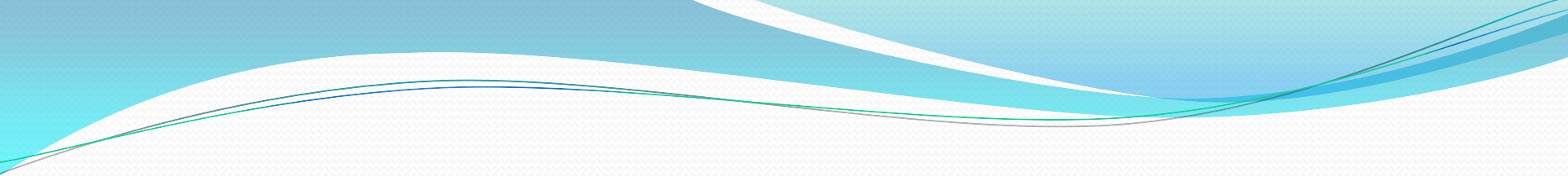


Principles of Internal and External Control of IT Systems and Their Use in Treasury

Nazim Kasumzade
Public Treasury Agency
Baku, Azerbaijan
02 October 2013

Content:

- Internal risks
- External risks
- Formal procedures and software solutions to control IT administrators
- Findings, conclusions and suggested solutions



Overall, principles of storage and access to confidential information, principles of IT systems building are similar in private and public sector.

It is a common belief, that large private companies spend more and, accordingly, have a much better protected system.

This presentation studies some general approaches applied both in Treasury and in private sector.

- The most probable risks associated with daily operations in Treasury include :
 - Access to confidential information without due authorization, particularly, by IT people and IT administrators
 - Possible deliberate damage caused by IT administrators
 - Negligence of system administrators

Overall, we can distinguish the following classes:

- Users
- Entrepreneurs
- Peepers
- Spies
- Avengers

Access to confidential information

- In absence of formal procedures and regulations on access to confidential information, system administrators will either have a direct and unlimited access, or can obtain it by applying usually minimum efforts.

One should understand that it is impossible to ban access of system administrators to confidential information, but, if one applies the correct approach, it is possible to regulate and control their access to such information. System administrators can do it just “for fun” (behavioral problem), but it can also be a deliberate action, which can entail serious consequences.

“Resentful” system administrators

- Employees of other units in an organization usually have a rather vague idea about ways and possibilities in terms of access to information and system as such the IT people have. In reality, system administrators have all passwords to access the root file system on servers, passwords to database, network passwords, and enjoy unlimited powers to launch any command. What if one of these employees feels resentful at the management of the company?

Negligence of system administrators

- IT risks will also include negligence of system administrators, which can lead to undesirable consequences. Even if it is an unintentional risk, it can also lead to rather deplorable results. What if a system administrator accessed the server as super-user and forgot to sign out while leaving it?

Examples:

- Edward Snowden – IT specialist
- Terry Childs – network administrator from San Francisco
- Jason Cornish – IT specialist
- Sergei Aleinikov – IT specialist
- Roger Duronio – system administrator

External risks

- Different forms of attacks are used both to gain access to confidential information and to cause damage :
attacks can be different :
- External hacking of the network
- Introduction of a trojan program
- Blocking servers from external access
- Changing the internal code of the used software

Formal Procedures and Software Solutions to Control IT Administrators used in Azerbaijan Treasury

- Our Treasury uses the principle of double control (“two button rule”) for authorization as “root” user, which requires introduction of a password by two employees. The same principle applies in case of the need to introduce some changes in software – any such change must be confirmed by two people in charge.
- We use Spectorsoft solutions to monitor activities of administrators and all other users of the system.
- Server rooms are equipped with cameras and sensors, which will send alarms if anybody penetrates the room
- Authorities of a system administrator are duplicated by external consulting service
- The network is managed by the Ministry, which excludes any possibility for system administrators to introduce any change

Findings, conclusions and suggested solutions

- Regular IT system audit
- Strict criteria for selection of IT personnel
- Internal rules for regulation of IT access