

Visible Ops Security Phase 3: Implement Development and Release Controls

**by M. E. Kabay, PhD, CISSP-ISSMP
CTO, School of Graduate Studies
Norwich University, Northfield VT**

In the last three columns, I have been highlighting the excellent booklet called *Visible Ops Security: Achieving Common Security and IT Operations Objectives in 4 Practical Steps* < <http://www.itpi.org/home/visibleopssec.php> > by Gene Kim, Paul Love and George Spafford.

Today I'm reviewing their chapter entitled, "Phase 3: Implement Development and Release Controls," which the authors introduce as follows: "...we move upstream to the development and release management processes, as well as to the internal audit and project management processes. We will involve stakeholders from development, project management, and release management so they get involved earlier with projects and we will also work with change management, purchasing, and accounting to maintain accurate situational awareness. We will define the model for engaging with individual project groups when there are information security relevant tasks that we can help with."

As in the other chapters, the authors provide a table of issues and narrative examples that will resonate with anyone who's been in the security field for a while. For example (quoting),

- Information security and audit do not work together (This afternoon, I had a pretty awful meeting with the internal IT auditor. Several things bothered me. First off, he blindsided me with a whole bunch of deficiencies on password controls for some random systems buried in some business processes that shouldn't even warrant being audited. To make matters worse, he even did a penetration test and hit us with findings from that. And then we ended up getting into a heated debate about IT controls instead of talking about the risks we are trying to mitigate. / I guess the thing that bothers me most is that we don't appear to be on the same page with respect to what the top business risks are. . . .)
- Project teams that do not involve information security risk building services contrary to the needs of the organization (For example, let's talk about the last application that the developers put into production. Instead of using the libraries we created to do authentication, they created their own nonstandard libraries, made worse because they haven't been trained on secure programming practices. Now we have to create another piece of complicated middleware to adequately control access. / The unique authentication method now becomes yet another one-off that we need to support. We keep making the mistake of favoring the project goals over the enterprise's goals – over and over again. It has slowly consumed all the air in the room and is killing us.)

The steps and tasks detailed in this chapter are a challenging agenda for anyone in the real world. The prescribed methodology (amply discussed in the text) has the following framework:

Step 1: Integrate with Internal Audit

Task 1: Formalize the relationship with audit

Task 2: Demonstrate value

Step 2: Integrate into Project Management

Task 1: Participate in PMO approval meetings

Task 2: Determine information security relevance

Task 3: Integrate into project review and approval

- Task 4: Leverage detective controls in change management
- Task 5: Link to detective controls in purchasing and accounting
- Step 3: Integrate into the Development Life Cycle
 - Task 1: Begin a dialog with development
 - Task 2: Establish requirements definition and secure coding practices
 - Task 3: Establish secure testing practices
- Step 4: Integrate into Release Management
 - Task 1: Formalize the relationship with release management
 - Task 2: Ensure standards for secure builds
 - Task 3: Integrate with release testing protocols
 - Task 4: Integrate into production acceptance
 - Task 5: Ensure adherence to release implementation instructions
 - Task 6: Ensure production matches known and trusted states

I don't think anyone can view this agenda as anything less than daunting, but the case for integrating security thoroughly into audit, project management, development and implementation (release) is so strong that I fully support the authors' views.

Readers interested in seeing my own perspective on these issues might like to look at my MS-PowerPoint lecture slides on operations security and production controls <
http://www.mekabay.com/courses/academic/norwich/is342/lectures/32_Operations_Security.ppt
>, monitoring and control systems <
http://www.mekabay.com/courses/academic/norwich/is342/lectures/38_Monitoring_Control.ppt
>, and application controls <
http://www.mekabay.com/courses/academic/norwich/is342/lectures/39_Application_Controls.ppt
>. The same links with ".pdf" instead of ".ppt" will download the lecture handouts instead of the slide files.

In the final column on this topic, I'll discuss Phase 4 of *Visible Ops Security*: "Continual Improvement."

* * *

M. E. Kabay, PhD, CISSP-ISSMP <<mailto:mekabay@gmail.com>> specializes in security and operations management consulting services. CV online.<<http://www.mekabay.com/cv/>>

Copyright © 2008 M. E. Kabay. All rights reserved.

Permission is hereby granted to *Network World* to distribute this article at will, to post it without limit on any Web site, and to republish it in any way they see fit.