Gartner

Research

Publication Date: 22 July 2005 ID Number: G00129252

Understanding Risk Analysis, Policy Audit and Vulnerability Assessment Terminology Is Key to Examining Your Security Conditions

Carsten Casper

Examining an organization's security condition requires assessments, analyses, audits, monitoring and management in the areas of risk, compliance, vulnerabilities, policies and security. But the terminology often varies, so understanding the terms and scope of the methods used is essential.

TABLE OF CONTENTS

1.0 Introduction 3

2.0 Examination Methods 4
- 2.1 Analysis 4
- 2.2 Assessment 4
- 2.3 Audit 4
- 2.4 Monitoring 5
- 2.5 Management 5

3.0 Examination Scope 5
- 3.1 Risk 5
- 3.2 Compliance 6
- 3.3 Vulnerabilities 6
- 3.4 Policy 7
- 3.5 Security 7

4.0 Means for Carrying Out an Examination 7

LIST OF TABLES

Table 1. Terminology Used, Independent of Industry, Technology and Country 5

Table 2. Types of Risks 6

LIST OF FIGURES

Figure 1. From Analysis to Management 3

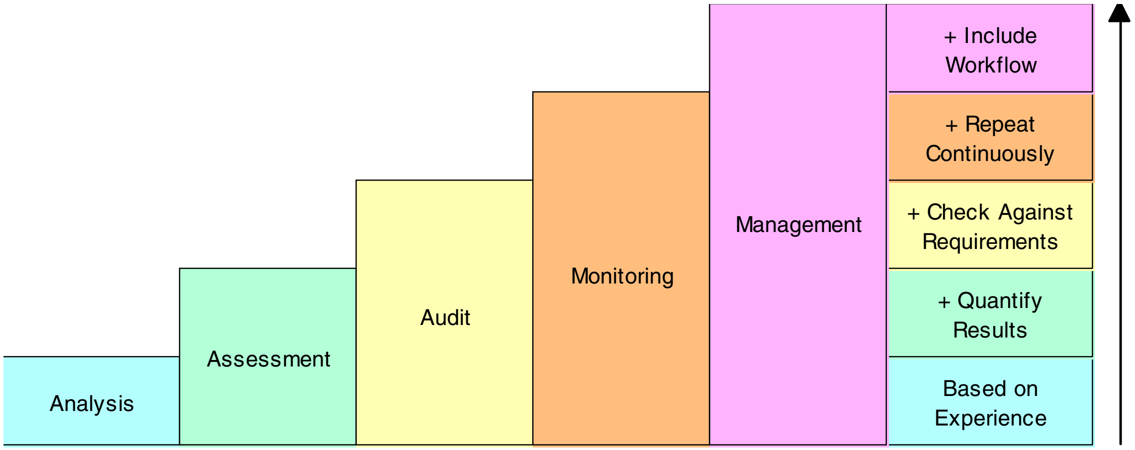
Figure 2. Finding the Right Term 8

ANALYSIS

1.0 Introduction

Examining an organization's security condition requires assessments, analyses, audits, monitoring and management in the areas of risk, compliance, vulnerabilities, policies and security. Risk analyses, policy audits and compliance assessments are examples of the various methods used to identify problems and describe the current situation in a given organization (see Fgure 1). Yet, confusion is omnipresent, because these terms and their scope hold different meanings for different actors. Thus, it is important for those involved in this examination to understand the commonalities and differences of each of these elements as much as the scope in which the methodologies and tools are valuable.

Figure 1. From Analysis to Management



- Analysis
- Assessment = Analysis + Valuation
- Audit = Assessment + Policy
- Monitoring = Audit + Time
- Management = Monitoring + Workflow

129252-1

Source: Gartner (July 2005)

This is paramount when lines of work between IT personnel and the rest of the organization cross. For example, while in more and more cases, IT is used to support and automate problem identification processes, IT organizations must be aware that the methodologies and technologies they use may already be applied elsewhere in the organization and that, at the same time, IT itself is part of the overall examination (for example, IT risks are part of operational risk assessments).

On the other hand, when IT organizations incorporate a business perspective in their examination procedures using the same terms for different things, or using different terms for the same thing, inevitable misunderstandings occur. Thus, IT organizations cannot use terms such as "analysis," "audit" or "assessment" freely, especially because these terms have been in use in the business world for decades.

Clarifying the terms and scope of the methods used is also essential to professional associations, which offer audit and assessment methodologies; they need to understand the variety of business and IT situations in which these methods might be used.

To avoid conflicting meanings, qualifications can be useful. However, typical qualifiers, such as "risk," "security" or "policy," are not precise enough. For example, the term "risk assessment" describes *what* is being assessed, while the broadness of the term "risk" can already add to the confusion, given the various types of risks (IT, financial, environmental and project). Similarly, the terms "security" (IT, information and physical) and "policy" take on various forms. As a result, it is often difficult for an organization to carry out an examination, to research the market for a methodology and to find a tool that matches its requirements. Vendors have trouble crafting appropriate marketing messages and product names. This is specifically the case in areas that undergo change, caused by new regulatory requirements (for example, in the area of corporate governance compliance) or competition in a mature market (for example, moving from vulnerability assessment to vulnerability management). When users look at specific vendor offerings or at a market in general, such vagueness in terminology causes different perceptions of what is available. Hence, it is necessary to clarify the scope of a "problem identification" — what is an appropriate method of examination and how can this exercise best be described so that all involved parties share a common understanding.

2.0 Examination Methods

Refer to Figure 1 for the most-common examination methods; they are described in a way that one builds on top of the other, assuming an increase in value as well as complexity (and thus, cost). One can argue what precisely the terms mean, but in absence of any standard, it is best to adhere to the plain meaning of the English term.

2.1 Analysis

An analysis examines a given situation, checking for obvious deficits according to professional experience or even common sense. The examination can be structured and repeatable, but it is not standardized. Its purpose is to get a better understanding of the problem. Results have to be interpreted. "Review" is a term similar to analysis. An IT security "penetration test" is an analysis whose mere purpose is to identify if a perimeter can be penetrated or not. An IT security "vulnerability scan" is an analysis, which identifies flaws, but determining if such a flaw really poses a problem for the organization is left to a subsequent step.

2.2 Assessment

An assessment goes further than an analysis, as it includes some sort of valuation by quantifying the results of the examination. An assessment not only identifies a problem, but also describes how much of a problem it is. A related term in IT security is "vulnerability assessment." As an extension of a "vulnerability scan," a "vulnerability assessment" sets the results of a scan into the context of the organization and assigns an urgency level. In general, an assessment uses a structured approach, is repeatable and describes the level of a problem, but it cannot be compared with other assessments outside of the organization as long as the structure of the assessment and the metrics used to quantify the results are not standardized.

2.3 Audit

An audit compares a given situation with some sort of standardized situation. This can be an external standard (for example, a law or an industry standard) or an internal one (that is, a policy document that describes how it should be). It does not make sense to audit against best practices, because best practices are not described in a formal way. The results of an audit explain how much reality deviates from an expected or required situation. Documents, processes, programs and organizations can all be subject to an audit. A related term to audit is "measurement" (as in "risk measurement").

2.4 Monitoring

Monitoring is an operational activity, which introduces the notion of time. Whereas the previous activities are snapshots at any given point in time (though these snapshots can be repeated), the process of monitoring is ongoing. Proper monitoring requires an established framework to be able to show trends and to repeat activities consistently and efficiently. Monitoring goes beyond the description of a situation; it already includes potential response steps.

2.5 Management

Management is the most comprehensive, most valuable and most expensive way of dealing with problems. It involves the steps of understanding the situation (analysis), determining the extent of the problem (assessment), standardizing the examination (audit), and continuing these activities over time (monitoring). Moreover, it adds the components of remediation, initiating and tracking changes, and also includes the necessary communication within the organization (workflow). It is a strategic activity.

3.0 Examination Scope

To put the methods of analysis, assessment, audit, monitoring and management into context, these terms are usually qualified using other terms, such as "risk," "security," "compliance," "policy" and "vulnerability." In fact, all possible combinations are in use around the world to some extent. Table 1 shows which ones are more common than others.

Table 1. Terminology Used, Independent of Industry, Technology and Country

Point in Time			Continuous	
Risk Analysis (+)	Risk Assessment (+)	Risk Audit (-)	Risk Monitoring (-)	Risk Management (+)
Compliance Analysis (-)	Compliance Assessment (o)	Compliance Audit (+)	Compliance Monitoring (+)	Compliance Management (+)
Vulnerability Analysis (o)	Vulnerability Assessment (+)	Vulnerability Audit (-)	Vulnerability Monitoring (-)	Vulnerability Management (o)
Security Analysis (-)	Security Assessment (-)	Security Audit (o)	Security Monitoring (o)	Security Management (+)
Policy Analysis (+)	Policy Assessment (-)	Policy Audit (-)	Policy Monitoring (-)	Policy Management (+)
Note: + = widespread, o = used occasionally and - = hardly ever used.				

Source: Gartner (July 2005)

Of course, these combined terms as well are subject to interpretation. Risk, compliance, security, policy and vulnerability need to be put into context.

3.1 Risk

Many types of risks are typically not included when IT risks or IT security risks are under examination (for example, financial risks and environmental risks — also see a comprehensive list in Table 2). However, which risks are addressed often depends on the context and is not always explicitly stated. No standard definition of risk categories exists. Moreover, different perspectives on risk converge as information technology organizations (ITOs) broaden their understanding and take risks of noncompliance and physical risks into account, while business managers deepen their understanding of IT risks. The Basel II regulation, for example, uses the term "operational risk" extensively, and IT security managers wonder what precisely that means for their IT operations, finding no clear answer in the regulation itself.

Table 2. Types of Risks

Types of Risks	
Actuarial risk	Information security risk
Credit risk	Insurance risk
Currency exchange risk	Legal risk
Derivatives risk	Liquidity risk
Emerging markets risk	Market risk
Energy risk	Operational risk
Environmental risk	Project risk
Equities risk	Reputation risk
Financial risk	Social risk
IT risk	Technology risk
IT security risk	

Source: Gartner (July 2005)

3.2 Compliance

In times when corporate governance has all the attention, the meaning of compliance seems obvious. But certain industries (pharmaceutical and financial) have long used audits and assessments to examine their compliance with specific regulations. Furthermore, the same organization can comply with a pharmaceutical regulation as much as with a firewall policy. Both situations have to be audited. Organizations must define a holistic compliance strategy, which describes the scope for various kinds of examinations and the relationship between them in clear terms. Generally speaking, they must take into account two types of compliance: compliance with external (legal) requirements, often called "regulatory compliance," and compliance with internal requirements, often called "policy compliance." However, even this line is blurred at times. The question of "privacy compliance," for example, can address compliance with privacy laws as much as compliance with a company's internal privacy policy. In fact, regulatory compliance often predicates policy compliance (that is, the regulations require that the organization institute internal policy).

3.3 Vulnerabilities

Many tool vendors use the term "vulnerability" to describe software defects. However, it can also be used to describe deficiencies in policies, processes or organizational structures. For example, a system that accepts an empty password (that is, a password of the length 0) can be considered a vulnerable system (and a tool would probably detect this as a vulnerability), even though the vendor consciously shipped the system this way. A low-security organization might not consider this empty password a vulnerability, whereas a security-conscious organization would probably tag it as a violation of a corporate policy. In any case, such technical vulnerabilities can be checked by technical means. Other vulnerabilities, such as an employee revealing a password for obscure reasons or in exchange for a gift, can typically not be caught by vulnerability scanners. However, organizations have to assess such social or behavior-caused vulnerabilities as well.

Vulnerabilities are related to threat and risk — and often mixed up with them. In essence, a vulnerability is a characteristic *of* a system or an organization, whereas a threat originates *from outside* the system. If a threat matches a vulnerability, then the system is at risk. A threat analysis is typically known only as part of a larger risk or security analysis.

3.4 Policy

A policy can be anything from a document that describes how to configure an operating system to a strategy to govern a country. The least common denominator is that a policy describes how a situation should be. The term "policy" should be avoided unless it can be qualified precisely (for example, IT procurement policy, e-mail usage policy, enterprise resource planning rollout policy, access control policy), and enforced effectively. In many cases, terms such as "guideline" (for detailed, low-level documents) or "strategy" (for high-level, long-term documents) are more descriptive and appropriate.

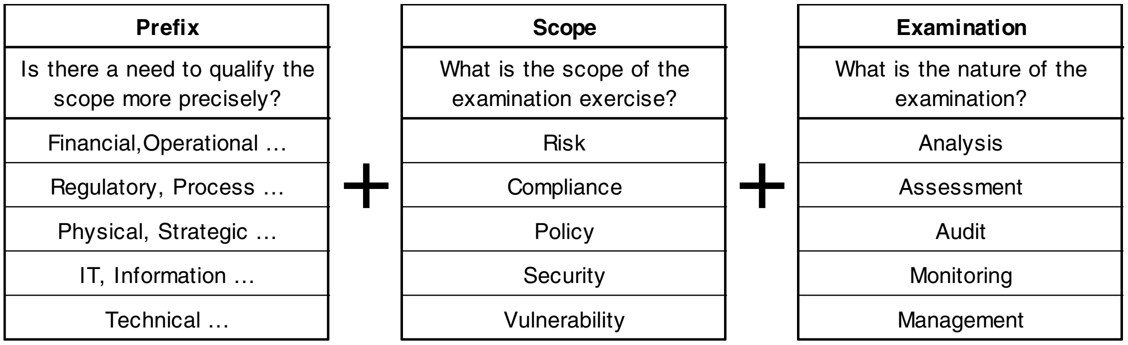
3.5 Security

For enterprises, security mostly consists of IT security, information security and physical security. For the government sector, but also for the energy, transport and telecommunications industries, the notion of national security or critical (information) infrastructure protection plays a role, although this distinction is usually rather obvious. Increasingly blurred, however, is the line between security and disaster recovery/business continuity (DR/BC) or, more broadly, "operations." Both disciplines use similar measurement techniques (for example, business impact analysis) and control mechanisms (for example, redundant resources). A DR/BC audit will evaluate how well an organization can recover from an incident, and a security audit will evaluate which mechanisms are in place to prevent the incident. There is also an overlap of threats against which security countermeasures and DR/BC countermeasures protect. A redundant data center, built to prevent data losses in case of a natural disaster, will also help if the primary data center has been hacked. Vice versa, major virus outbreaks and ongoing denial-of-service attacks can have devastating effects, against which IT security measures, such as firewalls and antivirus software, are possible protections. However, for the choice of technologies and procedures, the origin of the risk (that is, the reason for doing something against it, the "motivation") does not really play a role. It does not help to determine the extent of a threat, either. In fact, organizations increasingly address security and DR/BC together, mutually using measurement results and enforcement technologies, even though they do not yet establish a common organization.

4.0 Means for Carrying Out an Examination

To describe an examination as precisely as possible, it is best not only to determine the scope on a high level, but also to use some additional qualifier or prefixes, as Figure 2 illustrates.

Figure 2. Finding the Right Term



Prefix		Scope		Examination
Is there a need to qualify the scope more precisely?		What is the scope of the examination exercise?		What is the nature of the examination?
Financial,Operational …		Risk		Analysis
Regulatory, Process …	+	Compliance	+	Assessment
Physical, Strategic …		Policy		Audit
IT, Information …		Security		Monitoring
Technical …		Vulnerability		Management

Note: Many, although not all, combinations are possible and in use: "Information security audit," "IT risk assessment," "vulnerability management," "regulatory compliance audit" and "operational risk analysis." None of these lists are complete. "Privacy audit," "risk measurement" or "policy compliance" are popular terms as well.

Source: Gartner (July 2005)

For many of the above-mentioned combinations, technologies are available to support the underlying process (see, for example, "Selecting the Risk Assessment Method of Choice," "Security Event Log Analysis: Process Development and Tool Selection," "META Trend Update: Security Management Centers of Gravity," "Risk Analysis Software: Perspective" and "Magic Quadrant for Security Information and Event Management, 2H05"). However, it is worth noting that the set of tools to consider is much broader. Generally speaking, tools fall under the following categories:

- Software tools — These examine IT resources directly, such as configuration or vulnerability scanners; these can also be appliances.
- "Paper" tools —These include questionnaires, checklists and interview guidelines to get a broader understanding, which includes strategic and organizational aspects.
- Automated paper tools — These include computer-based checklists and Web surveys to execute an examination more efficiently while being flexible enough to include various nontechnical aspects.
- Collaboration tools —These include interviews or the Delphi method to get an agreement on the current situation.
- Management tools — These include databases, e-mail or ticketing systems to enable a tracking over time and a workflow between affected parties.

These tools' applicability is not restricted to one type of examination. The challenge is to assemble a set of tools for a given purpose. For each examination project, we suggest to start as granular as possible and to broaden the scope, only if a method exists to address each of the individual problems. For example, if you use a vulnerability scanner for a vulnerability assessment, do not turn this examination into a risk assessment, when there is not yet a clear understanding of risk in the organization and how other types of risk (such as physical and information security) are addressed. To start an analysis, audit, assessment, monitoring or management activity, pursue the following steps:

- Identify the target environment to be examined (for example, infrastructure domain, specific application and business process).

- Identify the audience(s) of the examination report (technical staff, business units, legal department and external parties).
- Select an appropriate examination method and be aware of the differences (refer to Figure 1).
- Qualify the scope of the examination as precisely as possible (refer to Figure 2). Do not set the scope of the examination larger than necessary.
- Relate to well-known standards and terminology wherever possible. Avoid generic terms.
- Pick an appropriate set of tools to carry out the examination (for example, paper, management and software tools)

Only if the examination is scoped properly and given a precise, descriptive name, can internal parties (IT, business and legal) as well as external parties (industry association, regulatory authority, vendor and consultant) communicate properly and efficiently.

RECOMMENDED READING

"Selecting the Risk Assessment Method of Choice"

"Security Event Log Analysis: Process Development and Tool Selection"

"META Trend Update: Security Management Centers of Gravity"

"Risk Analysis Software: Perspective"

"Magic Quadrant for Security Information and Event Management, 2H05"

Acronym Key and Glossary Terms

BC	business continuity
DR	disaster recovery
ITO	information technology organization

REGIONAL HEADQUARTERS

Corporate Headquarters
56 Top Gallant Road
Stamford, CT 06902-7700
U.S.A.
+1 203 964 0096

European Headquarters
Tamesis
The Glanty
Egham
Surrey, TW20 9AW
UNITED KINGDOM
+44 1784 431611

Asia/Pacific Headquarters
Level 7, 40 Miller Street
North Sydney
New South Wales 2060
AUSTRALIA
+61 2 9459 4600

Latin America Headquarters
Av. das Nações Unidas 12.551
9 andar—WTC
04578-903 São Paulo SP
BRAZIL
+55 11 3443 1509