



Red Three Consulting

The auditors are here – and they
just want to ask you a few
questions



About Us

- The reports you need from the software you already have
- Lawson, Oracle, AS400
- Technical development for Customizations and Integration



Before We Begin 5Ps

- **Purpose**
 - To keep the company in business.
- **Proactive**
 - The more you have ready, the less they will ask for.
- **Process**
 - Much of this is a process question, not a technical question
- **People**
 - At some point, you have to trust someone
- **Positive**
 - You can learn something, you can improve your life.



Types of Audits

- Financial Systems
- IT
- Sarbanes Oxley
- HIPAA
- SAS 70



Today's Focus

- Lawson
- Financial Systems



Background

- Not an auditor nor do I play one on TV.
- Clients who've had both Sarbanes and Accounting Audit requirements.
- We defend, we don't audit.
- This is what we tell clients – and our clients are generally long term.



Agenda

- Network
- Login
- Application Security
- Data Security
- Disaster Recovery
- Change Management

Network

- Your enterprise software should be within the firewall
 - Just because it runs in a browser doesn't mean it should be exposed to the public internet. EVER.
- Network penetration test to show that your firewall is secure
- External transmissions – encryption (PGP or SecureFTP, not both)
- Internal transmissions – people still use Telnet.

Logging In

- Passwords – need to follow corporate policy. You don't necessarily need a password change policy
- Advantage of Portal - Keep people off the servers – you can show example of profiles
- Process to remove old users
- Root/QSECOFR/Windows Admin – process and or LOGCMD
 - Process with separate person to administer password



Application Access

- Are you in a Sarbanes/Separation of Powers World?
- Minimum – separate AP from AR etc.
- IT locked out of production system – or inquiry only
- Tracking Security class changes
 - Good policy and documentation will help you avoid complex technical solutions.



Data Access

- Database level – control update access.
- ODBC vs. OLEDB – some people get away with ODBC
- Report Distribution methodology



DR/Change Management

- Having one server or one set of servers is very difficult in the new world of appservers/webserver/database servers— you need multiple sets depending on your DR and change management requirements.



Disaster Recovery

- Backup and Verification
- Duplicate servers – offsite solutions
- Explicit statement of what the company is willing to tolerate



Change management

- What do you need to track?
 - Patching
 - Customizations
 - Data fixes
 - Reports/Crystal
- Software/Process/Scripting
- ROI during upgrades