Design of a Framework for the Best Practices in Computer Forensics within the Cybersecurity Infrastructure in the Regulated Industry

Author: Eduardo Vázquez Ruiz
Advisor: Professor Jeffrey Duffany PhD.
Computer Science Department

Abstract

This Project is focused directly on the design of a Framework based on the join of the most important systems Cybersecurity and Forensic Analysis to avoid attacks in regulated industries and if we were already attacked, we know how to solve them. The technology has been evolved in an advanced way in the last ten years and along with this, there is the evolution of cyber-attacks. During this Project we will be able to appraise the important concepts within the good practices in the industry and see an incorporation of these in a Framework that unites the cyber-industry and the Forensic analysis, so that the use of this format can facilitate the industry incorporate their methodologies without them being affected.

Introduction

When we talk about Computer Forensics we can understand that it is related to an event that occurred or a crime committed where a device or computer system is involved. But what happens if this is entirely related to a regulated industry company? We know there are some differences between what Cybersecurity and Computer Forensics is, but when we see it closely we know their relationship.

Computer forensics is the practice of collecting, analyzing and reporting on digital data in a way that is legally admissible. It can be used in the detection and prevention of crime and in any dispute where evidence is stored digitally. More recently, Regulated Industries have used computer forensics to their benefit in a variety of cases.

Cybersecurity is the protection of internet-connected systems, including hardware, software and data, from cyberattacks. In a computing context, security comprises cybersecurity and physical security both are used by enterprises to protect against unauthorized access to data centers and other computerized systems.

Background

Framework Design

The Design of this Framework takes as reference the NIST Cybersecurity Framework.[1]

The typical IT Infrastructure

Seven Domains of IT Infrastructure can be found in a typical scenario. [2] These domains are not directly presented in the proposed Framework, but we can say that they are present within it.

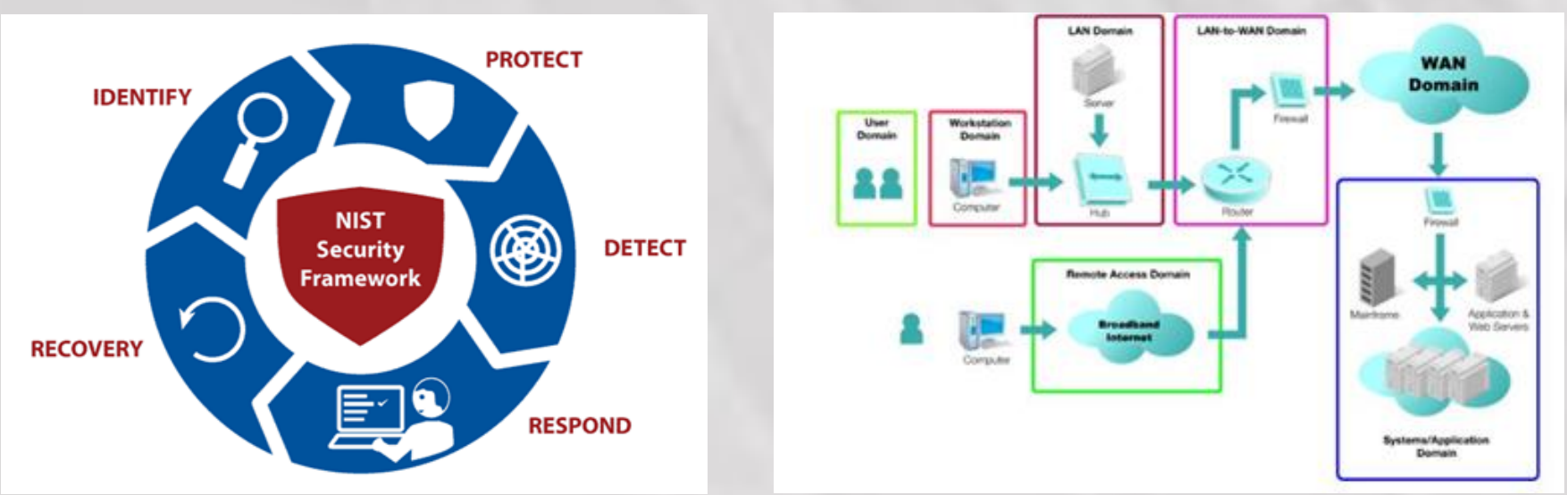


Figure 1
Framework design for a Regulated Industry and The Seven Domains

Problem

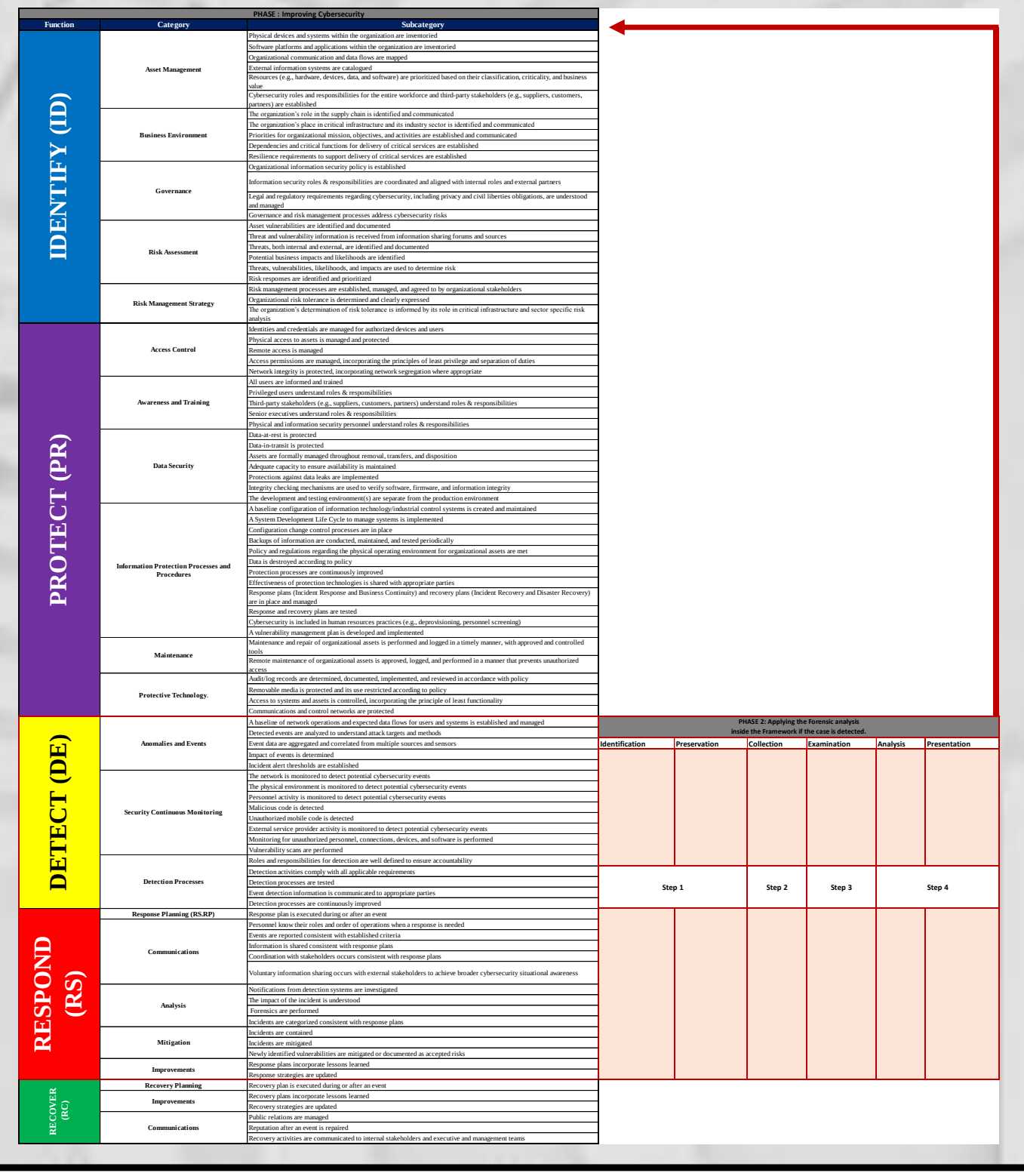
Cybercriminals are adopting new strategies to launch cyberattacks within modified and ever-changing digital ecosystems. In a regulated industry IT Security field, there are a lot of technological aspects, such as access control, biometrics, encryption, network security, security algorithm, etc. A set of fundamental principles come from the ISO 27000 standards. IT bases its security on these principles, but a framework that can include aspects of the regulated industry and strengthen cybersecurity is proposed in this project.

Methodology

Presenting the design

A Regulated Industry can use the Framework as a key part of its systematic process for identifying, assessing, and managing cybersecurity risk. The regulated Industry has his own gestion system and his process is the Quality compliance and the manufacturing process and procedures. The Framework is not designed to replace existing processes; an organization can use its current process and overlay it onto the Framework to determine gaps in its current cybersecurity risk approach and develop a roadmap to improvement.

Table 1
Framework Process Model


IDENTIFY (ID)
PROTECT (PR)
DETECT (DE)
RESPOND (RS)
RECOVER (RC)
Step 1
Step 2
Step 3
Step 4

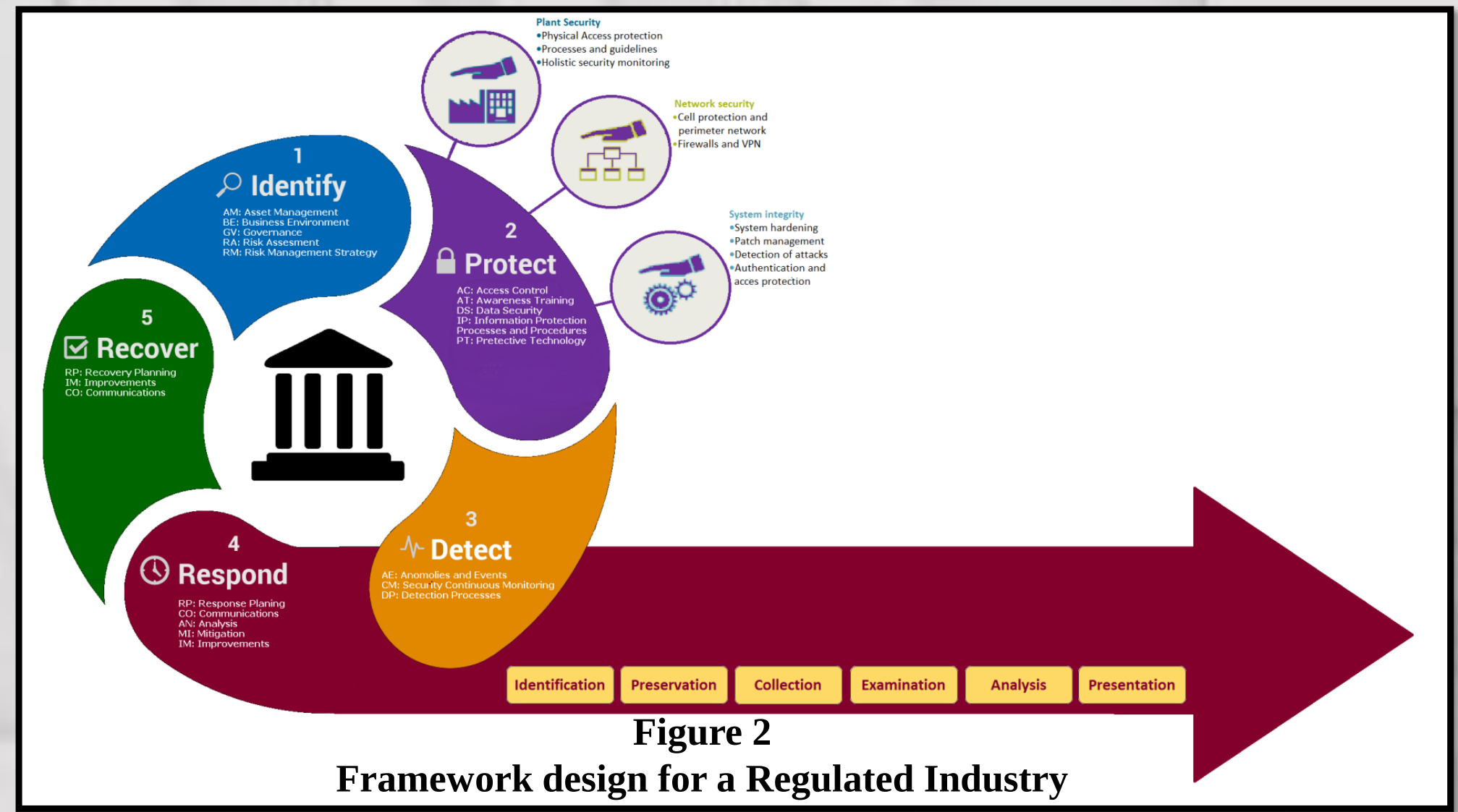


Figure 2
Framework design for a Regulated Industry

Testing the Framework

To verify the efficiency and operation of this Framework, it was put into practice in a normal regulated environment and it was decided to compare the current status with the new one, in this case a regulated company was chosen as an example to analyze this scenario.

In figure 8 we can see a representation of the IT current security framework illustrated. The composition of the work segments within the diagram indicates the areas to be reinforce.

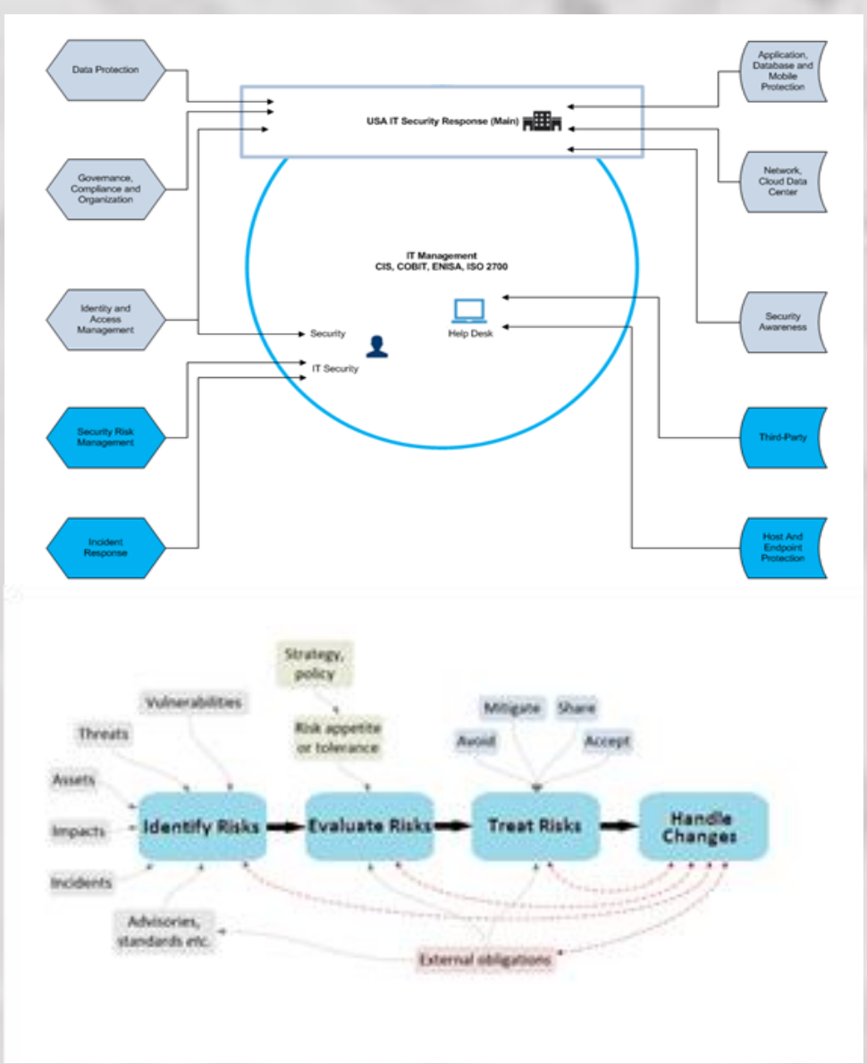


Figure 3
IT security Levels for the selected Industry And Selected Industry Actual Framework

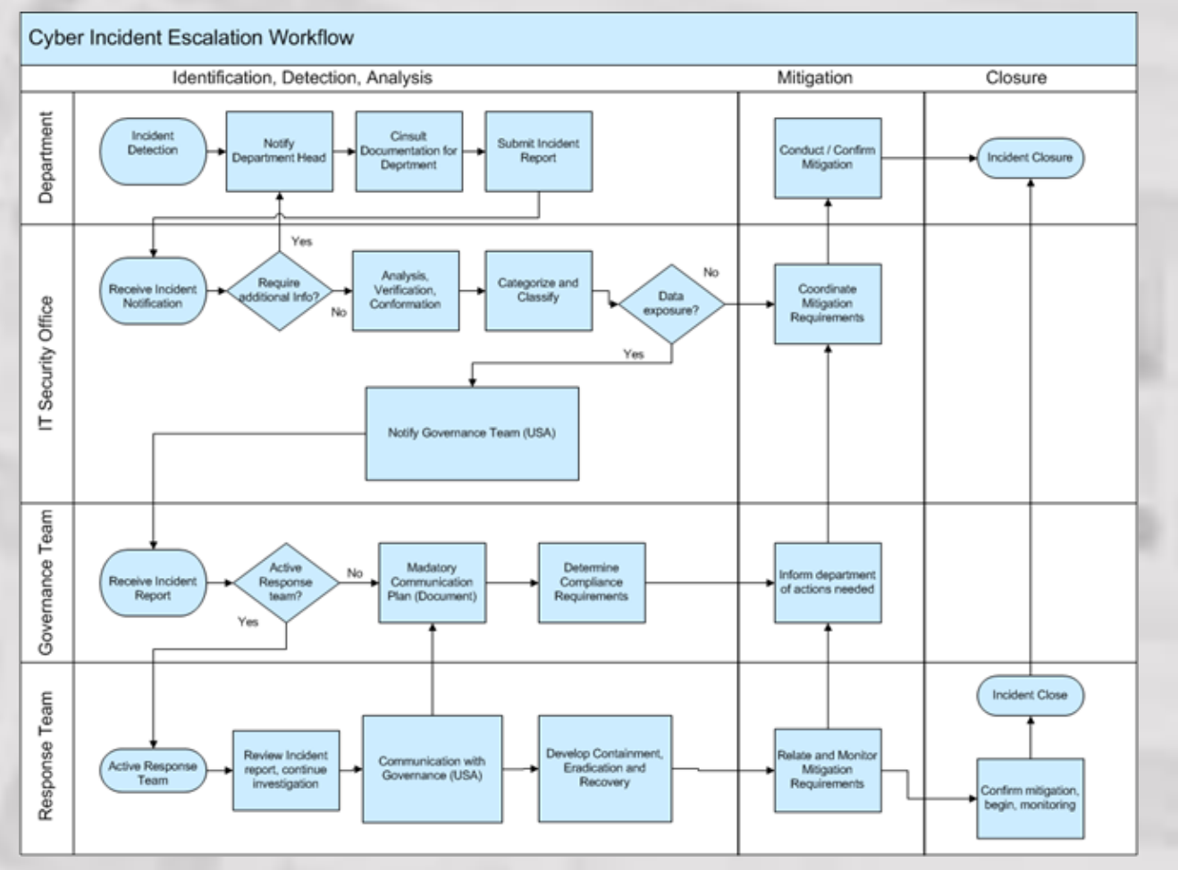


Figure 4
Cyber Incident escalation Workflow of the Selected Industry

Analysis

Testing with a Software

The use of software is very favorable in these cases for the handling of documents according to the category assigned within the Framework. The software used is NIST_CSF_Tool_1.0-WIN. This software is created by NIST in File Maker Pro and we can use it for the editing of our framework. The analysis of this would facilitate the inclusion of the different documents of the industry in a referential frame.

Portions of this software are Copyright 1984-2012 by FileMaker, Inc. All Rights Reserved.

Figure 5
Startup window screen

The software uses the database as a starting point and this gives us the ability to navigate from the beginning with the chain of elements. As you incorporate the elements you can navigate through them. The Framework provides the required program elements.

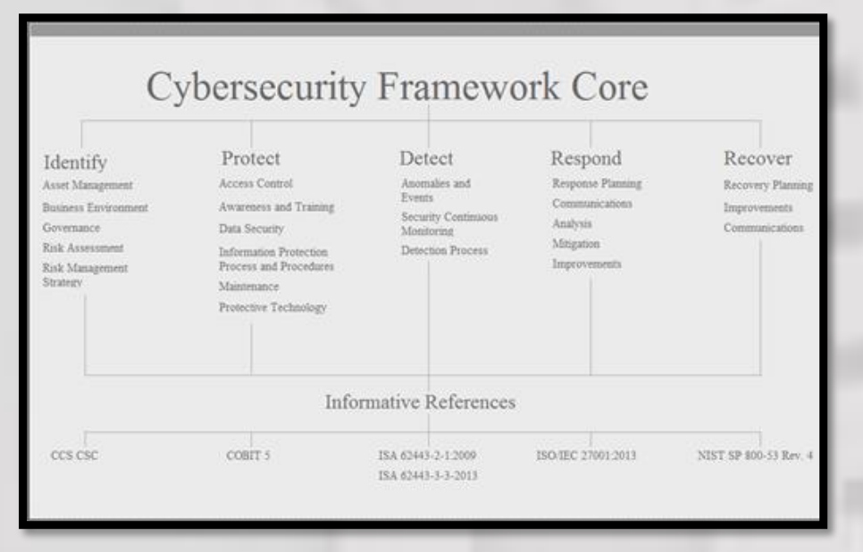


Figure 6
Home screen

Identify and Protect

In this area we will place the documentation related to our Framework. It is important to take into account all the regulations within the framework, even if they are not directly related to cybersecurity as long as the Framework can be completely aligned to the Industry.

Detect and Respond

In the case to this project, a forensic threat would not be allowed for proves because of the regulation the industry, but we can signal que the preparation of identifiers was initialization in our test, that are: Identification, preservation, collection, examination, Analysis, Presentation (recover).

Recover

As we indicated earlier, this scenario is always shown if we carry a threat, or a vulnerability detected, otherwise this Framework gives us the ability to maintain the continuous improvement as provided by the cycle of best practices.

Incorporating the data and documenting in the Framework

Selecting each one of the elements this directs us to the data base for each element. This is where you can incorporate the reports and documents.

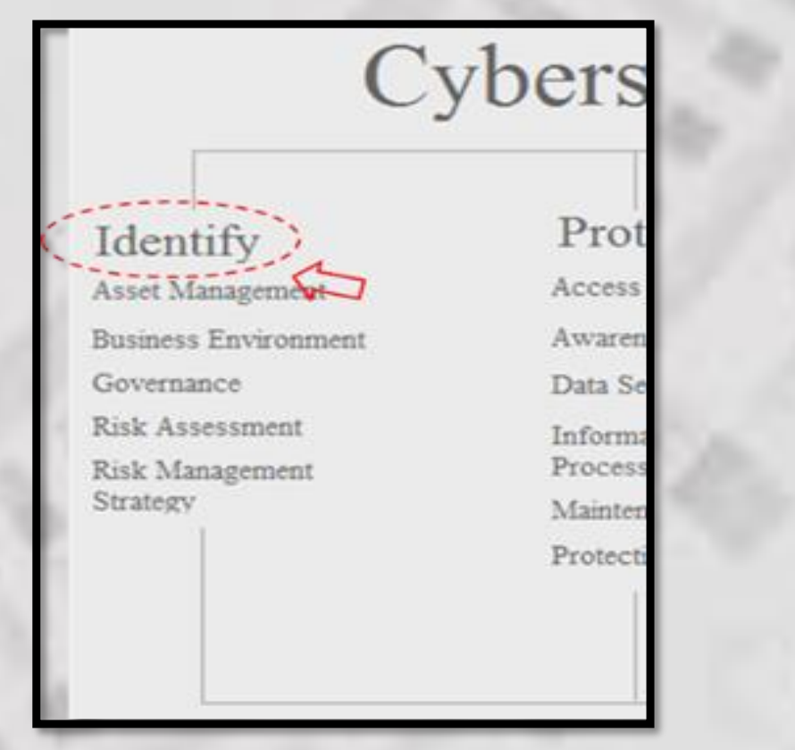


Figure 7
Selecting example

At the bottom of the Menu this shows us the area of informative documents for this ISO regulated industry and the quality and compliance documents can be incorporated as this can relate us to cybersecurity.

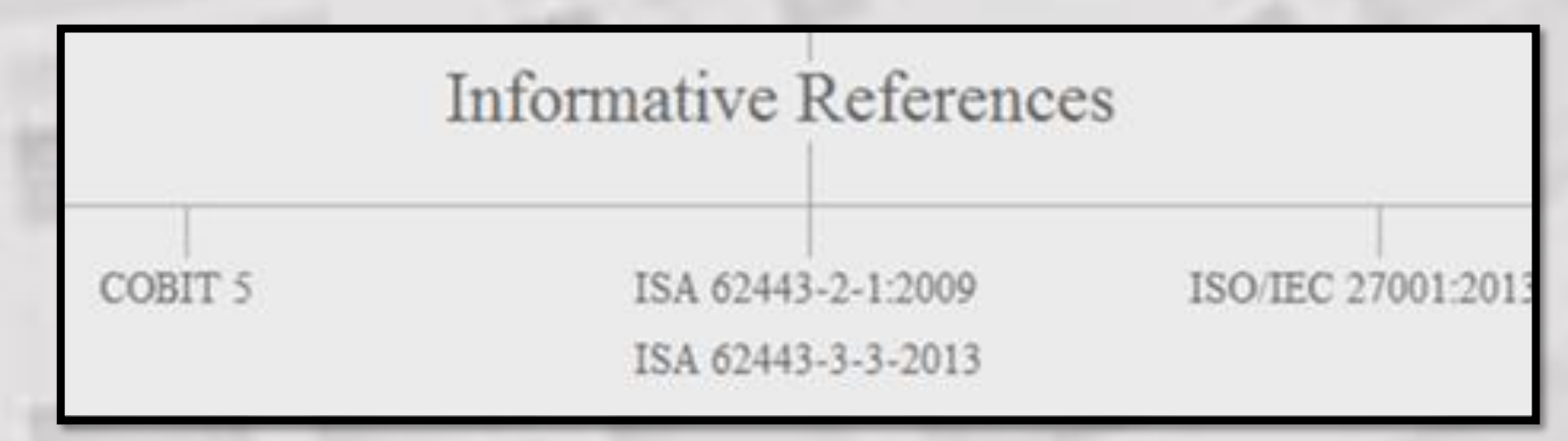


Figure 8
Informative Reference software screen

Discussion

After entering all the information obtained, this will save how the information is recorded in the database using excel.

This will generate a table in excel with most of the framework addressed. Now is the time when we can complete our Framework by completing the Forensic Analysis action and directing the information to this section. (See Table 1)

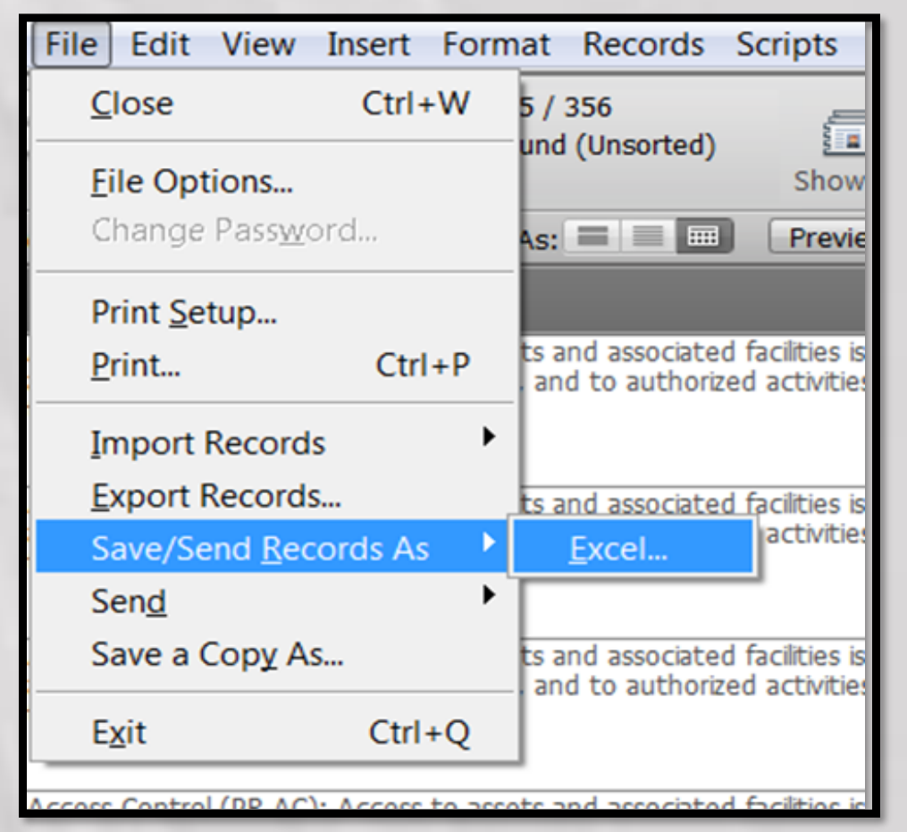


Figure 9
Save/Send Records example screen

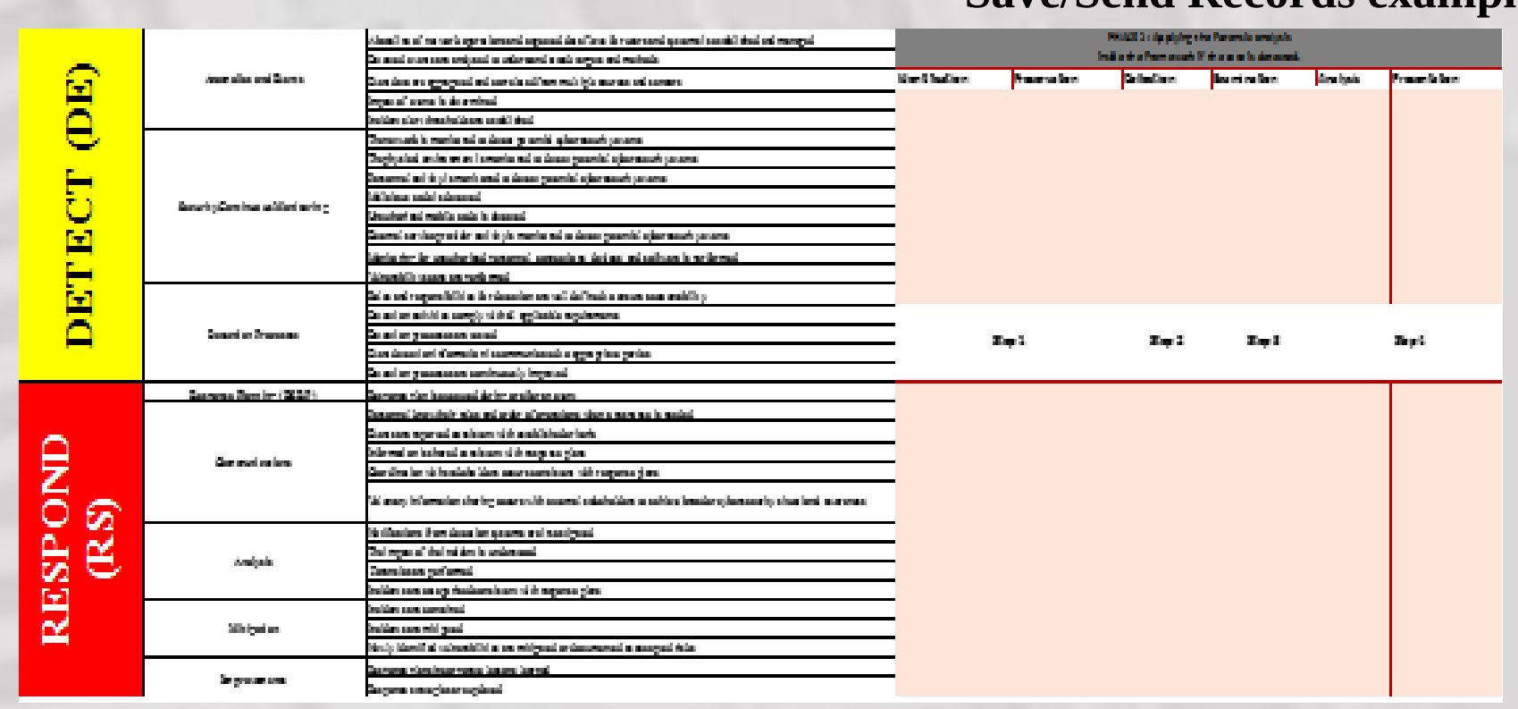

DETECT (DE)
RESPOND (RS)
Step 1
Step 2
Step 3
Step 4

Figure 10
Zoom of the forensic area in table 1

This more organized way shows us that at any point that is not being monitored it is easy to detect any vulnerability. The continuous way of carrying the Framework will facilitate the long-term improvement due to changes in technology.

Conclusion

The choice to use a particular IT security framework can be driven by multiple factors. The type of industry or compliance requirements could be deciding factors. The ISO 27000 series that is used for the Industry is the magnum opus of information security frameworks with applicability in any industry, although the implementation process is long and involved. However, it is best used where the company needs to market information security capabilities through the ISO 27000 certification, and this is the case. This proposed Framework in this article also can be used by any company and not necessarily a regulated industry to build a technology-specific information security plan. Any of them will help a security professional organize and manage an information security program. The only bad choice among these frameworks is not choosing any of them.

Future Work

After making this framework part of the cybersecurity culture, it is important to maintain the continuous improvement and continue implementing updates as the technology changes.

References

[1]National Institute of Standards and Technology, “Framework for Improving Critical Infrastructure Cybersecurity” CSRC., Gaithersburg, MD., USA, Version 1.1, April 16, 2018.

[2]Martin M. Weiss, “Compliance Law Requirements and Business Drivers,” in Auditing IT Infrastructures for Compliance, 1th ed. Mississauga, Ontario, Canada: World Headquarters, 2011, ch8. sec. 2, pp.169–188.

[3]"Guidelines for Smart Grid Cyber Security". National Institute of Standards and Technology. 2010-08-01. Retrieved 2014-03-30.

[4]Knapp, E. D., & Samani, R. (2013). “Applied Cyber Security and the Smart Grid Implementing Security Controls into the Modern Power Infrastructure”. Burlington: Elsevier Science.

[5]Evans, Dave “The Internet of Things How the Next Evolution of the Internet Is Changing Everything.” Cisco Internet Business Solutions Group (IBSG). April 2011.

[6]Wolfgang Schwab “The State of Industrial Cybersecurity 2018.” PAC – a CXP Group Company. June 2018