Information Systems Audit Internship

Diogo Manuel Leal da Costa

Activities Report

Abstract—As a means to disclose the art of audit, this report summarizes the experience and knowledge acquired from concluding an internship assignment at Caixa Geral de Depósitos (CGD) as an Internal Auditor. It covers the importance and main concepts for Information Systems Audit as well as the steps needed to undertake any audit project. This particular project focused on information security of CGD's networked multifunctional printers, with the goal of assessing how well the information that runs all over the company is protected. In order to properly assess printer's information security level, a risk analysis had to be ran, having as output a list of tests to apply to the controls designed to mitigate the risks. However, as a result of the interviews with the entities responsible for CGD's printers, the audit team discovered that the process owner of the printers had never designed controls to mitigate printers' risks nor even showed any concern in identifying them. Therefore, this project was concluded without seeing necessary the execution of any planned tests and the situation was reported according the findings.

Index Terms—CGD, audit, risk, risk analysis, scope, network, protocol, multifunctional printer, information, security, framework, information technology, information systems, business process

Which are really relevant?

TOO MANY !!

1 INTRODUCTION

WE, humans, were born perfectly imperfect. In an attempt to overcome our worst limitation – imperfection – and to objectify something that will never be objective – perfection – we've created measurement systems, mathematics, physics, social rules, and so on.

Every single man-made system we encounter in our daily lives has to be submitted to some kind of control or revision. The ultimate reason that has led us to this, besides our imperfection, is time. Systems tend to deteriorate over time, just as much as everything that we can say that exists. That is why we go to the doctor, or a car has to go through a periodic vehicle inspection, or a Company has to be subjected to audit.

Audit is quite similar to going to a doctor's appointment, only for Enterprises. Its main goal is to perceive what is wrong or what could be wrong or what will go wrong if no countermeasures are taken to subdue a Business' inner processes. With this notion in mind we are forced to answer a few more questions. How do we audit? What concepts lie beneath this process? How can we say that an audit methodology is better than another?

The audit project developed at CGD to study these matters worried about printers' information security. Printers, these days, are no longer empty-headed machines whose only goal is print and scan all day. They are wired throughout a whole Company's network, sending e-mails, faxes, storing print jobs, scan jobs, with a horde of new functionalities. Hence the new name – multifunctional printer (MFP).

Large Companies often deal with sensitive and/or confidential information that require to be safe from mal-intentioned hands. The critical aspect of this new generation of printers is precisely the fact that they store this kind of information in a Hard Disk Driver (HDD), i.e., the information is kept permanently in the disk until it is eventually deleted. But what if someone who should not have access to certain information reaches its content before

- *Diogo Manuel Leal da Costa, nr. 72770,*
  E-mail: diogo.leal@tecnico.ulisboa.pt,
  Instituto Superior Técnico, Universidade de Lisboa.

Manuscript received January 3rd, 2015.

(**1.0**) Excelent	ACTIVITY					DOCUMENT						
(**0.8**) Very Good	Objectives x2	Options x1	Execution x4	S+C x1	SCORE	Structure x0.25	Ortogr. x0.25	Gramm. x0,.25	Format x0.25	Title x0.5	Filename x0.5	SCORE
(**0.6**) Good												
(**0.4**) Fair	1.6	0 8	3.2	1	5.6	0.25	0.25	0.2	0.25	0.5	0.5	1.95
(**0.2**) Weak												

it is wiped? This is what it is called a risk.

The next few pages will focus on answering these questions supported by the experience gained from an internship while in the business branch of information systems audit, at CGD.

2 Background

Information systems audit has been a huge target of standardization, mainly because of security concerns. Our lives are increasingly more dependent on technology, millions of bits and bytes of information scattered all over the big World Wide Web (WWW) waiting on some snitch to get advantage of it. Moreover, Companies urge for mass information storage requires Information Technology (IT) processes to assure proper handling of such amount of information.

Being aware of this, ISO[1], ISACA[2], CCTA[3], CIS[4], amidst so many other entities, have created and been improving a series of standards (Frameworks) that every information systems auditor should have as guide.

inadequate verb

ISO developed quality and information systems management standards (9001 and 27001, respectively), ISACA developed a widely known and used framework called COBIT[5], and CCTA developed ITIL[6]. What all of these have in common is a set of good practices and metrics to evaluate the operability of information systems. In CGD, all information systems auditors are encouraged to request for certification in these frameworks, in order to raise the quality bar.

The problem with some of these tools is that they are sometimes ambiguous and subjective, very susceptible to different views of implementation. Therefore, there are no right or wrong methodologies, there are good methods and not so good methods, depending on how it suit~~s~~ a particular Business. Thus the general tendency at CGD's Internal Audit Division is adjusting these frameworks' guidelines to the Company's objectives. Nevertheless, they help train auditors in opening their minds to important concepts for auditing.

They

Finally, to grant a better insight on this audit project, CIS has published an online security benchmark for MFPs. This benchmark meticulously approaches every parameter that should be analyzed when installing a printer. With the support of these tools, the project stands on the right path towards an accurate audit.

3 Procedure

All of the frameworks mentioned in section 2 defend that for every risk there must be a control that mitigates or eliminates it. Hence, every control must be tested in order to verify that it properly contains the risk. The result of the tests performed over these controls will directly contribute to the final assessment of printers' information security.

Hereupon, the first step in auditing a system is identifying risks. However, to successfully identify the risks, the audit team had to be aware not only of the system itself but also of its boundaries (scope), so that all sources of potential risk could be covered.

Knowing the system is the bulk of the audit process. A thorough study of the printers' universe was ran in order to comprehend all its underlying concepts and infrastructure. This study also included learning the best practices in securing a printer's information.

Only after being acquainted to the system and acknowledging its risks, it was possible to sketch a security test~~s~~ matrix to evaluate the effectiveness of the controls that ought to be implemented for printer's safe use.

The test~~s~~ matrix had in regard the benchmark created by CIS. It covered the verification of some protocols' state (activated/deactivated, default fields) such as FTP[7], SNMP[8], SMTP[9], among other protocols that increase the device's exposure to external threats. Also, after a deeper study of the printer's functionalities it was possible to define a set of configurations

[1] International Organization for Standardization
[2] Information Systems Audit and Control Association
[3] Central Computer and Telecommunications Agency (UK Government Agency)
[4] Center for Internet Security
[5] Control Objectives for Information and related Technology
[6] Information Technology Infrastructure Library
[7] File Transfer Protocol
[8] Simple Network Management Protocol
[9] Simple Mail Transfer Protocol

that would enhance its security, which was included in the test~~s~~ matrix.

The second role of an auditor is investigating. Within a Company there's always someone responsible for something, and printers are not an exception. It was crucial to resort to any means necessary (e.g. division board) to discover who was in charge of CGD's printers – the interlocutor – and retrieve information about how they were being handled.

Several meetings and interviews were conducted alongside the printer's claimed process owner, between other seconded interveners, in order to ascertain the facts that would allow to draw conclusions and evidence to support them.

Having gathered the facts, the project was closed by writing the final report. The report presented the work developed and the necessary recommendations to alert the auditee to amend identified unconformities.

What Subject ?

4 Results

As a result of the held interviews, it was finally reached the conclusion that there was no concern over this subject. The questionnaires addressed to the auditees allowed to unveil the following facts/unconformities:

1) No risk analysis was led by the process owner.
   Consequences:
   a) No risks were identified;
   b) Increased printers' exposure to threats.

2) Printers' configurations by default.
   Consequences:
   a) Predictable system – meaning anyone smart enough to read a printer's user manual will know exactly how to own it (e.g. admin default password is in user's manual, therefore anyone can do whatever one pleases with the printer).

3) The process owner lacks technical knowledge to administrate IT processes.
   Consequences:
   a) Unawareness to the importance of a printer's information security.

4) The process itself is poorly conceived.
   Consequences:
   a) There are entities in CGD that have fewer responsibilities than they should have over printers, and vice-versa;
   b) Responsibilities' repudiation – meaning each party can disclaim its responsability in a task.

5) CGD's security department was not involved in the process.
   Consequences:
   a) No security criteria established to be implemented on the printers.

When faced with this scenario, the audit team decided not to run any tests on the printers. If, as mentioned in section 3, for every identified risk there must be a control, once there were no risks identified by the process owner then there were also no controls to be tested.

Still, in order to demonstrate that no controls were implemented, evidences had to be collected. To prove that printer's information was not safe, the audit team managed to alter the SMTP server address and receive every scan job all users sent from the printer. This hack was possible due to the administrator password being by default, which allows to modify any admin settings of a printer.

Another possible means to achieve this was via Telnet – a tool that establishes point-to-point connection between two machines – which offers an even broader set of options. The password to access a printer via Telnet was discovered by brute-force. Nonetheless, this task took very little effort, seeing as the password was as obvious as "administrator". Once connected to the printer, it was possible not only to modify settings but also make it unavailable – shut down, reboot, set to sleep mode, etc.

Thus, multifunctional printers at CGD were assessed as having no security standards designed nor implemented. It was clearly proven that MFPs' information had zero protection.

5 Conclusion

The first reason for which these unexpected results were not so unexpected was having discovered that CGD's information security department was not involved in the process. Without their envelopment no security criteria was established to be implemented on the printers, hence the printers' configurations being by default. Also, the fact that the process wasn't thought through, gave root to loose ends that nobody felt responsible for tightening the knot.

Based on this, the report's recommendations focused on:

1) Alerting for the necessity of a structured communication plan between process' interveners
2) Alerting for the urgency in implementing a set of configurations suggested by the best practices

The main conclusion to retain out of this audit is that if the process was well-structured the remaining unconformities would probably not exist.

Later on, it is foreseen by the information systems audit department that, when the recommendations are implemented by the respective entities, a follow-up audit ought to be conducted. This follow-up's goal will be to apply the tests that were not executed, given the circumstances of this first audit, and reassess printers' information security.

Despite CIS' security benchmark has not actually been put to practice in this audit, the remaining frameworks clearly helped sculpting its procedure. Henceforth, every audit ought to go through:

- A risk analysis
- A scope selection
- A work plan (design tests, define interlocutor, create agenda, etc.)

Concluding, each audit is different from another, there is a vast number of articles providing hints on how to design tests for a given subject. However, the steps needed to accomplish it are always the same.

The execution of this project made possible to minutely understand an audit's workflow and how to apply it in projects to come.

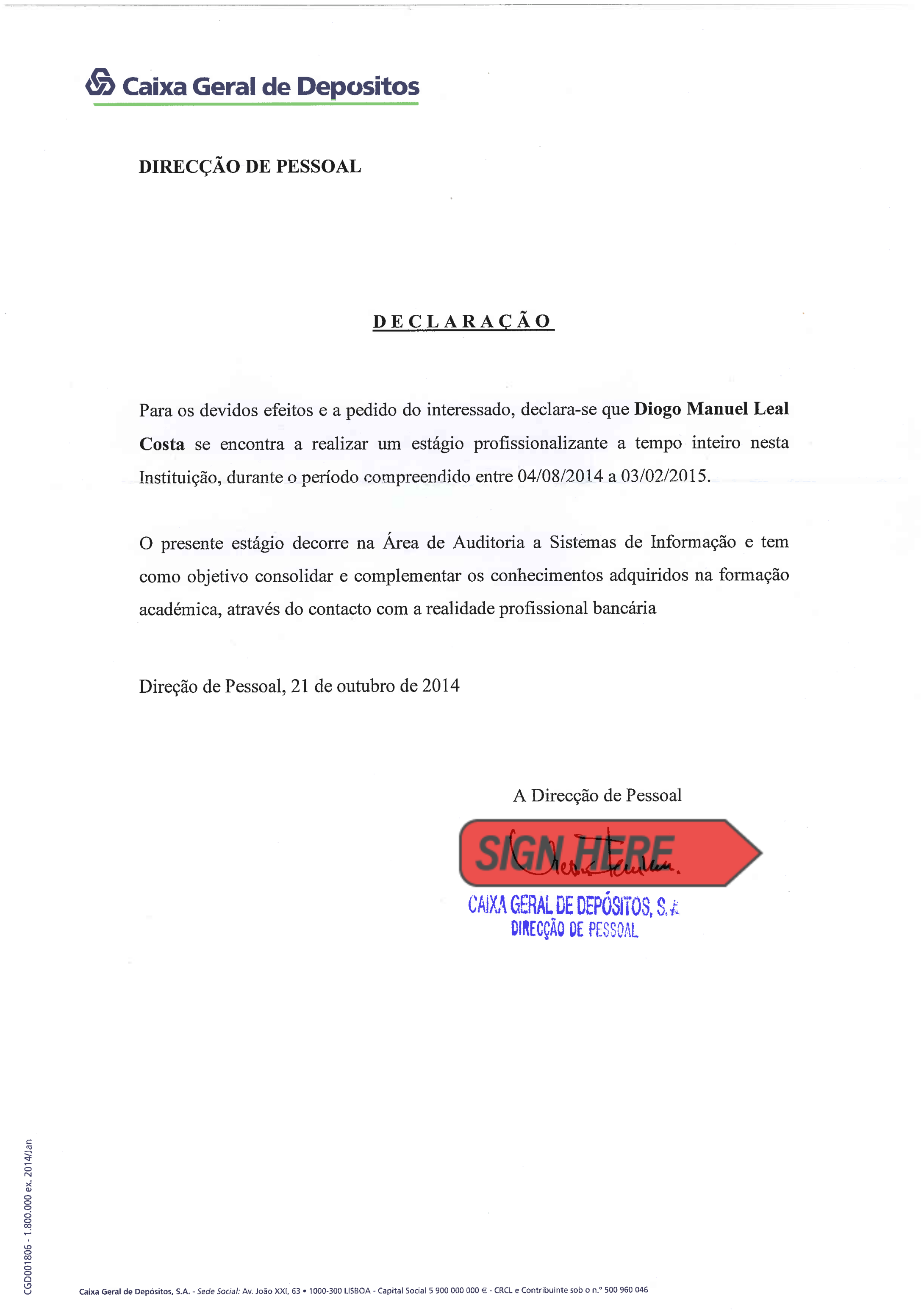
Acknowledgments

A huge thanks to my mentors from CGD's Internal Audit Division, Pedro Madeira and Rui Pereira, who guided me throughout this whole project and helped me out of my confort zone.

In this type of document (Technical), the CONCLUSION should start with a SUMMARY of the subject addressed and then should highlight the results.

Diogo Costa graduated at Instituto Superior Técnico (IST) in Computers Engineering, 2014. Currently accomplishing a Masters' Degree in Intelligent Systems and Software Engineering. Working at CGD in an interniship in Information Systems Internal Audit.

Appendix
Statements of Execution



Caixa Geral de Depositos

DIRECÇÃO DE PESSOAL

DECLARAÇÃO

Para os devidos efeitos e a pedido do interessado, declara-se que **Diogo Manuel Leal Costa** se encontra a realizar um estágio profissionalizante a tempo inteiro nesta Instituição, durante o período compreendido entre 04/08/2014 a 03/02/2015.

O presente estágio decorre na Área de Auditoria a Sistemas de Informação e tem como objetivo consolidar e complementar os conhecimentos adquiridos na formação académica, através do contacto com a realidade profissional bancária

Direção de Pessoal, 21 de outubro de 2014

A Direcção de Pessoal

SIGN HERE

CAIXA GERAL DE DEPÓSITOS, S.A.
DIRECÇÃO DE PESSOAL

CGD001806 - 1.800.000 ex. 2014/Jan

Caixa Geral de Depósitos, S.A. - *Sede Social:* Av. João XXI, 63 • 1000-300 LISBOA - Capital Social 5 900 000 000 € - CRCL e Contribuinte sob o n.º 500 960 046