
Gunnar Wahlgren¹, Stewart Kowalski²
Stockholm University
1: (wahlgren@dsv.su.se), 2: (stewart@dsv.su.se)

ABSTRACT

We combined ISO 27005 framework for IT Security Risk Management with NIST Multitier framework and we claim that IT Security Risk Management framework exist at each organizational levels. In this paper we concentrate on the monitoring and communication steps of IT Security Risk Management and especially escalation of new IT Security Incidents. We present a first draft to an IT Security Risk Escalation Capability Maturity Model based on ISACA’s Risk IT Framework. Finally we will use our approach in a cloud computing environment as we believe that it is necessary to react fast on incident and therefore a need to have a well-documented and communicated monitoring and escalation processes between different organizational levels.

KEYWORDS


1 INTRODUCTION

Cloud computing is fast growing and a majority of organization will use some form of cloud computing in the near future [1]. This make cloud computing critical as millions of users could be affected e.g. in cyber-attacks so the question to ask is: Do we need to have a new IT Security Risk Management framework for managing IT Security Risks at the speed of change?

According to ISO27005 [2] IT Security Risk Management consists of three main steps: (i) IT Security Risk Assessment, (ii) IT Security Risk Monitoring, and (iii) IT Security Risk Communication. During the different eras in history of computing, from mainframe to cloud computing, IT Security Risk Assessment has almost remained the same and a number of different tools have been developed during the years [3]. The most important purpose of IT Security Risk Assessment is to determine the acceptable risk level of the organization and, if necessary, install new countermeasures to reach that level.

The main step that has change is primarily IT Security Risk Monitoring as it is necessary to react fast on new threats and incidents. This means that also the third main step, IT Security Risk Communication between different organizational levels, also need to be changed so Organizations have a well-documented and communicated monitoring and escalation processes. This is especially important in a cloud computing environment where resources are shared between other cloud customers and can be rapidly changed [4].

The purpose of this paper is to propose a model for IT Security Risk Management for cloud computing where the focus is on IT Security Risk Communication and to some extent IT Security Risk Monitoring. The paper is divided into 4 sections. In the
first section we present ISO27005 and other framework. In the second section we present our approach. In the third section we discuss how our approach could be used for Cloud Computing. In the last section we conclude the paper with suggestions for future research.

2 BACKGROUND

2.1 IT Security Risk

We use the term IT Security Risk to distinguish it from other Business Risk like investment risk, credit risk, market risk etc. NIST Special Publication 800-30 page 8 [5] has the following definition: “Risk is a function of the likelihood of a given threat-source’s exercising a particular potential vulnerability and the resulting impact of that adverse event on the organization”. IT Security Risks are then: “Adverse Event on the Information Technology Systems of an Organization”.

There are basically two ways to calculate risk; Quantified or Qualified approaches. The quantitative approach uses the expected number of adverse events per year and the average cost for the occurrence of one event. The qualitative approach, on the other hand, use a scale with (e.g.) three values; low, medium or high. This scale is used for expressing both the expected number of events and the cost for one occurrence.

All organisations today have some kind of information system (IS) based on information Technology (IT). Organizations are exposed of different threats both inside and outside the organization. These threats can be avoided with help of countermeasure of different kind.

However it is difficult to justify spending effort on countermeasures for an IT-system that have little business impact for the organisation. To find the right mix of countermeasures a number of IT Security Risk Management methods and tools have been developed to assist the organization. ISO 27005 is an international standard that describe how IT Security Risk Management should be performed.

2.2 IT Security Risk Management

The term IT Risk Management refers to approaches and methods that lead to cost effective security solutions and countermeasures ISO27005 [2]. This is done by a process of measuring the security risk to IT systems and assuring adequate levels of protection. IT Security Risk Management is a continuous process and consists of the following steps listed below and outlined in figure 1.

- Risk Assessment that consists of Risk Analysis and Risk Evaluation.
- Risk Analysis that consists of Risk Identification and Risk Estimation.
- Risk Identification where identification of assets, threats, existing countermeasures, vulnerabilities and consequences (impacts) is made.
- Risk Estimation where impacts of threats to different assets are calculated using the quantitative or qualitative approach.
- Risk Evaluation where different risks are compared against risk levels based on risk evaluation and risk acceptance criteria.
- Risk Treatment where, if necessary, new countermeasures are installed.
- Risk Acceptance where residual risks to different assets are stated.
- Risk Communication where the risks are communicated to the organization.
- Risk Monitoring and Review where a continuous monitoring of risk is done.

The result of risk assessment and risk treatment is an IT security risk model that represents how an organization handles threats to information assets with help of countermeasures of different kind. In the rest of the paper we will discuss some important issues how risk communication and risk monitoring could be done in organizations.

### 2.3 NIST Multitier Organization-Wide Risk Management

Organization can be modeled to have three different levels where IT Security Risk Management decisions are made: (i) Top management, (ii) Middle management, and (iii) Operational Staff. The decision of top management is often of strategic nature while middle management is of tactical nature. Staff on the other hand had to deal with real IT security risk incidents and often had to react directly. According to NIST [6] an organization normally has three different levels (Tiers) where one can look at the organization from different views.

![Figure 2: NIST Multitier Organization-Wide Risk Management.](image)

On the first Tier we look at risks from an organizational perspective. Risk management activities at Tier 1 directly affect activities on the other tiers by implementing governance structure that is consistent with the strategic goals of the organization. Governance includes such thing as determination of risk tolerance. Risk tolerance is the level of risk that is acceptable to the organization. Risk tolerance is often influence by the culture of the organization.

Tier 2 view risk from a mission/business processes perspective by designing and implementing processes that support business functions defined at Tier one. Important issues at Tier 2 are enterprise architecture where information security architecture is integral part. Another issue is risk response strategies, which could be; accept, avoid, mitigate, share, and transfer.

Information system perspective at Tier 3 is guided by the risk decisions and activities at Tier 1 and 2. Risk management activities at Tier 3 are also integrated into the system development life cycle. At Tier 3 risk-based decisions are made regarding the implementation, operation and monitoring of organizational information system.
2.4 Cloud Computing Benefits

Cloud computing is not a new technology but a new way of delivering computing resources [7]. Cloud providers are offering on-demand computing services which could reduce IT cost and increase capabilities for cloud customers. According to European Network and Information Security Agency (ENISA) [7] some of the top benefits are:

- Cloud resources like storage, CPU time, memory, can be rapidly scaled to respond to sudden peaks in demand.
- Security and the benefits of scale which means that cloud-based countermeasures, when implemented on a large scale, can be more robust and cost-effective compared to in-house computing. Cloud provider can also afford to hire security specialist dealing with specific security threats and have the economic resources to use multiple locations.
- Massive concentration of resources and data is a danger as it could attract attackers but there are also some benefits with resource concentration. It is easier and cheaper for cloud providers to control such things as patch management, incident management, and maintenance processes etc.

2.5 Cloud Computing Risks

However there are also some risks. D Vohradsky [9] has made a ranking comparison of top risks identified by different organizations like Cloud Security Alliance (SCA), Open Web Application Security Project (OWASP), and European Network and Information Security Agency (ENISA). Some of the most important top security risks are:

- Loss of governance as it is necessarily to leave some controls to the cloud provider on issues which may affect security. Service Level Agreement (SLA) for example may prohibit the cloud customers to use some controls like penetration testing thus leaving a gap in the cloud customers’ security defenses.
- Lock-in varies according to the cloud service models (SaaS, etc.) but in all case means that it is difficult for a cloud customer to mitigate to another cloud provider or back to an in-house IT environment.
- Isolation failures like failure to separating storage, memory, etc. between different cloud customers and insecure or incomplete data deletion.
- Compliance risks meaning problems for cloud customers in achieving certification e.g. to meet regulatory requirements. That could depend on the fact that the cloud provider cannot provide evidence of his own compliance or that the cloud provider does not permit audit by the cloud customers.
- Malicious insider at the cloud provider who could cause damages which is often far greater compared to in-house computing as it could affects a number of other cloud customers.

3 APPROACH

3.1 Combination of ISO and NIST framework

First we combined the ISO and NIST framework. After the first initial IT Security Risk Assessment and Risk Treatment which act as a base for the organization we believe that IT Security Risk Management exists at each organizational level. The first initial Risk Assessment / Risk Treatment is a collaboration between Tier 2 which have the knowledge what impact different threat will have and Tier 3 which have
knowledge of different threats to the IT environment. The Risk Assessment / Risk Treatment are governed by Tier 1 perception of risk tolerance and the risk culture of the organization.

**Figure 3:** Combination of ISO and NIST framework.

The framework for each organizational level all consist of the three basic steps.

- Evaluate the new incident with IT Security Risk Assessment of some kind.
- In some cases mitigate the new risk (IT Security Risk Treatment) with help of new countermeasures or in some cases just accept the new risk.
- Use IT Security Risk Communication of the new risk to other organizational levels if necessary.

Operational level (Tier three) handles a lot of incidents. Examples are surveillance of IT systems, servers, and networks. Other examples are end users error reports etc. Incidents at next level, Middle Management level (Tier two), are such thing that could influence the business processes that Middle Management is responsible for. At Top Management level (Tier one) incident that concern the core mission of the organization and incident that might affect risk tolerance. Example of communication from the top level to lower levels is policy document of different kind.

An important aspect is the difference in authority, competence and responsibility on the different organizational levels. The different level use different terms and concepts depending on their authority, IT competence and responsibility. The top management has for example high authority but sometimes lack the IT competence and language to communicate with individuals in IT operations.

### 3.2 IT Security Risk Monitoring

To maintain an acceptable IT security risk level IT Security Risk Monitoring need to be an ongoing process. NIST Special Publication 800-137 page vi [10] define Information Security Continuous Monitoring (CM) as “maintaining ongoing awareness of information security, vulnerabilities, and threats to support organizational risk management decisions”. According to NIST Interagency Report 7756 [11], the data sources for CM include people, process, technology, and environment. Many CM implementations focus on technology as it is easy to automate data collection. The people, process, and environment data sources could not always have fully automated data collection and will in most cases require some human data collection effort.

A number of Data Collection methods can be used to collect data. Examples are Surveys, Standards Based Methods and Tools, as well as Sensors of different kind. The methods could be both automated and manual. Data collection could be truly
continual (always on) or continuous (collected periodically at some set interval). Figure 5 describe combination of data sources and data collection methods.

![Diagram of data sources and data collection methods]

**Figure 4: IT Security Risk Monitoring.**

The frequency of risk monitoring (automated or manual) depends among other things changes in organizations information system, the potential impact of risks and the degree the threat space is changing. The frequency could also be affected if automated or manual monitoring is used. By using automation it is possible to monitor a greater number of security metrics although it is not possible to fully automate all metrics, some metrics still need human analysis. NIST [10] describe eleven security automation domains that support continuous monitoring. Examples of such domain are Vulnerability management, Assets management, Network management, Information management, Configuration management, and Event management.

### 3.3 IT Security Metrics

IT Security Risk Monitoring use Security Metrics of different kind. According to Brotby [12] metrics is a term used to indicate a measure based on a reference and involves at least two points, the measure and the reference. There is some difference between monitoring and metrics but both serve the same purpose of providing information. In this paper we use monitoring as simply paying attention to the information supplied by metrics.

![Diagram of handling incident with help of security metrics]

**Figure 5: Handling of incident with help of security metrics.**

Security metrics can be categorized by what they measure like Performance, Outcomes, Trends, and Probabilities. How these things are measured can be further categorized by the methods used to measure them. Methods can include Maturity, Benchmarking, and Statistical analysis. Security metrics may also be classified according to how they are measured for example Quality, Throughput, Frequency, and Magnitude. Brotby [12] propose a taxonomy that defines 10 fundamental characteristics of metrics, including the following categories:

- **Objective/Subjective**
- **Quantitative/Qualitative**
- **Static/Dynamic**
- **Absolute/Relative**
- **Direct/Indirect**

Some of the questions one need to ask when handling possible incident are:

- Is it actually an incident?
- Is it a security incident?
- Are there multiple events and impacts?
- What immediate actions must be taken?
- Who must be notified?
- Is it becoming a disaster?

3.4 IT Security Risk Escalation

When handling incidents of different kind, each level has to consider if the incident would harm the acceptable risk level of the organization. Each level has basically three alternatives; you can accept the risk, you can try to mitigate the risk (risk treatment), or you can escalate the risk to the organizational level above. Reasons to escalate could for example be budgetary considerations to implement new countermeasures, or that the incident is so serious that help from a higher level is needed. One alternative for Top Management is to externalize the IT risk using insurance.

An incident is an event that has a human root cause. All incidents are events but many events are not incidents. However in this paper we will consistently make use of the term incident. An incident is an observable change to the normal behavior of a system. A normal incident does not affect critical components and to not require participation of senior personnel.

Incidents are often handled by a Help Desk which may filter incidents before some incidents are sent to The First Responder who performs the preliminary analysis. In some cases senior technical resources are assigned to resolve an incident.

An escalated incident on the other hand affects critical production system and normally need participation of senior personnel. An emergency incident needs to be handle by an Emergency Response team. Escalation process can either be Technical or Management.

3.5 IT Security Risk Escalation Maturity Model

According to Philips page 3 [13] a Capability Maturity Mode is “a model for judging the maturity of the processes of an organization and for identifying the key practices that are required to increase the maturity of these processes”. We present a first draft to an IT Security Risk Escalation Capability Maturity Model. We will use ISACA’s Risk IT Framework [14] as a starting point when we defined our model and will use the following maturity levels:

0. Non-existent when processes are not applied at all.
1. Initial when processes are performed ad hoc and disorganized.
2. Repeatable when processes follow a regular pattern.
3. Defined when processes are documented and communicated
4. Managed when processes are monitored and measured.
5. Optimized good practices are followed and automated.

Our model is built around the following attributes:
- Awareness and communication.
- Responsibility and accountability.
• Goal setting and measurement.
• Policies, standards and procedures.
• Skills and expertise.
• Tools and automation.

Escalation can be of both technical and management type which will affect some of the attributes as both need be fulfilled to reach the maturity level. Our maturity model is presented in Appendix (Table 2 and 3).

The maturity model could be used to identify both where the organization is today and as a target for improvement. In the next section we will use our approach in a cloud computing environment to identify the minimum maturity level and which attributes that are most important.

4 THE NEW APPROACH APPLIED TO CLOUD COMPUTING

4.1 Characteristics of Cloud Computing

According to NIST [15] cloud computing is composed of five essential characteristics, three service models, and four deployment models. Essential characteristics of cloud computing are:

• **On-demand self-service.** A cloud customer can when needed automatically use computing capabilities, like server time and network storage without requiring human interaction by the service provider.
• **Broad network access.** Computer resources are available over the network and accessed through standard mechanisms like mobile phones, tablets, laptops, and workstations.
• **Resource pooling.** The provider’s computing resources (e.g. storage, processing, memory, and network bandwidth) are dynamically assigned and reassigned according to consumer demand. The customer generally has no control or knowledge over the exact location of the provided resources.
• **Rapid elasticity.** Cloud customers can scale up and down the usage of computer resources in some cases automatically when required and can be purchased in any quantity at any time.
• **Measured service.** Cloud resource usage (e.g., storage, processing, bandwidth, and active user accounts) can be monitored, controlled, and reported. Both the cloud provider and customer can use information of the utilized service.

4.2 Cloud Computing Service Models

Three different kinds of Service Models are used:

• **Software as a Service (SaaS)** meaning that the cloud provider delivers software application as a service (like web-based mail) to the cloud customer. The cloud customers do not need to invest in software license and servers and the cloud providers are able to use the economics of scale as the service can be used by a number of different cloud customers.
• **Platform as a Service (PaaS)** meaning that the cloud provider delivers service that the cloud customer could use to build own application like.
• **Infrastructure as a Service (IaaS)** meaning that the cloud provider delivers processing, storage, networks, and other fundamental computing resources to the cloud customers who can use this to deploy and run own developed or bought software.

4.3 Cloud Computing Deployment Models

There are also different Deployment Models for the cloud infrastructure:
• **Private cloud.** The cloud infrastructure is used by a single organization that consists of multiple customers (e.g., business units). Private cloud may be owned, managed, and operated by the organization, a third party, or some combination of them, and it may exist on or off premises. The advantages are among other things complete control of data. The main disadvantages are huge investment and maintenance costs.

• **Community cloud.** The cloud infrastructure is used by a specific community of customers from organizations that have shared concerns (e.g., mission, security requirements, policy, and compliance considerations). Community cloud may be owned, managed, and operated by one or more of the organizations in the community, a third party, or some combination of them, and it may exist on or off premises. The advantages are among other things better control of data. The main disadvantages are investment and maintenance costs.

• **Public cloud.** The cloud infrastructure is used by the general public. Public cloud may be owned, managed, and operated by a business, academic, or government organization, or some combination of them. It exists on the premises of the cloud provider. The main advantages are that services could be used by pay-per-usage schemes and no initial investments for hardware and software are needed. Disadvantages are among other things the risk of not having complete control of data.

• **Hybrid cloud.** The cloud infrastructure is a mixture of two or more distinct cloud infrastructures (private, community, or public) that remain unique entities, but are bound together by standardized or proprietary technology that enables data and application portability. The advantages are that hybrid clouds are more flexible than both public and private clouds but the disadvantage is to determine what services that should be used for public and/or private clouds.

![Figure 7: The NIST Cloud Visual Models [16.]](image)

### 4.4 Cloud Computing and Traditional Outsourcing

There is some difference between cloud computing and traditional outsourcing. According to Annamalai [16] the advantages are lower investment in hardware infrastructure and lower operating cost. Elasticity and scalability could be done on demand and quick procurement of services is easy. The disadvantages are poorer legal and data proximity compliance and the cloud customers do not hold entire control of data. There are also some differences in the degree of control an organization have when using Cloud Computing, Traditional Outsourcing, or In-House Computing which is illustrated in the figure below.

![Figure 8: Degree of control.](image)
However the degree of control also differs depending on what kind of deployment model that are used. For example using a private cloud could in some sense be compared to In-House Computing.

Table 1: Degree of control and Deployment Model

<table>
<thead>
<tr>
<th>Deployment Model</th>
<th>Software as a Service</th>
<th>Platform as a Service</th>
<th>Infrastructure as a Service</th>
</tr>
</thead>
<tbody>
<tr>
<td>Private cloud</td>
<td>High</td>
<td>High</td>
<td>High</td>
</tr>
<tr>
<td>Community cloud</td>
<td>Medium</td>
<td>Medium</td>
<td>Medium</td>
</tr>
<tr>
<td>Public cloud</td>
<td>Low</td>
<td>Low</td>
<td>Low</td>
</tr>
<tr>
<td>Hybrid cloud</td>
<td>Medium</td>
<td>Medium</td>
<td>Medium</td>
</tr>
</tbody>
</table>

4.5 Monitoring in a Cloud Computing Environment

Characteristics of cloud computing (and other third party services) are that most of the monitoring needs to be done by the cloud provider but it still up to the organization to judge the risk.

Cloud services offered by the cloud provider are defined in a service level agreement (SLA). Example of important questions to be asked concerning monitoring according to ENISA [4] are:

- **Service availability.** Which functions should be covered by availability monitoring? How to define when a system is unavailable and how availability is measured (e.g. by user reports, sample requests etc.)?
- **Incident response.** What is the definition of minimum response times and what kind of severity classification of different incidents exist? What incident management capabilities are in place?
- **Service elasticity and load tolerance.** For which resources should elasticity be monitored and what kind of elasticity tests (e.g. burst tests) should be used?
- **Data life-cycle management.** What kind of back-up operations will be used and in what way are back-ups tested?
- **Technical compliance and vulnerability management.** How are technical compliance defined? What kind of software updates and handling of patches will be applied? What are the procedures for vulnerability discovery and reporting?
- **Change management.** How is change management defined? What will happen if critical changes to system configuration take place if this for example will result in loss of certification status (e.g. ISO)?
- **Data isolation.** How are data isolation tested when data exist memory or at rest? How is secure deletion done? Could data isolation be tested independently?
- **Log management and forensics.** How are log management and forensics defined? What metrics are in place? Are logs tested frequently for availability?

4.6 Escalation Maturity Model applied to Cloud Computing

Compared to traditional outsourcing cloud computing are even more complex as resources are shared between customers and can be rapidly changed. This means that incident reporting in a fast way are even more important and ccommunication
between organizational levels must work probably, especially escalation routines. In this part we will use the escalation maturity model to point out which parameters that is most important in a cloud computing environment. Of course, all organizations should strive to reach the highest maturity level. However in a cloud computing environment where most monitoring result are delivered by the cloud provider the minimum escalation maturity level for an organization should at least be the third level (Defined). The most important attributes are:

- Responsibilities and Accountability.
- Policies, Standards, and Procedures.

5 CONCLUSIONS AND FUTURE RESEARCH

There are profits to be found in the cloud and there is no need to reinvent the wheel for risk management but there is a needed to review and develop risk communication (escalation) and risk monitoring process at all levels in the organization when moving into the cloud.

One contribution of our work is that IT Security Risk Management can be better adapted to the current situation. The maturity escalation model could be for example be used by organizations to understand where shortcomings exist and act as a goal for where they should be.

We will use the same methods as Karokola [17] so the next step is a desktop analysis of our approach on different organizations using various scenarios. For each organization a number of people representing the different organizational levels (strategic, tactical, and operational) will be asked for their ratings of some dimensions. A scale with percentage will be used. Examples of dimensions are:

- Simplicity
- Coverage and completeness
- Flexibility
- Relevance
- Usefulness

6 REFERENCES


APPENDIX: IT Security Risk Escalation Capability Maturity Model

**Table 2: IT Security Risk Escalation Capability Maturity Model part 1**

<table>
<thead>
<tr>
<th>Level</th>
<th>Awareness and Communication</th>
<th>Responsibility and Accountability</th>
<th>Goal Setting and Measurement</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Non-existent</strong></td>
<td>Does not recognize the need.</td>
<td>No support for individual responsibility and minimal accountability</td>
<td>Minimal reporting to management.</td>
</tr>
<tr>
<td><strong>Initial</strong></td>
<td>Minimal individual awareness of threats.</td>
<td>Roles only partially defined and contain overlaps. Confusion about responsibilities and a culture of blame tends to exist.</td>
<td>Regular manual reporting to local management.</td>
</tr>
<tr>
<td><strong>Repeatable</strong></td>
<td>Individual awareness of threats.</td>
<td>General understanding and individual awareness of business impacting threats.</td>
<td>Regular reporting to management.</td>
</tr>
<tr>
<td><strong>Defined</strong></td>
<td>Both technical and management roles are clearly defined and job description includes risk response responsibilities. Both technical and management responsibility and accountability are defined.</td>
<td>Both technical and management responsibility and accountability are accepted. A reward culture is in place that motivates positive action.</td>
<td>Regular reporting to business management.</td>
</tr>
<tr>
<td><strong>Managed</strong></td>
<td>Individual understanding and awareness of requirements for responding to risk.</td>
<td>The organization is well aware of requirements for responding to risk.</td>
<td>Reporting includes measure of effectiveness.</td>
</tr>
<tr>
<td><strong>Optimized</strong></td>
<td>The organization is well aware of requirements for responding to risk.</td>
<td>Employees at every level take direct responsibility and the organization collaborates with external entities.</td>
<td></td>
</tr>
</tbody>
</table>

**Table 3: IT Security Risk Escalation Capability Maturity Model part 2**

<table>
<thead>
<tr>
<th>Level</th>
<th>Policies, Standards and Procedures</th>
<th>Skills and expertise</th>
<th>Tools and automation</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Non-existent</strong></td>
<td>Does not recognize the need.</td>
<td>Skills requirements exist on an ad hoc basis but are not actively developed. IT personnel lack skills to determine the business relevance and may force the organization to accept risk beyond tolerance level.</td>
<td>No workflow around incidents exists.</td>
</tr>
<tr>
<td><strong>Initial</strong></td>
<td>Minimal standards and procedures exist but are not kept up to date.</td>
<td>Minimum skill requirement are identified and some training is provided but is only provided in response of a need and occurs on the job.</td>
<td>Tools may exist but there is no coordinated approach.</td>
</tr>
<tr>
<td><strong>Repeatable</strong></td>
<td>Policies and standards are established.</td>
<td>Both technical and management policies and standards are defined and documented.</td>
<td>Workflow tools are used to escalate incidents.</td>
</tr>
<tr>
<td><strong>Defined</strong></td>
<td>Both technical and management policies and standards are defined and documented.</td>
<td>Both technical and management skills requirements are defined and documented and a formal training plan has been developed.</td>
<td>Automation of workflow tools.</td>
</tr>
<tr>
<td><strong>Managed</strong></td>
<td>Both technical and management policies and standards reflect business risk tolerance.</td>
<td>Both technical and management skill requirements are routinely updated and the effectiveness of the training plan is evaluated.</td>
<td></td>
</tr>
<tr>
<td><strong>Optimized</strong></td>
<td>Both technical and management policies and standards are dynamically updated.</td>
<td>Continuous improvement of both technical and management skill requirements and training.</td>
<td>Real-time monitoring of risk incidents.</td>
</tr>
</tbody>
</table>