Infosüsteemi auditi tugitarkvara (CAAT) - ülevaade ja näide

Jaak Tepandi, CISA

TTÜ, Tepinfo, EVS TK4, EISAÜ

Teemad

- CAAT - ülevaade ja lisad
- CAAT Eestis
- IDEA ja CaseWare Examiner

Auditi tugitarkvara (CAAT), näited

- COBIT orientatsiooniga
  - ISACA COBIT Online, COBIT Advisor,…
- Andmeanalüüs ja -kaevandamine
  - IDEA (Interactive Data Extraction and Analysis), ACL, …
- Auditi korraldus
  - WorkForce, AutoAudit, TeamMate,…

Auditi tugitarkvara (CAAT), näited (2)

- Kvaliteedijuhtimist soodustav
  - CMM Advisor,…
- Üldotstarbeline (auditi) tarkvara
  - Kõikvõimalikud tehted andmetega, võrdlemine, Excel, Word, …
- Üldotstarbelise tarkvara auditi suunitlusega funktsioonid
  - auditi jälg ja logid andmebaasi- ja operatsioonisüsteemides

Auditi tugitarkvara (CAAT), turve (3)

- Turbega seotud info analüüs
  - CaseWare Examiner, DumpSec,…
- Portide skaneerimine / skaneerimise avastamine
  - palju võimalusi - pordiskännerid veebist, Nessus, psad (Linux), …
- Spybot ja Co

Muu

- WWW testimise vahendid
  - WebArt (ka koormustestid), Doctor HTML, Bobby…
- Litsentside analüüs
  - BSA-lt, …
- Mahu prognoos
  - COCOMO- I põhinevad,…

Auditi tugitarkvara (CAAT), arutelu

- Kuidas on CAAT eesti keeles?
  - CASE - tarkvara raaltehnoloogia
  - CA instruction - raalõpe
  - CAAT - auditi tugitarkvara (ATT)?
- Milliseid CAAT klasse /nimetusi lisada?
- Mida kasutatakse Eestis? Kes kasutab? Cobit, korraldus, turve, andmeanalüüs (ACL, IDEA)
- Hinnang?

IDEA

- **IDEA** is a PC based File Interrogation Tool for use by auditors, accountants, investigators, and IT staff. It analyzes data in many ways and allows extraction, sampling, and manipulation of data in order to identify errors, problems, specific issues, and trends.
- See **http://www.audittools.com/index.html**

IDEA

- Import on väga hea
- Analüüsid väga head
- CaseWare Examiner on lisavõimalus

Identifying exceptional items

- Exception testing can be used to identify unusual items. These may be simply large items or where the relationship between two pieces of information on an item do not correlate, such as rate of pay and pay grade. Many fields of information can also be checked for allowable values. The tests are performed using the Extraction function

Performing Analyses

- IDEA can help with the preparation of figures for an analytical review. In particular, it can generate analyses which would not otherwise be available. The File Stratification function will give a profile of the population in value bands, groups of codes or dates. This is particularly useful when auditing assets such as accounts receivables, inventories, loans or for a breakdown of transactions

Analyses (2)

- Additionally, the information can be summarized to identify trends. If graphical analysis is required by particular codes or sub-codes then charting can be used. Figures can also be compared against previous years to determine then the file should be output to a spreadsheet (either use cut and paste or File Export then chose either an MS Excel, Lotus 123, or dBASE format which most spreadsheet packages can read)

Checking Calculations

- Total
- Check
- Exception test of miscalculations
- Join databases
- … and other

Cross matching data between systems

- One of the common ways to test the validity of an item is to cross-check it against some other information. An example would be checking addresses or bank details of employees against those on Accounts Payable files to see if an employees were also purporting to be suppliers. These tests are carried out by importing both files and then using the Join Databases option. Another effective test for completeness is to cross-check between a master file and transactions to see if there are any items on the master file for which a transaction has not been raised

Testing for Gaps and Duplicates

- IDEA can be used to test for completeness including testing for gaps in a numeric sequence (or missing items). To test for gaps there must be a sequential number on source documentation. Inventory and sales files can be tested for completeness of despatch note numbers and purchases files for received numbers. It may also be appropriate to test for gaps on a series of check numbers and also for completeness of inventory ticket numbers
- Dates may also be tested for gaps, such as days for which there are no transactions

Sampling

- Statistical sampling is commonly used to test for validity in a manner which then allows for evaluation across a population. The more sophisticated methods such as Monetary Unit Sampling are difficult to implement manually. Where ever tests need to refer to physical documentation or assets rather than computer records then an appropriate statistical sampling technique should be used. IDEA offers 4 types of sampling: systematic,random, stratified random, monetary

Types of sampling (2)

- Systematic which should be used for samples to evenly cover a population range
- Random which should be used where statistical projections are required on various attributes of the population without bias
- Stratified Random Sampling which is used either where the population consists of different groups (items have a different risk) which need separately evaluating, or if Classical Variables Sampling (Variables Estimation Sampling) is to be used
- Monetary Unit which should be used where a financial assessment of error is required with items than can be partially wrong

Auditing e-mail logs using IDEA

- E-mail logs generally contain information such as the sender and recipient address, subject title, date and time of transmission, size of file, service provider etc. Ensure the organization has a published policy related to employee use of e-mail before undertaking any of these tests

Common tests include:

- Total length of time spent on e-mails (receiving and responding) by organization as a whole, by individuals, etc
- Summarize by service providers
- Summarize numbers of e-mails by employee, sort in order
- Isolate, summarize and examine personal e-mails
- Stratify by time and examine any unusual activity e.g. lunchtime, weekends, bank holidays
- Stratify by size of files
- Analyze file attachments, by size, by type
- Analyze incoming e-mails, identify common domain addresses
- Match with list of employees and extract any e-mails that are sent by invalid employees
- Analyze any dormant (mittekasutatav) accounts

CaseWare Examiner

- An auditing tool for network administrators and computer security auditors
- Windows (NT, 2000, or XP) security data files (logs) may be viewed in a list format with tools provided with the operating system
- However, it is difficult to form conclusions, or to view trends and assess compliance with security rules by viewing the logs in this manner
- IDEA will import these logs and extract other system information (often from registry settings), then perform a series of analyses to profile the information in a meaningful way
- Further testing is easily completed with IDEA's analysis tasks

CaseWare Examiner - importing and automated testing (http://www.audittools.com/examiner_intro_e.html)

Log file	Standard tests	Advanced tests
Application events	Number of events by Category, EventID, Source, Type and User	All errors
Security events	Number of events by Category, EventID, Source, Type and User	Accounts with expired password, unknown username or bad password, disabled accounts, failures, locked out accounts, policy changes, unsuccessful logons
System events	Number of events by Category, EventID, Source, Type and User	Errors, remote access callback numbers, remote access connections
Users	Summaries of dial in access accounts, password required accounts, disabled and locked accounts, "never expires" passwords	Accounts not requiring passwords or with "never expires" passwords, accounts with remote dial in access, disabled and locked accounts
Groups	All administrators and operators, number in each type of group membership and user groups	Accounts belonging to five or more groups, administrator and operator user details
Printers	Printers with "All" access, printers with owners	
Shares	Shares with "All" access, unprotected shares	
Services	Number of records by Type and Status	

Target and Compatibility

- ***Examiner*** **is compatible with IDEA 2002 SP1, and is intended for the audit of security data from Windows XP, 2000, and NT4.0**

A five-step process

Auditing security data using *Examiner* can be thought of as a five-step process:

1. Setup of the logging policies and procedures
2. Extracting security information into files for import to IDEA
3. Importing the files to IDEA
4. Profiling of the imported files by analyzing the fields, and extracting out specific information
5. Analysis and review of the results

IDEA ja CaseWare Examiner - Kasutatud materjalid

- http://www.audittools.com/index.html
- http://www.audittools.com/examiner_intro_e.html
- DATAS 2000 for IDEA. Digital Analysis Tests And Statistics. Mario Perez, AuditTools AS, June 9, 2000