FASTPATH

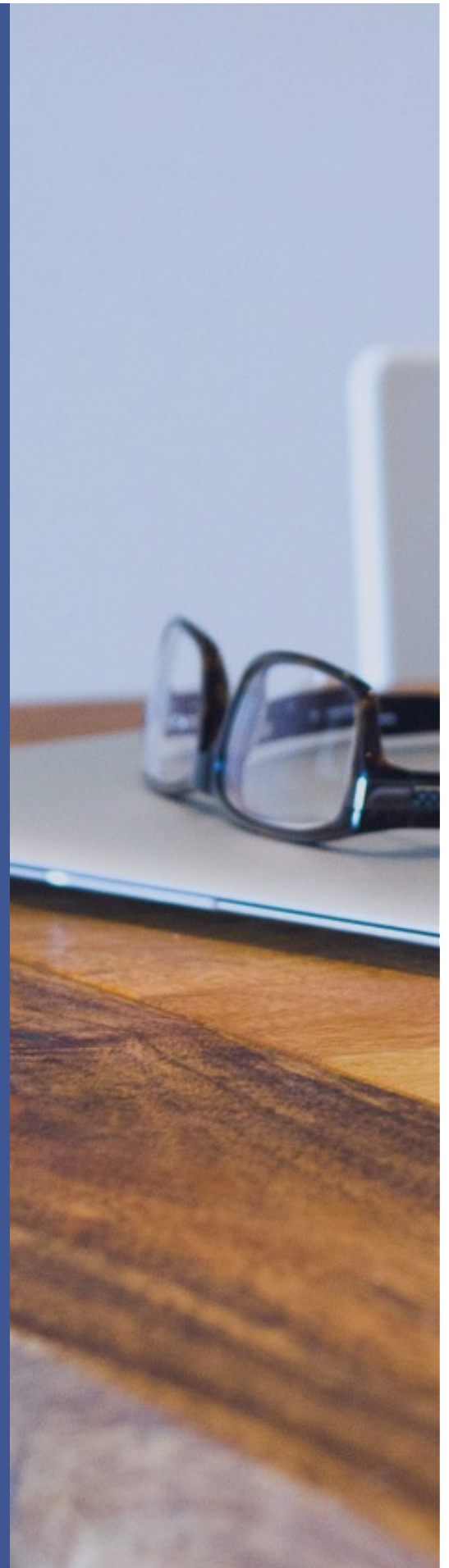# Security & Controls in Microsoft Dynamics AX

Understanding, Implementing, and Maintaining

Table of Contents

Introduction

Here are the necessary steps to take to secure your Microsoft Dynamics AX environment. Whether your on premise or using Dynamics 365, the tips here will help keep your data safe.

We are all concerned with security – in every aspect of our lives. We are especially concerned with security and control when it comes to our business processes.

In this Ebook, we will walk through the necessary steps to take to secure your Microsoft Dynamics AX environment. Whether you are on premise or using Dynamics 365, these tips will help keep your data safe.

Key Subjects

We have broken down the ebook into three basic sections.

- Understanding the basics, key terms and needs
- The initial setup of native security and controls
- Tools to maintain your security

If you have questions after reading this book, please feel free to reach out. The Fastpath team is always available to help.

-Dennis Christiansen

Security and Controls in Microsoft Dynamics AX

So, what do we mean when we talk about security and control within Dynamics AX?

We need to understand basic terms as they apply to security and controls in Dynamics AX. Security refers to the features in AX that apply to user application permissions, such as passwords and permissions. These features of security are built into the application. Controls, however, refer to procedures external to the application. A good example of an external control is Positive Pay, in which your bank compares payments with a previous transaction list before processing them.

Organizations should use a combination of Security and Control measures to ensure against operational or financial risks.

Understanding risk

Business risks to an organization may take different forms. Some are clearly intentional, such as fraud and theft. Others, however, might be accidental, like when a summer intern mistakenly creates a new general ledger account and starts posting transactions to it, throwing off your financial statements. A good balance of Securities and Controls will help mitigate both malicious and accidental risks.

With proper security and controls, organizations not only guard against risks, but they can help ensure that management's decisions are based on accurate and timely data. Controls can improve the visibility of processes. They can also help guard against errors to instill a greater measure of confidence in your teams. Finally, good controls help with compliance and save time preparing for audits.

If a business does not concern itself with security and controls, they open themselves up to a host of risks including errors, misstatements, and fraud. In some firms, security oversight has been relegated to the IT team, who may have little awareness of overall business processes and goals. This could lead to inappropriate data sharing or users with access they shouldn't have.

All businesses face risks; these might vary by industry, season, geography, company size, etc. Examples include fires, earthquakes, fraud, theft and financial misstatement.

Achieving a Proper Security Environment within Microsoft Dynamics AX

In this section, we will talk about how business risks relate to your key business systems, determine who should have security access and how to keep on top of security and controls in a way that ensures a balanced and workable business environment.

Mitigating risks within your key business systems

The first step in managing risk is to identify where the vulnerable spots are in your business processes. Companies should start by documenting business processes and then basing security on the business process maps. Identify high-risk processes and determine the systems through which those processes are run. Now, define risks, reviews, reviewers, and periodicity of reviews. Instead of auditing every process and access point, use a risk-based approach to monitor the high-risk ones. Identifying these points can significantly reduce the effort required to monitor ongoing controls. Lastly, organizations need to provide evidence that these reviews are actually taking place as scheduled. Without evidence, there is no way to confirm that reviews are actually happening.

Next, companies need to define who has access to your system. Admin users have permission to access any part of the system and will have the authority to add or delete any information from your Dynamics AX. This is a weighty responsibility and Admin users must understand the enormity of it and respect the trust placed in them.

Microsoft Dynamics AX provides options for monitoring changes made within the solution, but it's designed for troubleshooting, not auditing, and reporting on changes can be problematic. A better option is to identify and monitor only high-risk actions and changes to reduce the data being reviewed.

Companies should focus on key areas (vendors, configuration, cash receipts) and key fields within each area (payment terms, addresses, pricing). In each case, audit trails should indicate who changed a particular piece of information, why it was changed, and both the original and new values.

The main goal with security and controls should be to identify potential risks and have a plan for how to address them individually. Each security risk should have a documented corresponding control in place to mitigate it.

Maintaining a Proper Security Environment within Microsoft Dynamics AX

This section will discuss segregation of duties in Dynamics AX, the difference between application security and database security, as well as how to create appropriate audit trails in Dynamics AX.

Applications Security Versus Database Security

Most businesses focus on application security within their business systems, which then means they decide who can have access to which tables, windows and menus. But they should also determine how this will affect their database security.

For example, suppose a developer routinely gained access to a database and changed the remit-to addresses on several vendor accounts just before checks were run, then changed them back afterwards. Management would be unable to determine who was actually paid, mainly because there was no way to review what happened in the database. Just because a company has determined appropriate access levels for applications doesn't mean companies can assume database security. What companies need is a clear audit trail.

An auditor should be able to clearly see where the risks are and what a company has done to mitigate them. In part two of this series we talked about determining security risks and then addressing each risk with a specific control. But this is only useful if there is follow up for each control detailing risks and responses. Auditors want to see this; so, each time an employee responds to a risk, their users should save a PDF or print a report as evidence.

Some options to address this include the Activity Tracking tool built into Dynamics AX, or an add-on tool like Fastpath's Audit Trail. For a deeper look at setting up audit trails in Dynamics AX, read our blog post: Five Things To Think About when Setting up Audit Trails.

Segregation of Duties

Another safeguard is ensuring you have proper segregation of duties for your Dynamics AX system in place. Ideally, you want more than one person required to complete a task.

For instance, the general rule should be that no individual should be able to create a vendor account and also create a purchase order on that account; nor create a general ledger account and then post a transaction to it. Perfect segregation of duties may be impossible, but segregation of duties conflicts should be documented along with mitigation details for each conflict.

Having a detailed worksheet of risks and controls helps document for auditors that the company recognizes the risks, has provided controls to mitigate those risks, and has justified the assignment of duties. This documentation helps ensure that audits run more efficiently, and having the worksheet available will make certain that employees understand the risks and responses. That will reduce the likelihood of accidents or abuses occurring.

In the world of business, security can make or break you. So start to secure your AX system today.

Meet the Author

Dennis is the Director of Dynamics AX Sales at Fastpath, Inc. A graduate of Marquette University, way too long ago, and a member of the Fastpath family for almost five years, Dennis is a professional problem solver.

The Work

Working with hundreds of clients and prospects over the years Dennis has gained a deep understanding of the security, audit and compliance challenges facing companies today.

He has seen and heard how difficult it is for companies to manage security and compliance in Microsoft Dynamics AX and more recently Dynamics 365. That's why he gets so excited when he can engage the Fastpath team of security and audit experts to deliver solutions to help companies meet their challenges.

Behind the Work

So what does he do when not helping folks with their security and compliance needs? Dennis has a great family with two boys keeping he and his wife plenty active with sports and other activities. He loves to travel, spend time in the Northwoods of Minnesota, and on rare occasion, play some golf.

Automate Your Security

At Fastpath, our mission is to deliver software solutions that seamlessly empower our clients to take control of their security, compliance and risk management initiatives.

We pride ourselves on delivering the highest level of customer support. If you are looking to achieve the level of security that will satisfy your auditors and benefit your business, contact our team at Fastpath

BOOK A DEMO