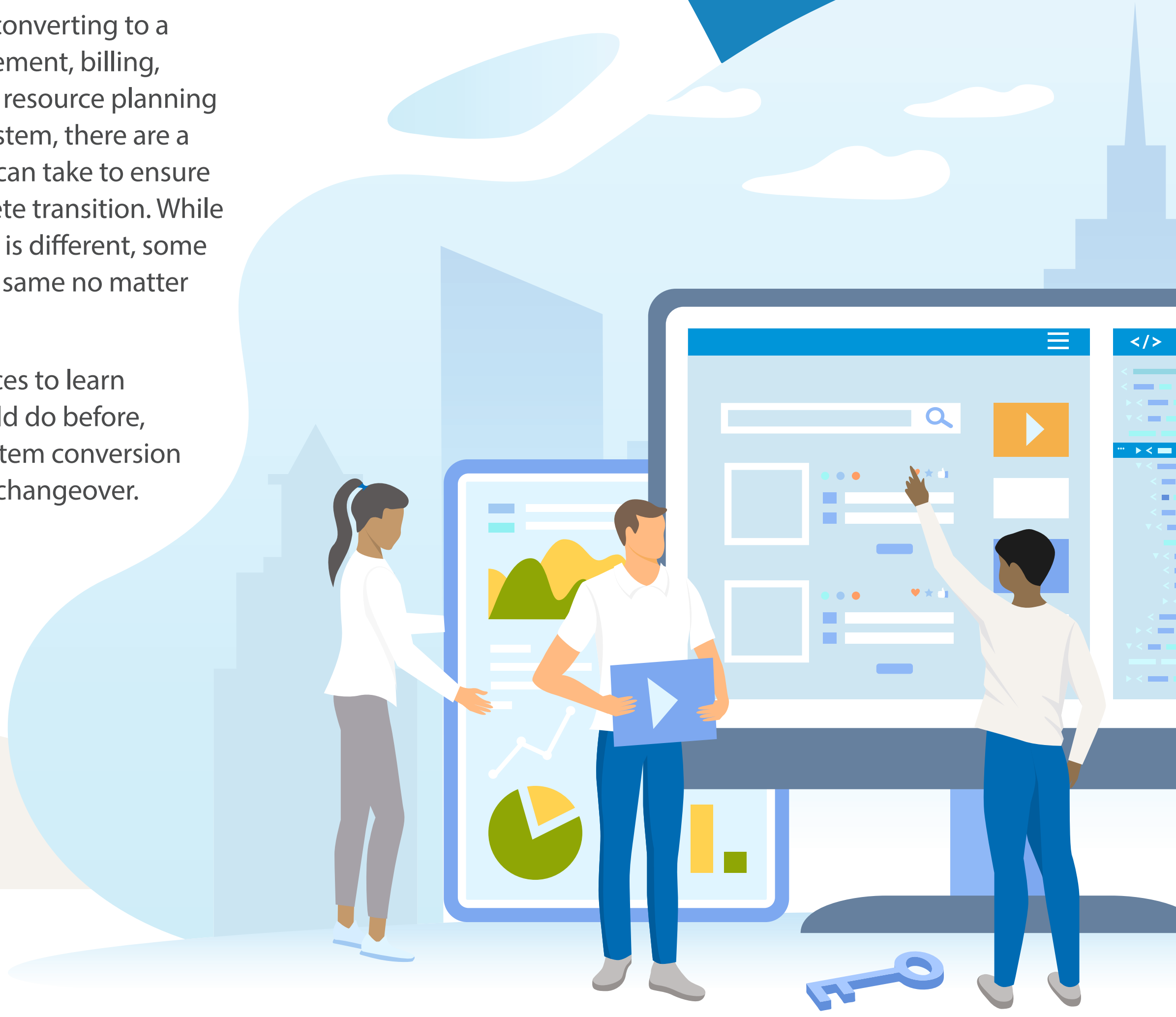
Center for Government Innovation

Office of the Washington State Auditor
Pat McCarthy

Best practices for implementing a new application system

If you're considering converting to a new financial management, billing, receipting, enterprise resource planning (ERP) or other new system, there are a number of steps you can take to ensure a smooth and complete transition. While each implementation is different, some best practices are the same no matter the type of system.

Use these best practices to learn about what you should do before, during and after a system conversion to ensure a seamless changeover.



October 2021

Before you purchase

1) **Evaluate the prospective system.** Before you purchase, you'll want to have enough understanding of the system to ensure it meets your needs. Does the new system calculate and communicate data in the way management and other users need? How will the new system affect existing processes? Does it have the approval and reporting functionality you need? Have you talked with other users to gauge their experience?

2) **Assess security options.** Evaluate each application system you're considering to determine if it meets the security requirements for your data and electronic infrastructure. Does the vendor use leading practices for designing and programming their system to minimize security and operational problems? Has a security expert evaluated the system to identify and address potential security vulnerabilities? While your vendor should provide guidance on how to securely implement any new system, *security is ultimately your responsibility*. You should perform due diligence to ensure security options align with your risk tolerance and are adequate for addressing your needs. Be sure to document your security evaluation and the expertise level of people involved.

3) **Contractual considerations.** You'll want to work with your legal counsel and security experts to properly develop contract requirements, but here are a few important topics to consider: Your contract should clearly outline expectations related to security protocols for how and when the vendor will have access to the data and system before, during and after the conversion. Consider how future patches and upgrades will be applied, and how technical support requests will be addressed, tracked and monitored. Additional topics to consider in your contract include responsibility for security breaches, security over a cloud-based service, or any known but unaddressed security weaknesses.

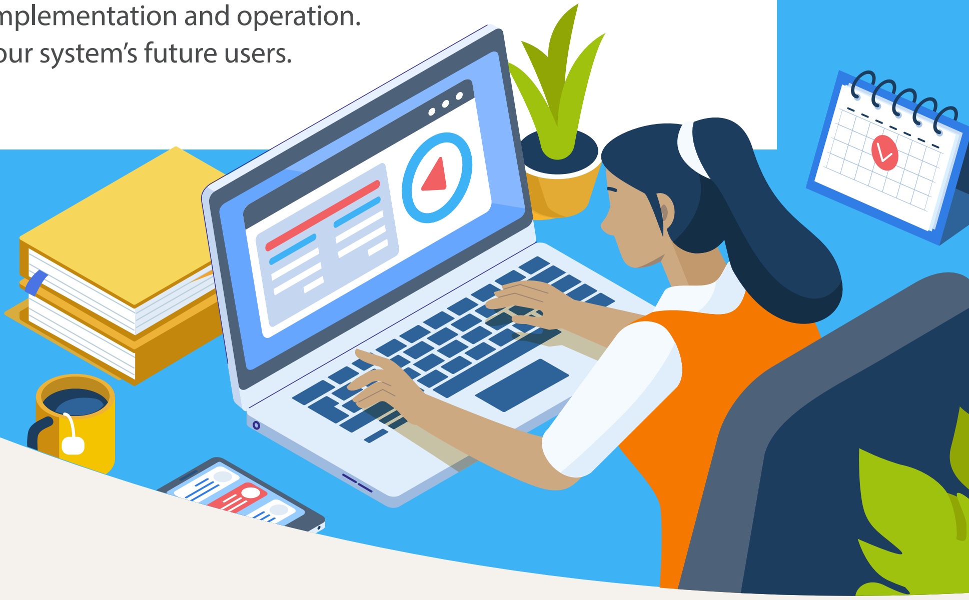
After you purchase, but before conversion

1) **Have a data cleanup plan.** Put in the work up front to examine your existing data to decide what data you'll want to transfer to the new system. This might include determining how it will be structured and whether it will transfer at a summary or detailed level. Make sure to document the rationale behind any significant data-related decisions or data changes.

2) **Test the new system.** Perform testing to deepen your understanding of how the new system will affect your processes. You should involve multiple users in the testing who are involved with, responsible for, or dependent on the data. Document your testing and keep this information. This documentation should include details like who performed the tests, the results, and confirmations that corrections were made (if necessary).

3) **Obtain system documentation.** New systems use different terminology and processes. It's important to make sure your employees and IT support staff have the resources and tools they need to learn the new system. This might include access to user manuals, but comprehensive help functions within the application itself are more common today.

4) **Provide adequate training.** Training should be early, ongoing, consistent, and role-specific so that employees are familiar with the new system and can use it before it goes live. Training before implementation is often overlooked, but it can minimize delays and errors in implementation and operation.
Keep those training resources for your system's future users.



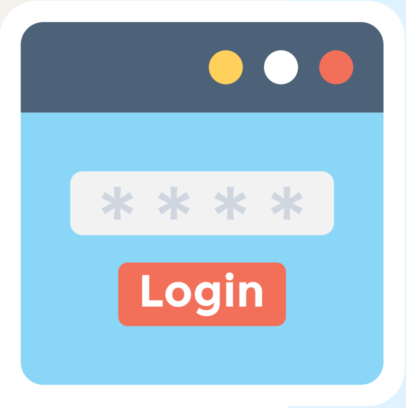
At the time of conversion

1) **Document crosswalks from the old to the new system.** A new system might have new or different terminology, account codes, processes and reports compared to your old system. Help your employees with the changes. Develop lists so that employees can track from the old system to the new system.

2) **Confirm that a complete and accurate data transfer happened.** Implement a method to ensure any data transfers (from the old to the new system) are complete and accurate. This might include comparing and documenting before and after reports, as well as documentation of the validation process, including who performed it, what the results were, and any corrections that were made. Multiple people involved with and responsible for the data should participate in the validation process. Remember, although it is acceptable to use a vendor to set up a new system—and even to convert data from the old system—*the integrity of the data is ultimately your responsibility.*

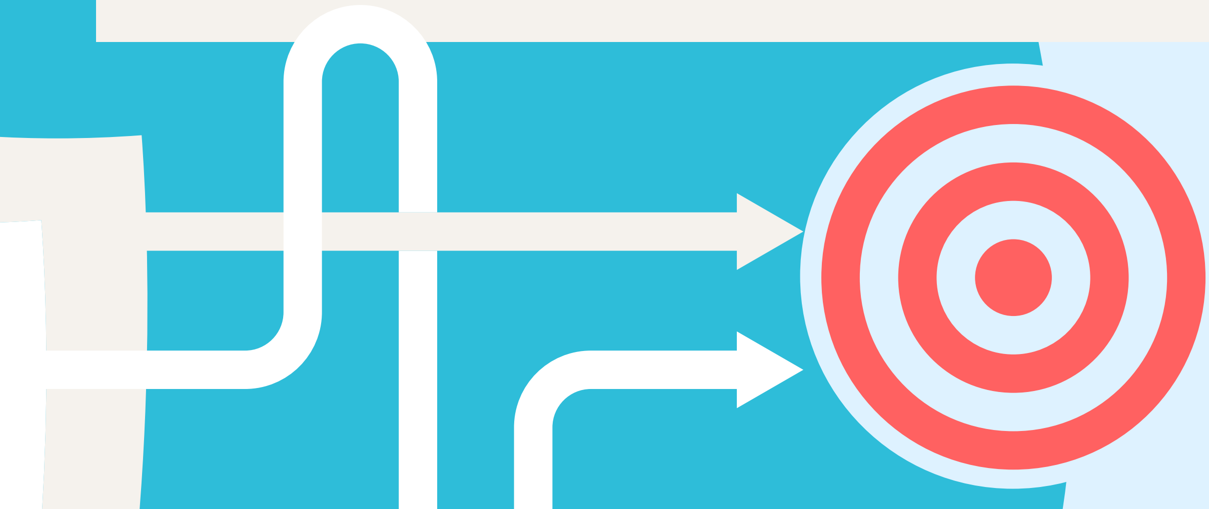
3) **Mitigate risks with elevated user access.** Employees are sometimes given higher levels of user access than they need during implementation so that they can get their work done, but this comes with some risk. If you elevate user access during the conversion, you should establish compensating controls to mitigate any risks you create. You should continue to evaluate and fine-tune user access throughout the first year of implementation to reduce risk.

4) **Monitor vendor access.** Vendor support is essential during the conversion process. However, your vendor should only have direct access to your system with your knowledge and approval. Remember, *the integrity and safeguarding of the data are solely your responsibility.* You will want to monitor vendor access to the system to ensure you are aware of any changes the vendor made, that you authorized them, and the system continues to perform as expected. It's also best to have policies and procedures for vendor access in order to minimize the risk of potential security holes that could compromise your data, and to help retain accountability over your data assets.



5) **Identify and disable default user IDs and passwords.** Default user IDs and passwords are very common in new systems and represent a high security risk. This is because this information is often public and shared among all systems from the same vendor, potentially allowing an attacker with this knowledge to log in and exercise administrative privileges. You'll want to check for these when you install any new application or hardware. First, identify default accounts by reviewing a list of users with system access and asking the vendor if there are any additional user IDs not included in the list. Then, disable all default user IDs or change all passwords associated with default IDs to long and complex passwords. To learn more, read this *publication* from the Cybersecurity & Infrastructure Security Agency (CISA).

6) **Implement multi-factor authentication.** If the new system is Internet-facing or contains confidential or sensitive information, you should work with your vendor to enable multi-factor authentication. This is a critical security feature that requires additional identity verification during the sign-on process, which can help you keep bad actors out of your new system. To learn more, read this *publication* from CISA.



After conversion

1) **Reevaluate user access within six months of deployment.** After conversion, it's time for a reevaluation to ensure employees have the system permissions they need to do their job—but no more. You don't want employees to have excessive system permissions because this can create a system security risk and violate segregation of duties. Make sure the person responsible for assigning security rights is knowledgeable about both the new system and the employee's job duties. It might require several departments working together to accomplish this. You should also adopt policies and procedures over the authentication and authorization of users. Your policy should cover how security rights are assigned, and also address how temporary leave, staffing reassignment and employee separation will be handled. Be sure to reevaluate user access on a regular basis or when there are further changes to the system or staffing.

2) **Communicate with your independent financial auditor.** Notify your auditor of any expected or in-progress conversions so that your auditor can plan accordingly. Remember, system conversions can affect the internal control structure and related processes of your operation. Therefore, your auditor might need to understand and review the conversion process, the new control processes and the data transfer. Additionally, keep system conversion documentation and maintain access to old systems, if possible, in preparation for your audit.

For assistance

This resource has been developed by the Center for Government Innovation at the Office of the Washington State Auditor. Please send any questions, comments or suggestions to *Center@sao.wa.gov*.

Disclaimer

This resource is provided for informational purposes only. It does not represent prescriptive guidance, legal advice, an audit recommendation or audit assurance. It does not relieve governments of their responsibilities to assess risks, design appropriate controls and make management decisions.