How I Learned to Stop Worrying and Love the Audit

Nate Howe
nate.howe@utdallas.edu
Chief Information Security Officer
University of Texas at Dallas
Do You Recognize The Title?

DR. STRANGELOVE OR: HOW I LEARNED TO STOP WORRYING AND LOVE THE BOMB

Education - Partnership - Solutions
My Experience
Why Fear Audits?

No one likes criticism...

“Someone who doesn’t know how to do my job, telling me what I did wrong”

“If the audit report contains issues I could get in trouble”
Why Fear Audits?
I’ll make your life miserable! I’ll thwart your every move!

HI. I’m the new sadist.

What happened to the old one?

He went to sadist paradise.

The auditing department?
Audience Survey

How does the term “audit” make you feel?

What good or bad audit experiences have you had?

What would you like to get from today’s conversation?
Definitions
What is a Control?

Internal control, as defined in accounting and auditing, is a process for assuring achievement of an organization's objectives in operational effectiveness and efficiency, reliable financial reporting, and compliance with laws, regulations, and policies.
What is an Audit?

Independent verification of controls

Specialties: Financial / Process / IT / Compliance

Phases: Planning, Fieldwork, Reporting, Issue Tracking

Types: Assessments, Pre-Implementation, Integrated

Typically starts with policies & procedures
Who is an Auditor?

Professional who specializes in verifying facts and creating structured documentation

Agent of management, board, or regulator, empowered to see all material he or she considers necessary to protect the organization

Someone who observes a variety of activities across an organization or industry

A natural skeptic
Key Message

Audit recommendations, if accomplished, should protect and improve the organization.

Unless you have proper issue tracking and accountability, audits waste time and will not create positive change.
Audit Process
Planning Phase

• Initial discovery meeting

• Review the scope memo

• Attend kickoff meeting

• Prepare materials for initial requests list
Initial Requests List

- Can never have too much documentation
- Refresh document dates
- Create “Note to the Files”
- Don’t let prior issues return
- Audit yourself first, don’t submit obvious issues!
Key Message

Being asked to support the audit process, without being included in the Planning Phase, causes frustration and confusion.
Fieldwork Phase

No two audits are alike

No two auditors can agree on documentation format

“They didn’t ask that during last year’s audit”
Fieldwork Phase

Never lie

Admit your own mistakes first

Limit the conversation to what you are asked directly

Be friendly, but don’t be friends
Fieldwork Phase

Do you need budget resources for your initiatives?

Then mention it to the auditor

Maybe this will show up as an issue

Maybe this creates leverage you need for your initiative
Reporting Phase

Close issues “during the audit” whenever possible
Reporting Phase

Don’t agree with the auditor...?

Validate the issues

Negotiate the action plans

Combine issues according to a similar theme

Set sufficiently distant action plan dates
Reporting Phase

When creating an action plan...

Consider what documentation would close the issue

Remember the auditor will need to collect documentation that a reasonable person would consider sufficient to prove the issue resolved

Be clear and specific about what documentation will be provided, because different people may be working on it next year
Reporting Phase

Would issue resolution cost money?

Provide conditional action plans

Commit to a budget request only, because it costs nothing to ask for resources

Create a second phase that only activates if budget is approved
Reporting Phase

Do not settle for point-in-time fixes that only address the symptoms

Seek lasting improvements

New processes and automation

Issues should not return if you design and operate proper control
Key Message

Not all audit recommendations can be implemented

Be specific about who in the organization is empowered to accept risk
Key Message

Audits are conducted between professionals who have different assignments, yet both want the organization to remain successful

Show respect to get respect
Love?

No, probably not...

But we should at least understand and value the process
We’ll be having an ISO 9000 audit soon. They’ll check to see if we follow our own documented procedures for everything we do.

I’ve divided our preparation tasks into two groups: unethical and unproductive.

I’ll train our department to lie to the auditor. You can document our inane procedures.

No fair. You did unethical last time too!
How I Learned to Stop Worrying and Love the Audit

Nate Howe
nate.howe@utdallas.edu
Chief Information Security Officer
University of Texas at Dallas