Due Diligence™
Separation of duties auditor for BPCS and ERP LX

In a nutshell: why your company should pay attention to separation of duties

Internal control principles and good business practice demand identification and management of separation of duty conflicts. It's not optional. It's not new. The principles were well known and practiced by world class organizations decades before IBM shipped the first System/34.

Enterprises have told us that attention to separation of duties isn't on the front burner because they've never heard about a situation at their company when a weakness was exploited. That line of reasoning is invalid; it rests on an 'argument from silence.'

Another rationale for putting off separation of duties work in BPCS/ERP LX is that it's way too much work. This document introduces **Due Diligence**, a software product which cuts the risk identification step down to several minutes.

Run silent run deep

The 1958 war film called "***Run Silent, Run Deep***" illustrated how submarines evaded detection by diving deep enough and staying quiet long enough. The submarine commander in the movie (Clark Gable) and his executive officer (Burt Lancaster) didn't attract attention by floating their ship on the surface and shooting off flares.

In like manner, separation of duties problems embedded in your BPCS / ERP LX user profiles don't attract attention to themselves either. They typically remain undetected for a long time ...and that's an internal control vulnerability for many enterprises.

The internal control risk: separation of duties (SOD)

Unbeaten Path's advice is to invest time finding and stomping out all the risk in BPCS/ERP LX rather than investigating what went wrong after the fact. That's easier said than done.

These three obvious conflicts aren't sitting silently hundreds of fathoms deep on the sea floor ...

ACP100 Vendor Master Maintenance	+	PUR500 P.O. Release/Maintenance
ORD700 Order Entry	+	ACR500 Cash and Memo Posting
ACP710 Bank Statement Posting	+	ACP650 Make Payments

.... but there are well over 100 other ones floating around down there, depending on what BPCS or ERP LX version you use.

Due Diligence: sonar for SOD conflicts

There's an automatic way to detect all the separation of duties conflicts floating around in your BPCS / ERP LX user profiles ... even the subtle, silent, x thousand fathoms deep variety.

Our **Due Diligence** software identifies and reports separation of duties conflicts based on internal control principles and best business practices. The product's search design is in harmony with regulatory requirements authored by Sarbanes-Oxley and the rest of the compliance alphabet: PCAOB, 21 CFR part 11, GLBA, COBIT, etc.

Due Diligence reports list users who have authorization to use a combination of BPCS/ERP LX applications, programs, program options, and/or transaction effects that violate separation of duties principles. Findings are reported to the person authorized to run Due Diligence.

- Click **here** to review technical details about Due Diligence software
- A description of the product's report selection process is available **here** including an explanation for the options on how to analyze valid BPCS/ERP LX profiles for individuals who have deactivated or disabled operating system profiles.

Where do segregation of duties vulnerabilities come from?

Many problems are created as time passes. When employees are moved into different roles and responsibilities over years of time, their BPCS user profiles must be updated for them to perform new duties. Kirsten's new accounting supervisor complains that she can't use BPCS to get her new job done ... but ... no-one complains that Kirsten can still do her **old** job in BPCS.

The accounting supervisor's call for immediate help creates a sense of urgency to add program authority for Kirsten. However, there may be no management advocate for performing the "clean out Kirsten's prior authorities" chore. The clean-out janitorial work ends up with a lower priority. Busy IT departments typically have a list of several hundred low priority projects that never receive attention.

Our net assessment of vanilla BPCS / ERP LX functionality for user profile maintenance is "**security by obscurity**." It's very clunky. Therefore, janitorial work on BPCS/ERP LX profiles typically ends up at the "approach-avoidance" end of the low-priority list.

Sometimes separation of duty vulnerabilities can be traced all the way back to the last time a new version of BPCS/ERP LX was implemented. The user profiles invented for conference room pilot testing were not thoroughly re-analyzed when it was time for the cutover to live production and ever since, the clunky nature of vanilla BPCS/ERP LX user profile maintenance has suppressed enthusiasm to go digging back through every profile.

- Click **here** to review details about vanilla BPCS/ERP LX user profile functionality
- Click **here** to see how **By Invitation Only**™ software greatly facilitates management of BPCS/ERP LX user security.

Sometimes the conflicts are unavoidable

Large manufacturing sites with a substantial office staff will have an easier time complying with the fine print on separation of duties principles than low-headcount sites. Due Diligence software will provide a thorough list of conflicts that merit a more clever mitigation strategy than "hire another person" and internal auditors must then look for some other way to manage the internal control risks associated with small-staff operations.

Enterprises in that situation design compensating business procedures to overcome the SOD problems. Frequently, those conflict resolution designs are scrutinized by internal audit and then presented to senior management for approval of what amounts to a SOD "waiver." Later, when an external auditor points to the same SOD problem, the company is very well prepared with the signed waiver documentation.

SOD Waiver functionality in Due Diligence

Due Diligences' waiver functionality encourages enterprises to formalize the practice of creating and maintaining mitigation plans for SOD conflicts. Due Diligence enables a security officer to enter and maintain management-approved SOD waivers down at the user-by-user level by BPCS environment. When a Due Diligence report run is launched, the user will be presented with a toggle option to either:

A. Print a specific "Waiver Number" next to conflicts appearing on Due Diligence reports, or ...

B. Exclude SOD conflicts which have approved waivers from Due Diligence reports

The objective is to have type **A** reports arrive with a Waiver Number printed on every line and type **B** reports arrive as a blank sheet of paper. An auditor reviewing a "type **A**" report will be able to match each Waiver Number reported by Due Diligence with a sequential file of signed waiver documents. That conclusive reconciliation process will keep all your SOD ducks in a row.

Another way to boost BPCS / ERP LX internal control

Unbeaten Path has helped companies design and implement SOX-audit-approved solutions for small headcount shops. One facet of our methodology is to observe changes to crucial database files with our **Stitch-in-Time**™ data integrity software. The product creates fool-proof audit trails.

- Click **here** for information about **Stitch-in-Time**® software
- A sample regulatory compliance vulnerability assessment report prepared by Unbeaten Path is available **here**.

Questions ?

It would be a privilege to answer any questions about **Due Diligence.**
Here's Unbeaten Path International's contact information:

Toll free North America: (888) 874-8008
International: (+USA) 262-681-3151
Send us an email (click **here**)

Unbeaten Path®

site navigation