ERMF Enterprise Risk Management Framework

Domenico Filitti
EXO Research
Potenza - Italy
m.filitti@exo-ricerca.it

Francesco Abenante
EXO Research
Potenza - Italy
f.abenante@exo-ricerca.it

Giuseppe Pace
EXO Research
Potenza - Italy
g.pace@exo-ricerca.it

The evolving network interconnection produces risks and critical situation among integrated systems based on shared platform and, in addiction to physical vulnerability, new generation threats exist now (social engineering attacks; hacking; the proliferation of malicious software; spyware and other potentially unwanted software).The ERMF framework development project was created in order to give support to security managers matching best practices, tools sw. and open source information. It works on real-time integrated risk assessment approach.

Inventory Assets, Assessment, Risk Analysis, Risk Treatment Plan, Vulnerability, Threats

1. INTRODUCTION

The evolving network interconnection produces risks and critical situation among integrated systems based on shared platform and, in addiction to physical vulnerability, new generation threats exist now (social engineering attacks; hacking; the proliferation of malicious software; spyware and other potentially unwanted software). Stuxnet could be a good example: a worn able to spy e re-programming PC e industrial PLC.

For this reason, it's necessary to protect infrastructures with new methodologies by evaluating your own vulnerabilities and investing in safety.

Managing large IT infrastructures involves to measure how safety is important understanding which kind of safety is necessary for our business. For this reason, it's important to understand the kind of risk and evaluating the right remediation priority. Usually, a budget is suitable in order to find the right tradeoff between needs and resources.

2. ERMF FRAMEWORK

The ERMF framework development project was created in order to give support to security managers matching best practices, tools sw. and open source information. It works on real-time integrated risk assessment approach.

The software solution was developed by using opens source products and technologies (S.O. : Linux; RDBMS: MySql; Application Server: Tomcat; Java language) in accordance with ISO 27001:2013 international standard.

ERMF is an integrated risk assessment framework able to support assets analysis and the maintenance of appropriate controls (information, software, physical, services, people, intangibles)

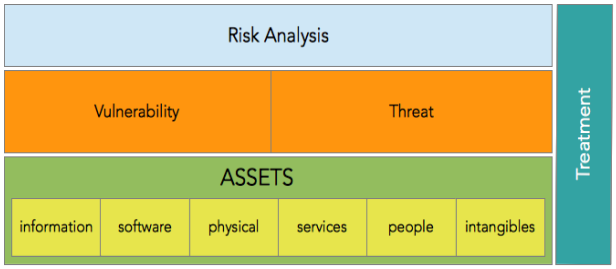


Figure 1: *Risk Assessment*

2.1 Asset management

The framework allows to identify and classify assets. For each class, the required information are stored in order to recover from a disaster, including type of asset, format, location, backup information, license information and a business value

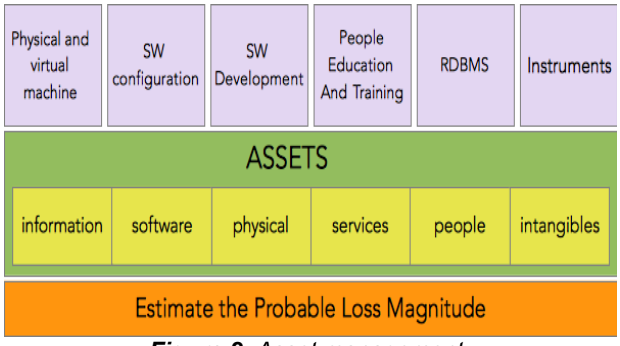


Figure 2: *Asset management*

For each asset, a set of software application module are included. For example, the modules security roles and responsibilities, training plan, training course are available for the asset people whereas organization's controls, configurations, virtual machine, computer network diagram are the modules created for the physical asset. Other system's interface (BugZilla, DPKG, YUM, RPM, MySQL, etc...) was developed for specific assets, like Sw Configuration, SW Development, RDBMS.

ERMF support the organization in estimating PLM to determine which threat action is most likely.

2.2 Vulnerability Assessment

ERMF support the security managers in vulnerability assessment, the process of identifying the vulnerabilities (OpenVas) and prioritizing them according to their severity.

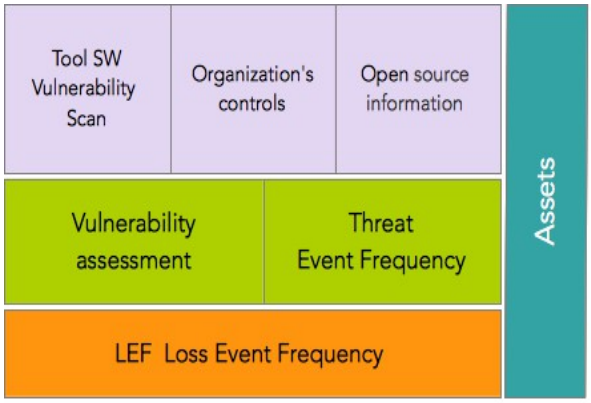
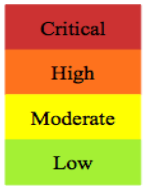


Figure 3: *Loss Event Frequency*

For each asset, it is estimated both the Probable Threat Event Frequency (TEF) and the related Vulnerabilities. Once we have estimates of Loss Event Frequency and Probable Loss Magnitude **ERMF** derive the Risk Value.



For each Asset/Threat a treatment is required: Reduction, Avoidance, Transfer, Retention

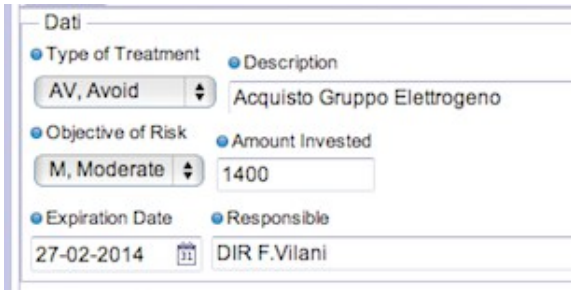


Figure 4: *Example: Treatment detail*

2.3 Reports

ERMF produces all the required reports: Inventory assets; Statement of Applicability; Risk Analysis; Business Impact Analysis; Risk Treatment Plan.

2.4 Use Case

ERMF is used in the following area:

- Web Application and data management for Public Administration
- Air pollution monitoring system (ambient air quality and stationary source emission industrial plants)
- Software House (software development)

Vulnerabilities

Actions	Description	Category	Level	Connected
	Specifiche incomplete per gli svil	3.01, Unclear or incomplete spe	L, Low	(24) software failure
	Insufficienti procedure per il testir	3.02, No or insufficient software	L, Low	(24) software failure (25) use of software by unauthorized users
	Insufficienti meccanismi di autent	3.04, Lack of identification and a	L, Low	(27) masquerading of user identity
	insufficiente o mancante log	3.05, Lack of audit-trail (could b	L, Low	(26) use of software in an unauthorized way
	Sessioni protette accessibili per a	3.11, No"logout" when leaving t	L, Low	(25) use of software by unauthorized users
	Assenza o insuffi di meccanismi a	3.12, Lack of effective change c	L, Low	(24) software failure
	Mancanza o insufficiente docime	3.13, Lack of documentation (cc	L, Low	(31) operational staff error - developer

<< < > >> 1

Figure 5: *Example: Asset – Vulnerabilities and related threats*

Threats

Actions	Description	Category	Level	LEF	Risk level	Expected Risk l	Treatment
	Errori in fase di proc	24, software failure	L, Low	Very Low	Low		Add Treatment
	Uso non autorizzato	25, use of software	L, Low	Very Low	Low		Add Treatment
	Uso del SW in modc	26, use of software	L, Low	Very Low	Low		Add Treatment
	Mascheramento ide	27, masquerading	L, Low	Very Low	Low		Add Treatment
	Errori del team di sv	31, operational sta	L, Low	Very Low	Low		Add Treatment

Figure 6: *Example: Asset - Threats*

3. REFERENCES

ISO/IEC 27001:2013 - Information security management system – Requirements

ISO/IEC 27002:2013 - Information technology -- Security techniques - Code of practice for information security management

ISO/IEC 27005:2011 - Information technology -- Security techniques - Information security risk management

FAIR – ISO/IEC 27005 Cookbook: The Open Group, (2010), United Kingdom