The IS Audit Process Part-1

Four key objectives

a. Defining auditing and auditors
b. The audit planning process
c. Risk analysis
d. Internal controls

Auditing & Auditors: an evaluation process of an org, system, processes, project or product. Produces a report and submit it to management with presentation. Electronic Data Processing Audit, collects organizations IS data and ensures IS safeguards their data to achieve organizations goals or objectives. Both internal and external auditors can run the IS audit. The plan should be long-term & short-term as well.

Focus:

a. New control issues
b. Change or upgrades to technology
c. Business processes, needs, goals
d. Auditing, evaluation techniques
e. Regulatory requirements (Sarbanes Oxley, HIPAA)
f. Deadlines of implementation
g. Key decision makers

Gather information >> identify stated components >> Assess Risk >> Perform Risk Analysis >> Conduct Internal Control Review >> Set Audit Scope and Objectives >> Assign Resources >> Develop Strategy

Risk Analysis

Identify factors that jeopardize a process or goal. Apply Mitigation, countermeasures and controls to avert this impact. Risk is ***"RISK is the potential that a given threat will exploit vulnerabilities of an asset (or group of assets) to cause loss or damage to the assets"***

IS/IT=Threats, impact & probability. Understand the words.

Assessing countermeasures

Cost benefit analysis, Cost of the countermeasures is compared to benefits. Management tolerance to risks. Preferred ways to reduce risk, minimize risk/potential impact. Risk assessment, risk mitigation, re-assessment is the cycle of assessing risks.

Purpose of Risk Analysis, helps auditors to

a. Identify threats to organizations to have controls in place
b. Evaluate countermeasures
c. Decide on auditing objectives
d. Support risk based auditing decision
e. Lead to implementation of internal controls

Internal Controls

Results of our risk analysis, to reduce risk. Mitigates risk business or objectives of the organization. Provides certain levels of identified risks, how to prevent it and how to put controls in place. Addresses undesired events. Controls are typically categorized as:

a. Preventative: determine issues, monitor operations. Prevents malicious acts.
b. Detective: mechanisms of reporting malicious act.
c. Corrective: basically minimizes the impact after the fact. Some type of Intrusion detention control, quarantine and remove the problem. Modify the system to make changes to take contingency planning and testing.

Goals of internal controls

a. Accounting operations
b. Daily business functions
c. Administration of systems and policy implementation
d. Data safeguarding
e. Legal compliance
f. AAA services, authentication, authorization, accounting for organization
g. Data accuracy on I/O, data hashing
h. Reliability of infra, redundant systems
i. Change or configuration management

General Control Methods

a. Internal accounting
b. Operational
c. administrative
d. ORG policy
e. Documentation
f. Facilities
g. Datacenter resources

The IS Audit Process Part-2

Additional methodologies, 6 main topics

a. Audit classification
b. Phases of the audit process
c. Risk based audit approach
d. Evidence
e. CAAT's (Computer assisted audit techniques)
f. CSA (Controlled self-assessment)

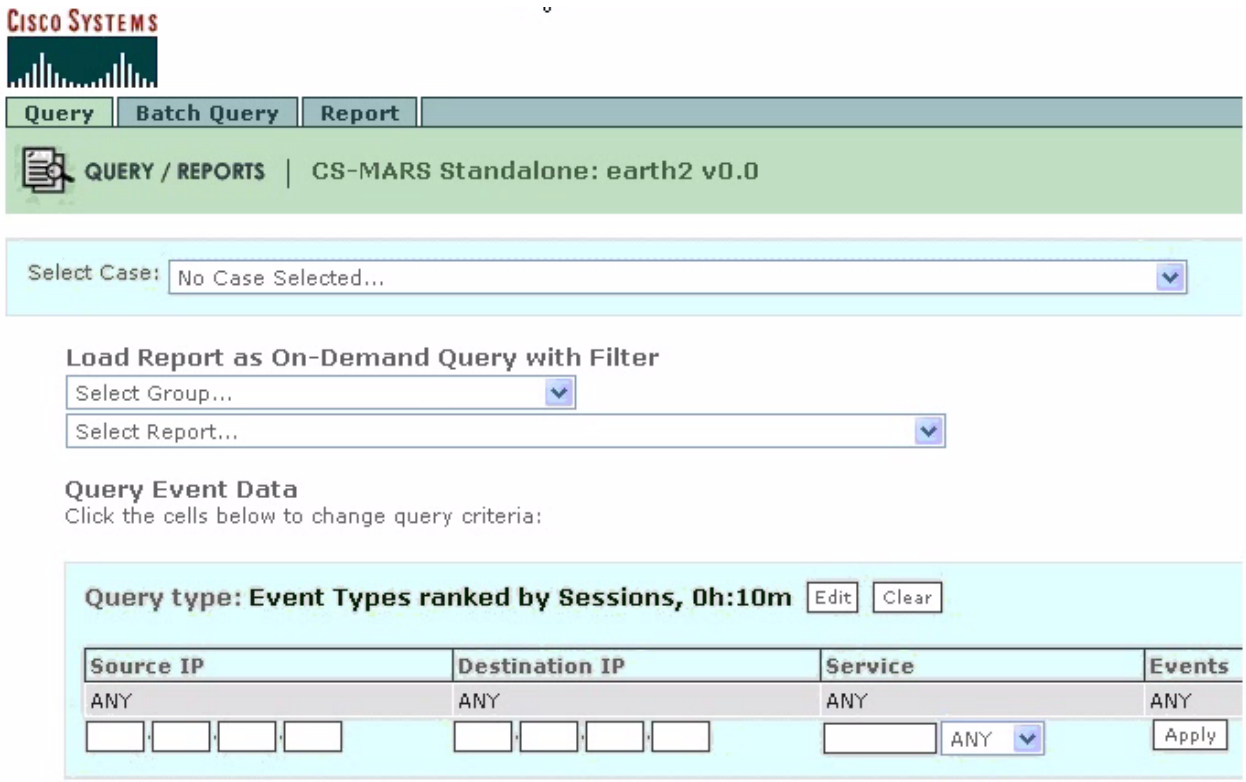
Audit Classification

Financial, operational, integrated, administrative, information systems, specialized (SAS 70), forensic auditing.

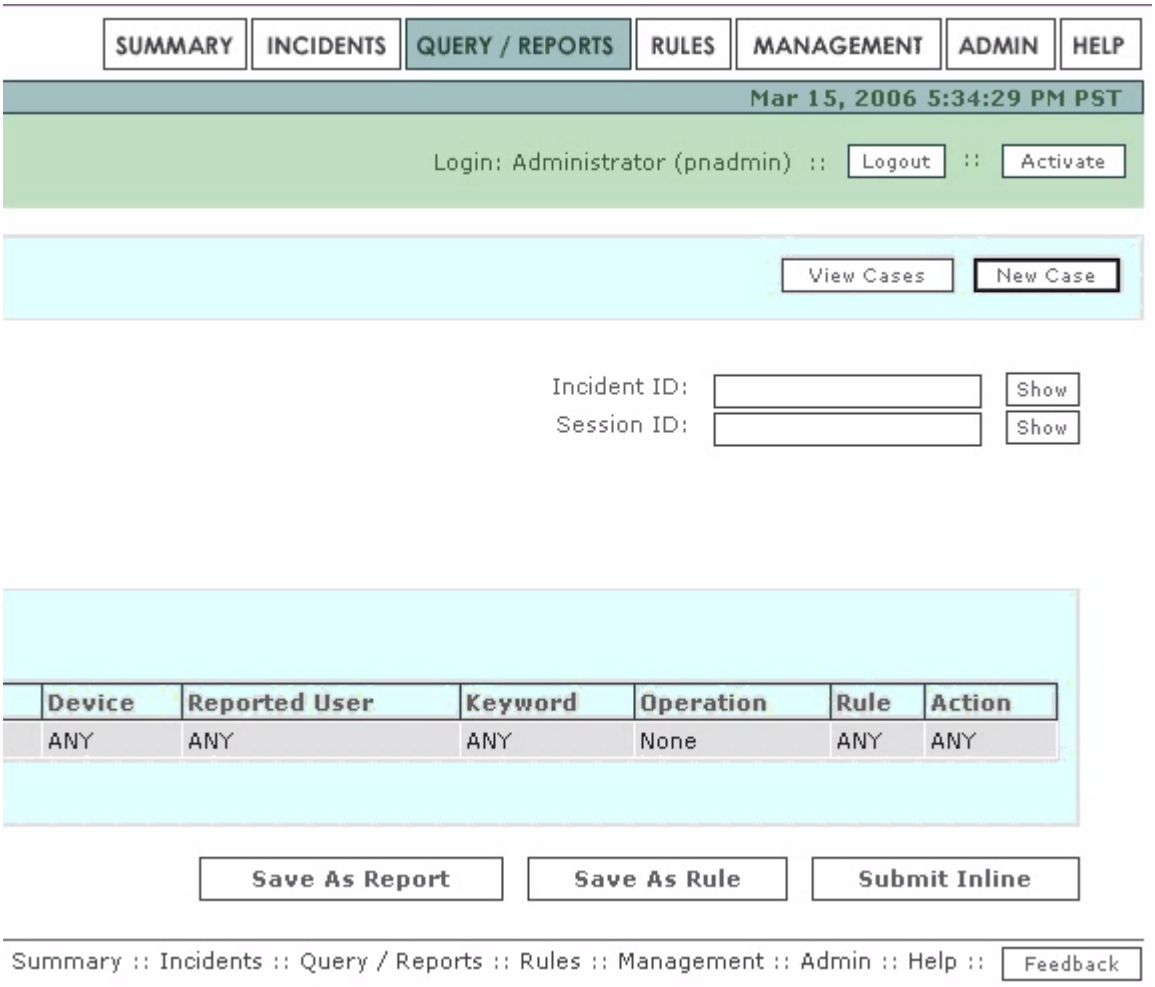
Phases of the Audit Process

Nothing typically stated.

Subject entity >> objective/target >> scope/function >> pre-audit planning & testing capabilities>> gather data within scope, mgmt. >> result evaluation >> Management communication process >> Report preparation, assessment report generated.



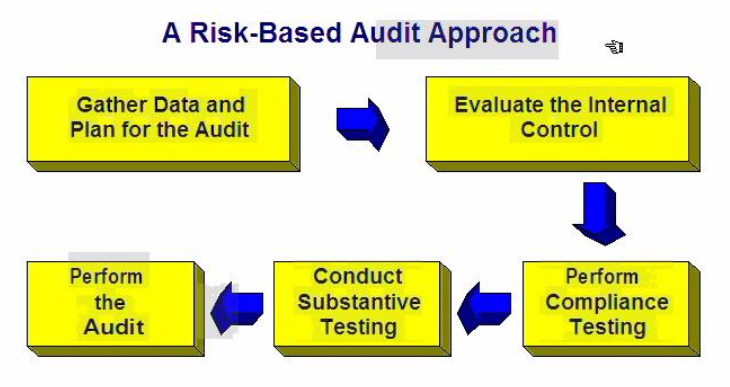
Integrated solution for monitoring, analysis and generates reports.



It can do a comprehensive audit, to verify controls.

Audit Risks (Humans makes errors)

a. Inherent Risk: over/underestimating assets
b. Overall Audit Risk: deleted logs, garbage data, too many logs
c. Control Risk: Misinformed data
d. Detection Risk: missed data, or irrelevant data, prior audit reports

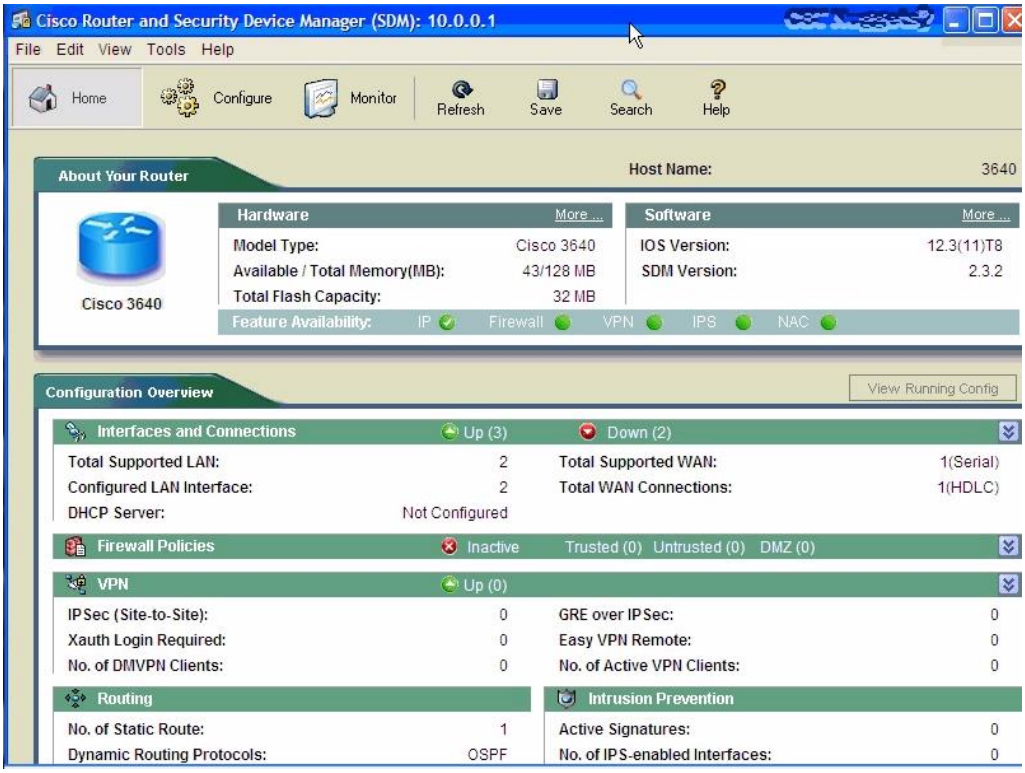


Evidence

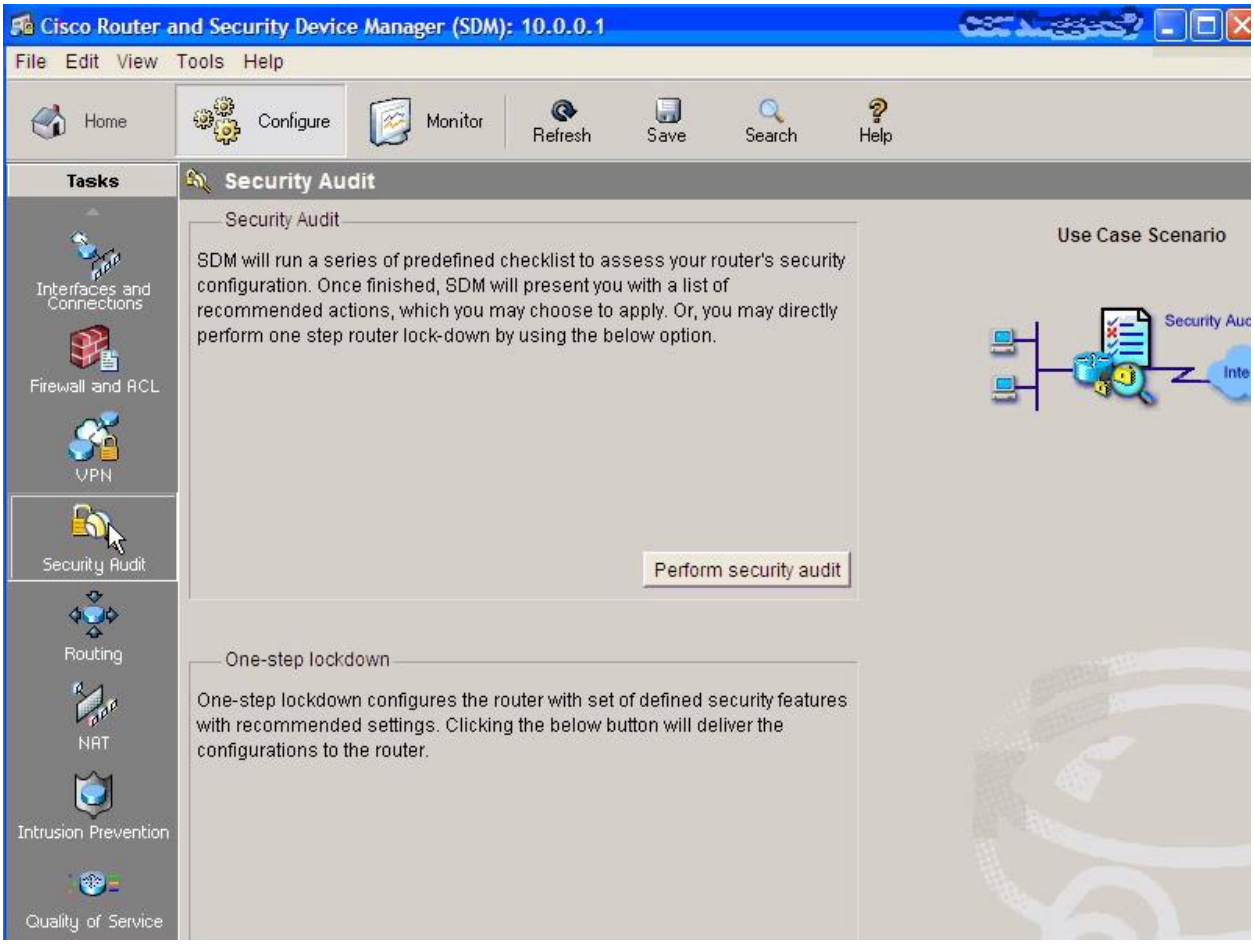
a. Established audit criteria or objectives, visual observation, power users, network engineers, management, baselines for security, optimization techniques etc.
b. Reliable data: affects the entire audit. How data evidence gathered, by certified people or not. Like CISM, CISSP or CISA. Timing of the evidence is also important, as time stamp is a required process. Time frame to run the audits.

Evidence Gathering Techniques

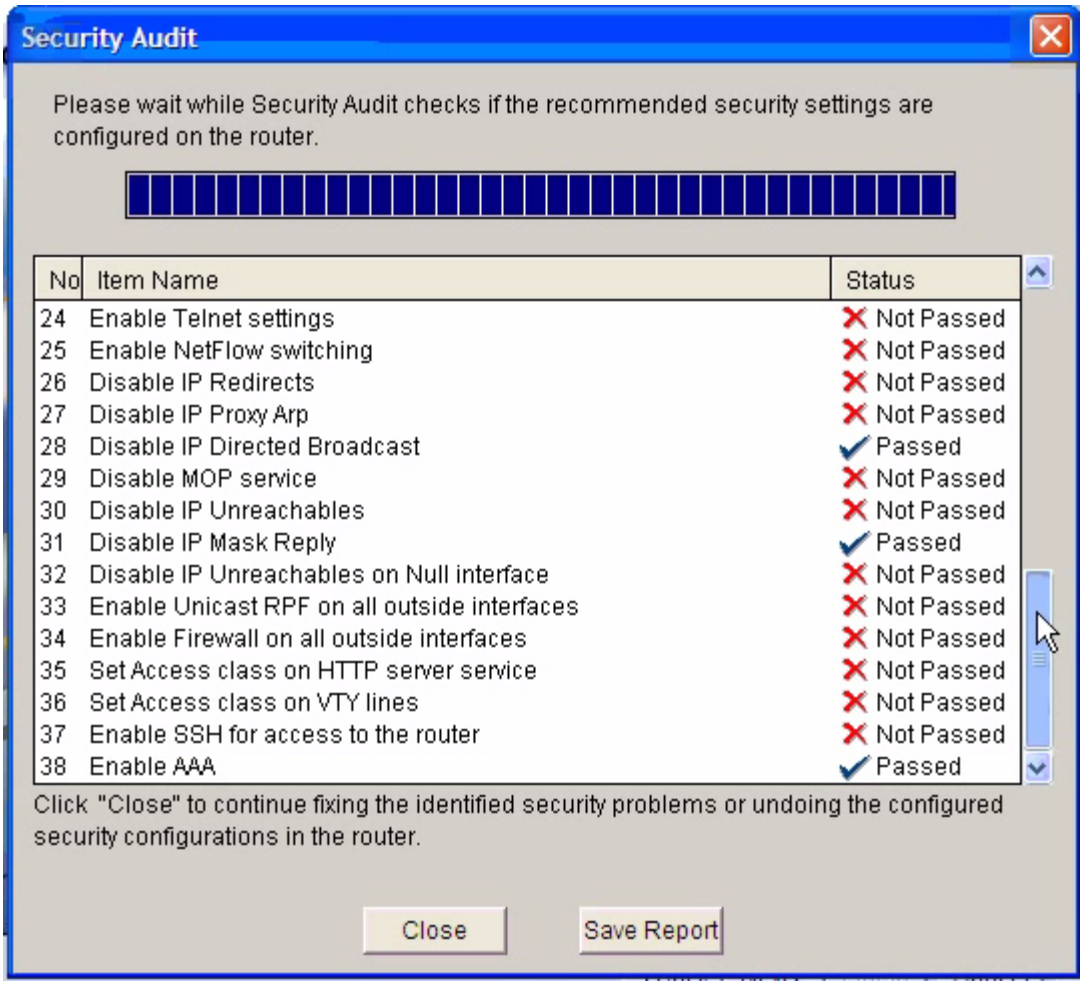
a. Observe IS ORG
b. Review policies, standards
c. IS documentation
d. Observe personnel/interview
e. Judgmental/statistical sampling. Educated guess, rely on the subjective judgment.
f. Utilize other experts
g. Computer assisted audit techniques. Security audit, annual review, vulnerability assessment, penetration testing.



Test it out for IPS, firewall, VLAN,

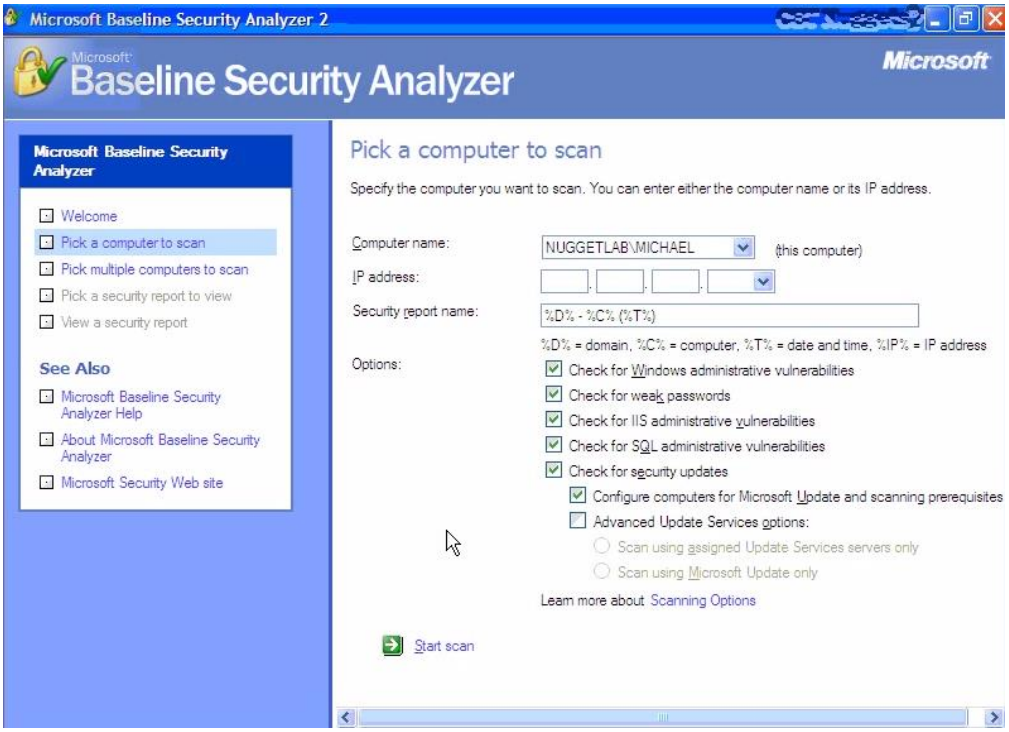


One step lockdown, [perform a security audit and such on each ports either serial or Ethernet internal or external or DMZ zone. What you are doing right now, is performing an audit. With recommended security settings, now the reports looks like this

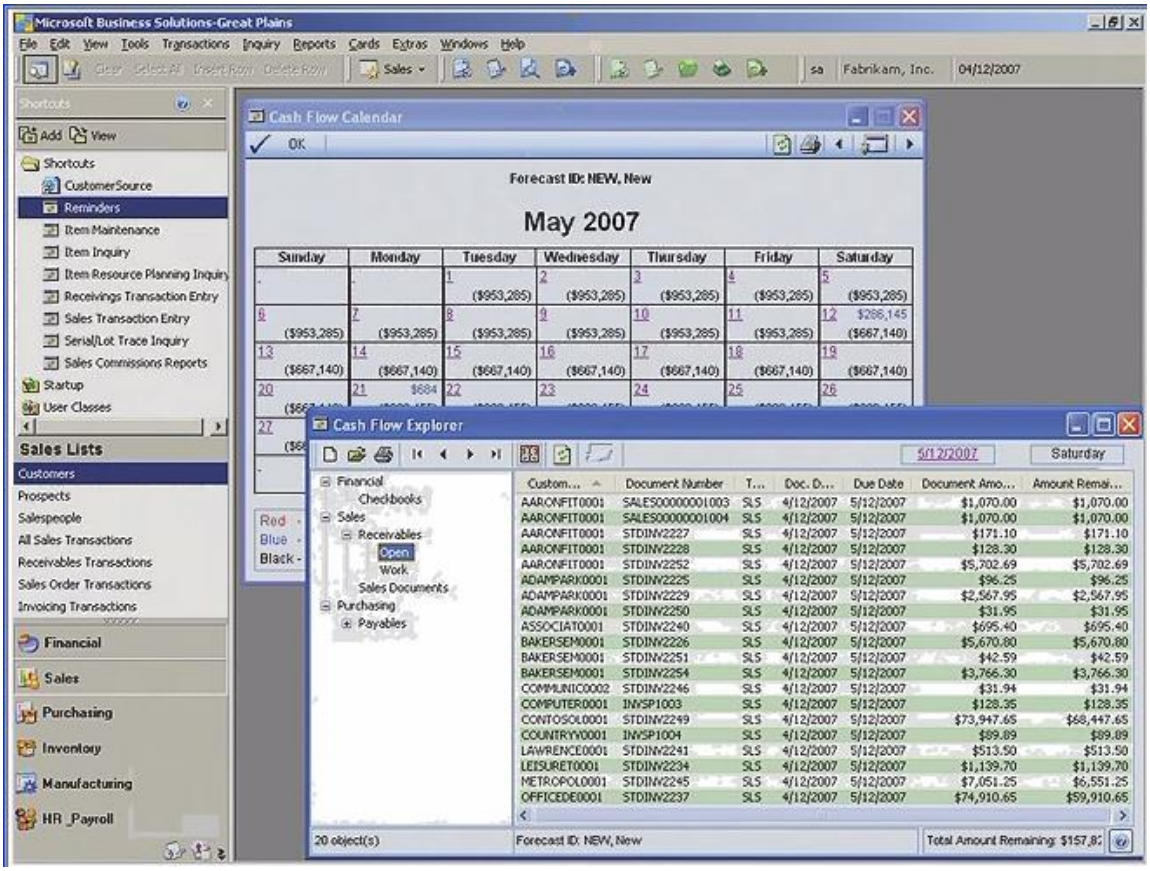


As you can see that there are security audits that haven't been passed. This vulnerabilities costs company's real damage. Save the report if you want to. Or you can fix the security problems, problem by problem. This was an example for security audit of a device by using computer assisted auditing. Looking at logs is also a major auditing scope, like firewall log, DOS attack logs.

You can also use Microsoft Baseline Security Analyzer 2.0.



Another Microsoft software, Great Plain from Microsoft Business Solutions (currently Dynamics GP). It also has auditing capabilities software wide.



Control Self-Assessment (CSA)

a. Internal controls are reliable for concerned parties
b. Controls are implemented to manage risks
c. Formal, documented and collaborative process derived from surveys, questionnaire, and workshops for CAAT
d. Employee cohesion, awareness, communication methods, improved audit process etc.