# Top 10 Security Mistakes to Avoid When Setting Up Security in Dynamics AX/365 for Finance and Operations

FASTPATH

FASTPATH

# Avoid These Top 10 Security Gotchas When Setting Up Security

Security in Dynamics AX and Dynamics 365 for Finance and Operations (Dynamics AX/365FO) no longer needs to be a burden.

In this paper, we address the top 10 "Security Gotchas," otherwise known as the 10 security pitfalls that many companies fall into because they're frustrated or simply do not have time to configure their security the right way.

By keeping this list top of mind and following our 10 rules of thumb, you will be equipped with a clear understanding of how your company should be approaching security, and what the best tangible practices are to reduce security risk and cost.

## 1. Dynamics AX/365FO Security is Hard

If you think security is difficult, you are not alone. Everyone experiences security pains—even Alex, our director of Dynamics AX/365FO. He works with ERP security every day and there are still situations where he has to dig into the lowest levels within a system to determine what the correct security should be.

But don't worry. Take a deep breath and focus instead on avoiding common pitfalls which we will address in this paper. Don't let your frustrations with security prompt you to take the easy way out. We promise that this only gets you into more trouble.

We also offer a variety of resources at the end of the paper. These will help guide you in your hour of need.

## 2. Overprovisioning a User's Security

This is a common mistake you want to avoid at all cost. No matter how frustrated you feel about security controls, you never want to give a user more access than they need.

When pressed for time, companies frequently will assign users the System Administrator Role in order to allow them to perform a high priority task. Keep in mind that the majority of users should never have this kind of access.

We understand that figuring out the right security permissions takes time, but it is essential that you don't just go with the "easiest" solution.

Assigning a user as the System Administrator is the biggest mistake you can make because it is extremely difficult to undo.

Once you give a user System Administrator access, trying to take it back is like putting toothpaste back inside the tube:

- It lets the user bypass all other security controls.
- It gives the user too much freedom that they will not want to give up.
- And like many companies, you're likely to forget to go back and remove that access.

Keeping tight control over your security is more important than finding a quick solution in the moment. Therefore, when one of your users needs to perform an important task, think twice before immediately assigning them as the System Administrator.

## 3. Segregation of Duties Done at Duty Level Not Object Level

Microsoft gives you some out-of-the-box Segregation of Duties (SoD) that comes with Dynamics AX/365FO. But if you've ever used these built-in security features, you'll notice that there is no custom ruleset. It just gives you some generic rules that come with the tool. And if you only use the out-of-the-box rules, the SoD analysis will be carried out at the duty level and not the object level.

### What's wrong with carrying out SoD analysis at the duty level?

When the rules are done at the duty level, SoD happens within the hierarchy of role, duty, and privilege. That means if the user has duty 1 and duty 2, that's considered a conflict.

Unfortunately, this approach to security leaves major gaps because there are ways to get around the rules. For example, if you assign privileges (such as giving a user the System Administrator role), this bypasses all duties and ignores any inherent risks. You can also end up with **false positives** or **false negatives** within your system, which means you're not accurately representing true risk.

Change one thing at the duty level and you could unknowingly create new conflicts. That's why when companies take this approach, they need to revalidate their ruleset every single time someone makes a change (which becomes a tedious process).

## How should you carry out your SoD analysis?

Rather than approaching SoD from the duty level, you can instead approach it from the object level—or what we call a business process. The object level looks at the specific things (objects) that allow a user or role to perform a task. It goes deeper than duty level.

In Dynamics AX/365FO, these business processes are made up of menu items, data entities, tables, services operations, etc., that allow a user to edit, create, or delete a particular business idea or area.

If you conduct SoD analysis at the object level,

- You can't get around the ruleset you set up.
- You're also eliminating false positives and false negatives. It doesn't matter what changes you make to roles, duties, or privileges. Those changes will be processed, but the ruleset will extract out what objects that user or role has access to and report accordingly.

Conducting your SoD analysis at the object level is more secure, but it does take more time because you will need to do some customizing.

## How do you begin creating a custom ruleset?

We will discuss a couple methodologies in this paper for how to approach your security framework.

To help companies save time when designing your security, Fastpath offers a solution that delivers over 100 rules designed by an internal audit team that helps companies quickly identify and remediate SoD issues. Used by some of the largest accounting firms in the world, Fastpath provides a cross-industry best practice ruleset that can be further modified to fit your business needs.

For more information, check out our article on SoD analysis.

## 4. Least Privilege Not Implemented During Security Design

When you take the least privilege approach to your security, you are reducing a user's access so that they are only allowed to perform the tasks necessary to carry out their work. This is important because if a user has more access than needed, they can intentionally or inadvertently perform actions that could put your company at risk.

With this in mind, there are two main methods for setting up security.

### Top-Down Approach

This essentially means you're using the out-of-the-box security features that Microsoft provides in Dynamics AX/365FO. However, you're taking the native roles, duties, and privileges that come built-in and then modifying them directly or cloning them and removing the access that the user should not have.

### Bottom-Up Approach

This approach fully adopts the least privilege methodology. Rather than using the out-of-the-box security features, you can base your security on the different processes you require for your particular business. This helps you ensure that each user has the least amount of privilege assigned to them so that they only have the access they need to carry out their day-to-day operations.

### What are the benefits you get with the bottom-up approach?

1. It eliminates or stops users from making changes to an environment they shouldn't be able to do. Sometimes, users don't know the ramifications of a change they made. They may click on a button that has a much larger impact than realized. This method removes this scenario entirely.
2. It reduces the cost associated with mitigating SoD risks inherent in a user's role. Because the user is not overprovisioned, you are eliminating SoD risks at the user level.
3. And finally, you're reducing costs associated with licensing. When you overprovision a user, it's possible that the user requires a higher-level license in order to perform their tasks. Make sure you're not spending more money than you have to.

While the bottom-up approach is more secure, not all companies have the time to implement it. If this is your case, then it is okay to take on the top-down approach or even use a hybrid method. For example, you can use the least privilege approach around high-risk areas through prioritization, and then you could use the top-down approach for low-risk areas.

## 5. Security in Domain of IT Not BPOs

Your security setup and configuration maintenance are all handled at the IT System Administrator level and not at the Business Process Owner level. So while your IT System Administrators know how to set up security, they have no idea what the user should be able to do on a day-to-day basis.

Your Business Process Owners, on the other hand, know exactly what a user should be able to do and what access they should have, although they don't have the rights or permissions to go in and configure the security in the app. As you can see, this can create a disconnect between the IT System Administrator team and the Business Owners.

In order to have a successful security implementation, it's crucial to join both departments. Don't just leave security in the domain of IT. Both teams need to be in constant communication in order to validate which user should be able to do what.

During a security redesign, it can feel like the easiest way is to just let the IT folks run with security and provision access to users the same way it was in the older system. For proper controls and to ensure you don't fall into this "gotcha", there needs to be an approval process in order to make sure everything is built correctly, with the least amount of risk.

## 6. No Consideration of SoD During Security Design

The bottom line here is that it's important to consider SoD when you start building a security framework. From the very start, you need to be identifying all of the high-risk business problems or high-risk tasks that a user can perform in a system that you are creating. For example, are you assigning multiple tasks to a user? And by doing so, are you causing a SoD conflict?

In order to make sure you are not creating more SoD risks as you build out user roles, you should first define what your users do in a day. Then, based on those user flows, decide what roles need to be assigned for those business processes.

As you start building out roles, you also need to be sure you're checking for SoD conflicts every step of the way (this is why having a custom ruleset is great to have on hand so that this validation process doesn't become tedious).

### What happens if you don't consider SoD during the security design?

Without considering SoD, your business is vulnerable. Poor internal controls could lead to fraud or asset misappropriation. For example, you wouldn't want one user to be able to create a vendor and then pay that vendor without any oversight. You want to always follow the least privilege approach that limits a user's access to a system to only the tasks they need to perform day-to-day.

It is important to understand that it is impossible to remove all SoD risks in an environment. It would take unlimited resources to have zero SoD risks, however, it does help significantly when you are actively minimizing risk to the best of your ability by prioritizing security.

## 7. Security Low Priority for Project Team

Security might not be the first thing your company wants to tackle when they're looking at an upgrade or new implementation. Oftentimes, it gets put at the bottom of the to-do list because many believe it doesn't have immediate ROI. But that's not necessarily true.

We already mentioned that by adopting the least privilege approach, you could be cutting down on user licensing costs. Microsoft oftentimes requires users with higher privileges to hold more licenses.

But the biggest reason why security should matter to business decision makers is the cost of having to mitigate SoD risks.

### What's the cost of mitigating SoD risks?

If you're not taking SoD into consideration, the cost to your company could be substantial. As we've mentioned before, when a user is overprovisioned, it's easy for them to create risk either intentionally or inadvertently. Don't give any one user the power to jeopardize your company's finances. One way to prevent this is by not relying on the out-of-the-box security features that come with Dynamics AX/365FO.

## 8. Process Controls / Mitigations Not Part of Security Design

In addition to considering SoD when you're building a security framework, it is also critical to include process controls and mitigations too. The reason why is because it's not feasible to remove every single SoD risk from your environment. As mentioned before, this would take too many resources, so the next best thing we can do is to set up a process control and mitigation system around the remaining risks.

### What does a mitigation / process control look like?

A control can either be something internal to the application, like a workflow, or something external, like requiring manager approval. The whole idea is that you want to be able to stop the user from performing one or more parts of the SoD risk or require a review of this user having this access (like a certification or a transaction log).

## 9. User Temporary Role Assignments Become Permanent

This one sounds obvious, but a lot of companies fall into this trap. When companies assign a role to a temporary user or contractor, they oftentimes forget to terminate it later. They also may forget to run a SoD analysis after creating the role to confirm that it doesn't have any inherent risks.

When you're creating a new role, ask yourself these questions:

1. Is it permanent or temporary?
2. Is there a process for removing it?
3. If it is temporary, who specifically is responsible for removing it? And on what schedule?
4. Does the new access create SoD conflicts for that user?
5. If there are SoD conflicts, do you have mitigation / process controls around them?

## 10. Dilution of 'Go-Live' Security Design

Even if you successfully steer clear of all the "Security Gotchas" listed so far, it will be all for nothing if your security model becomes diluted. Security is not a one-time setup and then you're done. You must perform periodic reviews of user access.

### Why do I need to perform periodic reviews?

- When you add new users, you need to validate that they are not being over-provisioned.
- You need to ensure you have a process for removing temporary access when it is given to a user.
- To ensure temporary users (such as contractors) are being terminated after their assignment ends.
- Finally, to ensure users who leave the company are terminated correctly.

Again, setting up security correctly is a great start, but you have to do these reviews to make sure that access is controlled at all times.

## Conclusion - What can you do to make sure you're not falling for any of these "Security Gotchas"?

- Look for (free) resources surrounding security
- Start early and start often
- Security design and process control / mitigation design should be done together
- Don't have a 'siloed' project and instead join your IT System Administrator team with your Business Process Owners
- Identify high-risk areas of your business to determine SoD conflicts
- Determine your security design methodology and follow it (whether that's the top-down, bottom-up, or a hybrid approach)
- Understand security is not a one-time exercise
- Have a process for user role assignment

As you continue on your security journey, check out the resources below from our own security experts:

D365FO Security Blog
D365FO Security Audit Field Manual
D365FO Resources From Fastpath
On-Demand Webinar: Top 10 Security Gotchas in D365FO/AX
eBook: Develop & Implement Least Privilege Security in D365FO

## About Fastpath

Founded in 2004, Fastpath has deep expertise in audit, security, and compliance, with multiple Certified Internal Auditors on the team. Fastpath has global partnerships with several audit firms and a client base which spans across multiple industries within both publicly traded and privately-held companies. Fastpath Assure® is a cloud-based audit platform that can track, review, approve and mitigate access risks across multiple systems from a single dashboard.

Contact us to discuss your needs or for a product demonstration. Visit our website for additional resources like this eBook, on-demand webinars and more.