MEHARI 2010

Überblick

Juli 2010

Arbeitsgruppe für Methoden

Für Fragen und Bemerkungen gehen Sie bitte zum Internetforum:
http://mehari.info/

CLUB DE LA SECURITE DE L'INFORMATION FRANÇAIS

11 rue de Mogador, 75009 PARIS
Tel.: +33 1 53 25 08 80 – Fax: +33 1 53 25 08 88 – e-mail: clusif@clusif.asso.fr
Web: http://www.clusif.asso.fr

Danksagung

CLUSIF möchte sich speziell bei Jean-Philippe Jouas für seinen außerordentlichen Beitrag, der Arbeitsgruppe für Methoden die an der Realisierung dieses Dokumentes mitgewirkt hat und Herrn Christian S. Fötinger (Safetybelt Consulting e. U.) für die Übersetzung bedanken.

Inhaltsverzeichnis

1. Einführung

MEHARI wurde ursprünglich entwickelt (und wird laufend geändert) um dem Chief Information Security Officer (CISO) bei seinen Aufgaben im Informationssicherheits-management zu unterstützen.

Dieser Überblick ist prinzipiell für CISOs gedacht, ist aber genauso für Auditoren, CIOs oder Risikomanager, die weitgehend denselben oder ähnlichen Herausforderungen gegenüberstehen, bestimmt.

Das Hauptziel dieses Dokumentes ist die Verwendung von MEHARI zu erklären. Eine detaillierte Beschreibung der Methodologie und entsprechende Werkzeuge werden mit anderen, bei CLUSIF erhältlichen Dokumenten, zur Verfügung gestellt.

MEHARI primäres Ziel ist es eine Methode und Werkzeuge für den Einsatz einer Risikoerfassung und eines Risikomanagements, speziell für den Bereich Informationssicherheit, gemäß der ISO/IEC 27005:2008 Anforderungen, zur Verfügung zu stellen[1].

Zusätzliche Ziele sind:

- Die Möglichkeit eine direkte und individuelle Analyse von Risikosituationen vorgegebener Szenarien zu erstellen.
- Fertige Werkzeuge, die speziell für kurz-, mittel- und langfristiges Sicherheitsmanagement entwickelt wurden und an verschiedene Reifegrade und betrachtete Maßnahmen angepasst werden können, zur Verfügung zu stellen.

Tatsächlich stellt MEHARI eine konsistente Methode, mit angemessenen Wissensdatenbanken zur Verfügung, um CISOs, Geschäftsführer und Sicherheitsmanager, oder andere Personen, die sich mit Risikominderung befassen, bei ihren verschiedenen Aufgaben zu unterstützen.

Die Beziehung zwischen ISO/IEC 27000 und MEHARI wird am Ende des Dokumentes beschrieben.

[1] Die Werkzeuge und zugehörigen Mittel, die von MEHARI zusätzlich zum Standard angeboten werden, sind im Dokument *‚MEHARI – Konzepte und funktionale Spezifikationen‘* beschrieben und erklärt.

2. Einsatz von MEHARI

MEHARI ist vor allem eine Methode zur Risikoanalyse und zum Risikomanagement.

In der Praxis heißt das, dass MEHARI und seine zugehörigen Wissensdatenbanken zur genauen Risikoanalyse von in Szenarien beschriebenen Risikosituationen, entwickelt wurden.

Im täglichen Leben, ist Sicherheitsmanagement eine Funktion oder Aktivität, die sich mit der Zeit entwickeln muss. Korrektive Managementmaßnahmen sind, abhängig davon, ob die Organisation in diesem Bereich noch nichts unternommen hat oder – im Gegensatz – substantielle Investitionen in Zeit und Aufwand getätigt hat, unterschiedlich.

Bei den ersten Schritten im Bereich der Sicherheit ist es ohne Zweifel ratsam, den Stand und die aktuellen Sicherheitsmaßnahmen und –policies der Organisation zu berücksichtigen und diese gegen ‚best practices' zu messen, um zu klären welche Lücke es zu schließen gilt.

Anschließend an diese Bestandsaufnahme und der Entscheidung eine Sicherheitsorganisation zu etablieren, müssen konkrete Maßnahmen beschlossen werden. Solche Entscheidungen, die normalerweise in Plänen, Unternehmensregeln, Policies oder einem Sicherheitsregelwerk zusammengefasst werden, sollten mittels einer strukturierten Herangehensweise getroffen werden. Diese kann auf einer Risikoanalyse, wie sie von ISO/IEC 27001 als Teil eines ISMS (Information Security Management System) gefordert wird, basieren. Es gibt auch andere Möglichkeiten, wie interne, externe (professionelle) oder gemischte Vergleiche.

An diesem Punkt ist es richtig, ohne speziell die Risikoanalyse zu nennen, die Frage nach den Einflussfaktoren, die sich auf die Sicherheit auswirken, zu stellen.

Wie auch immer die Entscheidung getroffen wurde, wird sehr oft die Person, die die letzte Entscheidung für die Aufbringung des notwendigen Budgets hat, fragen, ‚Ist das wirklich notwendig?'. Aufgrund mangelnd vorbereitender Bestandsaufnahmen von – und einer generellen Zustimmung zu – den Einflussfaktoren, werden viele Sicherheitsprojekte abgelehnt oder verzögert.

Oft später, aber manchmal bereits am Beginn der Auseinandersetzung mit Sicherheit, wird nach dem tatsächlichen Risiko, dem das Unternehmen ausgesetzt ist, gefragt. Dies geschieht meist mit ähnlichen Sätzen, wie: „Sind alle Risiken denen das Unternehmen ausgesetzt ist, identifiziert worden, und gibt es eine Garantie, das die Restrisiken akzeptabel sind?" Diese Frage könnte genauso leicht unternehmensweit oder in Bezug zu einem einzelnen Projekt gestellt werden. Es wird dafür eine Methode benötigt, die eine Risikoanalyse beinhaltet.

MEHARI begründet sich auf dem Prinzip, dass die, für die jeweiligen Stufen der Sicherheitsentwicklung, notwendigen Werkzeuge konsistent sein müssen. Daher kann davon ausgegangen werden, dass jedes Ergebnis, das in einer Stufe erzielt wurde, von anderen Werkzeugen später in einer anderen Ebene oder sonst wo in der Organisation wieder verwendet werden kann.

Die verschiedenen Werkzeuge und Module von MEHARI, die eine direkte und individuelle Risikoanalyse begleiten, können, da sie verschiedene Managementziele ansprechen und konsistente Ergebnisse der Entscheidungen garantieren, getrennt voneinander, in jeder Stufe der Sicherheitsentwicklung, verwendet werden.

Diese Werkzeuge und Module – im Folgenden kurz beschrieben – umfassen eine konsistente Risikoerfassungsmethode mit notwendigen unterstützenden Werkzeugen und Modulen zur Analyse der Einflussfaktoren und der Überprüfung (Audit) der Qualität von Sicherheitsmaßnahmen, etc.

1.1 Risikoanalyse und -erhebung

In nahezu jeder Publikation über Sicherheit und ebenso in den ISO/IEC Standards wird die Risikoanalyse als der Treiber beschrieben um Sicherheitsanforderungen auszudrücken. Jedoch, verabsäumen die meisten die Erklärung welche Methoden angewendet werden sollen.

Seit über 15 Jahren hat MEHARI einen strukturierten Ansatz für Risikoevaluierung[2] zur Verfügung gestellt, der sich auf einfachen Prinzipien begründet.

Eine Risikosituation kann von verschiedenen Faktoren charakterisiert werden:

- Strukturelle (oder organisatorische) Faktoren, die nicht von Sicherheitsmaßnahmen abhängen, aber von den Kernprozessen der Organisation, ihrer Umgebung und ihren Zusammenhängen.
- Risikominimierende Faktoren, die direkt auf eingesetzte Sicherheitsmaßnahmen wirken.

Tatsächlich wird die Bedrohungsanalyse dazu verwendet um das maximale Niveau der Folgen einer Risikosituation festzustellen. Das ist typischerweise ein struktureller Faktor, während die Bestandsaufnahme dazu verwendet wird risikominimierende Faktoren zu bewerten.

MEHARI ermöglicht eine qualitative und quantitative Bewertung dieser Faktoren und unterstützt als Ergebnis bei der Beurteilung der Risikoniveaus. Dabei integriert MEHARI Werkzeuge (wie Erhebungskriterien, Formeln, etc.) und eine Wissensdatenbank (im speziellen zur Diagnose von Sicherheitsmaßnahmen), die wichtige Ergänzungen zum Minimalrahmen der ISO/IEC 27005 sind.

1.1.1 Systematische Analyse der Risikosituationen

Um die Frage ‚Was sind die spezifischen Risiken der Organisation und sind sie akzeptierbar oder nicht?', zu beantworten benötigt man einen strukturierten Ansatz um alle potentiellen Risikosituationen zu identifizieren, die Kritischsten individuell zu analysieren und anschließend jene Maßnahmen zu erkennen, die das Risiko auf ein annehmbares Niveau reduzieren.

Der Ansatz, der von MEHARI zur Verfügung gestellt wird, basiert auf einer Wissensdatenbank von Risikosituationen und damit verknüpften Prozeduren zur Evaluierung der charakteristischen Faktoren der Risiken und Erhebung des Niveaus. Zusätzlich bietet die Methode Hilfestellung bei der Auswahl eines entsprechenden Risikobearbeitungsplans.

[2] Eine detaillierte Beschreibung des Risikomodells von MEHARI finden Sie in „*MEHARI General Concepts and Principal Mechanisms*", auf der Webseite von CLUSIF (http://www.clusif.asso.fr).

Für die Risikoerhebung werden 2 Hauptoptionen vorgeschlagen:

- Entweder die Verwendung des Funktionssets der Wissensdatenbank (für MS Excel oder Open Office), die es erlauben die Ergebnisse der MEHARI Module (z. B. Klassifizierung der Assets aus der Umfeldanalyse, Sicherheitsdiagnose) zu integrieren. Aus diesen Funktionen ist es möglich den aktuellen Risikowert zu erheben und zusätzliche Maßnahmen zur Reduktion vorzuschlagen.
- Oder die Anwendung einer Applikation (wie RISICARE[3]) die eine erweiterte Benutzeroberfläche bietet und Simulationen und Visualisierungen zur weiteren Optimierung erlaubt.

1.1.2 Spontananalyse von Risikosituationen

Dieselben Tools können, zu jedem Zeitpunkt in anderen Sicherheitsmanagementansätzen, verwendet werden.

In einigen Sicherheitsüberwachungsmodi, wenn Risikomanagement nicht das Hauptziel ist und Sicherheit mittels Audits oder Sicherheitsregelwerken geleitet wird, kann es immer Fälle geben, in denen die Regeln nicht angewendet werden können. Eine spontane Risikoanalyse kann helfen die weitere Vorgehensweise zu bestimmen.

1.1.3 Risikoanalyse in neuen Projekten

Das Risikoanalysemodell und der Mechanismus können im Projektmanagement, zur Planung gegen Risiken und für Entscheidungen welche Messgrößen als Ergebnis verwendet werden, eingesetzt werden.

1.2 Risikoerhebung

MEHARI beinhaltet tiefgehende Fragen zu Diagnose von etablierten Sicherheitskontrollen, die es erlauben die Qualität der Mechanismen und Lösungen zur Risikominderung[4] festzustellen.

1.2.1 Die Verwundbarkeitsüberprüfung, ein Element der Risikoanalyse

MEHARI stellt ein strukturiertes Risikomodell welches „Risiko minimierende Faktoren“ im Rahmen der Sicherheitsmaßnahmen berücksichtigt.

Die sich ergebende Schwachstellenerhebung wird deshalb ein wichtiger Beitrag für die Risikoanalyse sein um sicherzustellen, dass das Sicherheitsservice seine Rolle erfüllt – was ein wesentlicher Punkt für die Glaubwürdigkeit und Zuverlässigkeit der Risikoanalyse ist.

Eine große Stärke von MEHARI ist die Möglichkeit das aktuelle Risikoniveau und zukünftige Niveaus basieren auf einer Wissensdatenbank, welche die Qualität der operativen oder geplanten Sicherheitsmaßnahmen bewertet, zu erheben.

1.2.2 Sicherheitspläne basierend auf der Verwundbarkeitsüberprüfung

Ein möglicher Ansatz ist es, Aktionspläne direkt aus der Statusanalyse der Sicherheitsservices zu erstellen.

Der Sicherheitsmanagementprozess der diesem Ansatz folgt ist sehr einfach: Führe eine Bestandsaufnahme durch und entscheide danach alle jene Bereiche zu verbessern die nicht die entsprechende Qualität liefern.

[3] Von BUC S.A Softwareentwickler

[4] Sicherheitskontrollen oder –maßnahmen sind in Detailmaßnahmen, Maßnahmen/Services und Domänen gruppiert

Zu diesem Zweck können die MEHARI Fragenkataloge verwendet werden.

Eine vorläufige Analyse welche geschäftlichen Einflussfaktoren ebenso betrachtet werden und stellte eine Verbindung zu dem entsprechenden Modul von MEHARI her. Die Umfeldanalyse erlaubt es die benötige Qualität der relevanten Sicherheitsmaßnahmen festzulegen und in Konsequenz andere Teile der Erhebung zu ignorieren.

1.2.3 Unterstützung durch die Wissensdatenbank bei der Erstellung eines "Security Reference Framework"

MEHARIs einzigartige Wissensdatenbank kann dazu verwendet werden, um sofort ein Rahmenwerk für die Sicherheit (oder eine Sicherheitspolicy) zu erstellen, die einen Regelsatz und Anleitungen enthält und beschreibt, denen das Unternehmen oder die Organisation folgen kann.

Dieser Ansatz wird oft in Organisationen oder Unternehmen, mit vielen unabhängigen operationellen Einheiten oder Niederlassungen, verwendet. Das sind typischerweise große multinationale Firmen mit vielen Zweigstellen. Es ist genauso aber anwendbar in mittleren Unternehmen mit einer großen Zahl von regionalen Außenstellen oder Agenturen. In diesen Fällen ist es schwer, unzählige Bestandsaufnahmen oder Risikoanalysen durchzuführen.

Erstellung eines Sicherheitsregelwerkes

MEHARIs Fragebögen zur Bestandsaufnahme sind eine gute Arbeitsgrundlage für Sicherheitsmanager um zu entscheiden, was in ihren Organisationen umgesetzt werden soll.

Managen der Ausnahmen von der Regel

Die Erzeugung eines Regelsatzes, mittels eines Sicherheitsregelwerkes, geht oft mit Schwierigkeiten bei der lokalen Implementierung einher. So müssen Ausnahmen und Verzicht auf die Regeln behandelt werden. Unter Verwendung einer zusammenhängenden Wissensdatenbank mit konsistenten Werkzeugen und einer analytischen Methodologie, wird es ermöglicht lokale Abweichungen zu verwalten. Anforderungen für Ausnahmen werden mit einer spezifischen Risikoanalyse der erkannten Schwierigkeiten, betrachtet.

1.2.4 Bereiche des Schwachstellenerfassungsmoduls

Aus dem Blickwinkel der Risikoanalyse, um Risiken zu identifizieren, und dem Wunsch alle nicht annehmbaren Risiken abzudecken, ist MEHARI nicht nur auf die IT-Domäne beschränkt.

Das Bestandsaufnahmemodul deckt, fern des Informationssystems, die gesamte Organisation und den Zutrittsschutz im Allgemeinen, genauso ab, wie das Arbeitsumfeld sowie rechtliche und regulierende Gesichtspunkte.

1.2.5 Überblick über das Erfassungsmodul

Ein Punkt dieser Schwachstellenerfassung muss festgehalten werden: Es stellt einen breiten und konsistenten Blick auf die Sicherheit zur Verfügung. Dies kann für vielerlei Ansätze verwendet werden, evolutionär in der Tiefe und der Feinheit der Analyse und während aller Stufen der Reifegradentwicklung einer unternehmensweiten Sicherheitsorganisation und -sensibilisierung.

1.3 Bedrohungsanalyse (Einflussfaktoren)

Sicherheit dient dem Schutz von Vermögenswerten. Welche Orientierung die Sicherheitspolicy auch hat, es gibt ein Prinzip dem alle Manager zustimmen; es muss eine Balance zwischen den Sicherheitsinvestitionen und der Bedeutung relevanter Geschäftseinflüsse geben.

Das bedeutet, dass richtiges Verständnis für Geschäftseinflüsse grundsätzlich vorhanden ist und die Analyse dieser Sicherheitsbedrohungen eine hohe Priorität und eine strikte und strukturierte Erhebungsmethode verlangt.

Das Ziel dieser Analyse ist es zwei Fragen zu beantworten:

"Was kann passieren, und wenn es passiert, wird es ernst sein?"

Dies zeigt, dass im Bereich der Sicherheit, Bedrohungen als Ergebnis von Ereignissen gesehen werden, die die zu erwartende Geschäftstätigkeiten eines Unternehmens oder einer Organisation stören.

MEHARI stellt ein Analysemodul für Einflussfaktoren zur Verfügung (beschrieben in *Analyse der Einflussfaktoren und Klassifizierung*), das zwei Arten von Ergebnissen erzeugt:

- eine Bewertungsskala von Störungen
- eine Klassifizierung von Informationen und IT Ressourcen

Die Bewertungsskala von Störungen
Die Identifikation von Störungen oder potentiellen Ereignissen ist ein Prozess, der mit der Aktivität des Unternehmens beginnt und besteht aus der Identifizierung möglicher Störungen in operationellen Prozessen. Dies führt zu:

- Einer Beschreibung von Typen möglicher Störungen
- Einer Definition der Parameter, die die Auswirkung jeder Störung beeinflussen
- Einer Bewertung von kritischen Schwellwerten dieser Parameter, die das Niveau der Auswirkung der Störung beeinflussen

Diese Ergebnisse machen die Bewertungsskala von Störungen aus.

Klassifizierung von Informationen und Ressourcen
Es ist normal, in der IT-Sicherheit, von der Klassifizierung von Informationen und IT-Ressourcen zu sprechen.

So eine Klassifizierung besteht daraus, für jeden Typ von Informationen, jede IT-Ressource und jedes Klassifizierungskriterium (Klassisch: Verfügbarkeit, Integrität und Vertraulichkeit, auch andere Kriterien wie Nachvollziehbarkeit können verwendet werden), typische Indikatoren dafür zu finden, welche Auswirkung für die Information oder Ressource besteht, wenn das Kriterium verletzt wird oder verloren geht.

Die Klassifizierung von Informationen und Ressourcen, bei Informationssystemen, ist die, in Sensibilitätsindikatoren in Verbindung mit IT-Ressourcen, übersetzte Bewertungsskala von Störungen.

Aufzeigen von Sicherheitseinflussfaktoren (und Bedrohungen)
Die Bewertungsskala für Störungen und die Klassifizierung von Informationen sind zwei klare Wege zur Hervorhebung von Sicherheitsbedrohungen.

Die Erste ist detaillierter und stellt dem CISO mehr Informationen zur Verfügung. Die Letztere ist allgemeiner und hilfreicher bei Sensibilisierung und Kommunikation, aber weniger granuliert.

1.3.1 Analyse der Einflussfaktoren, die Basis für die Risikoanalyse

Selbstverständlich ist dieses Modul ein Schlüssel in der Risikoanalyse. Ohne ein gemeinsames Übereinkommen über die Konsequenzen von potentiellen Störungen, kann kein Urteil über Risikoniveaus möglich sein.

MEHARI bietet eine rigorose Methode zur Erhebung der Einflussfaktoren und der Asset-Bewertung an, die objektive und rationale Ergebnisse liefern.

1.3.2 Die Analyse der Einflussfaktoren: Eckpfeiler jeder strategischen Aktionsplanung

Zweifelsfrei wird die Analyse der Einflussfaktoren (relevante Personen) sehr oft für jede Form der Implementierung eines Sicherheitsplanes benötigt. Tatsächlich ist es notwendig, gleich welcher Ansatz auch verwendet wird, Ressourcen zu bilden, um die Aktionspläne umzusetzen und zwangläufig wird dabei auch nach der Berechtigung für solche Investitionen gefragt.

Die Ressourcen und Mittel, die der Sicherheit zur Verfügung gestellt werden, stehen, wie für Versicherungspolizzen, in direktem Verhältnis zum Risiko. Gibt es keine Übereinkunft über eine potentielle Störung, wird nur in den seltensten Fällen Budget zur Verfügung gestellt.

1.3.3 Klassifizierung: ein wesentliches Element der Sicherheitspolitik

Sicherheitsregelwerke, Sicherheitspolitiken und damit verbundene Ansätze zum Sicherheitsmanagement wurden bereits in diesem Dokument erwähnt.

In der Praxis sind Unternehmen, die Sicherheit mittels eines Regelwerks verwalten, gezwungen in den Regeln Unterschiede, zwischen den zur Sensibilisierung der verarbeitenden Information auszuführenden Tätigkeiten, zu machen. Es ist normal sich auf eine Klassifizierung von Informationen und IT-Ressourcen zu beziehen.

Die Bedrohungsanalyse von MEHARI stellt ein Mittel zur Verfügung um diese Klassifizierung durchzuführen.

1.3.4 Bedrohungsanalyse: Die Basis der Sicherheitsplanung

Der Prozess der Bedrohungsanalyse, der unzweifelhaft die Beteiligung von operationellen Managern erfordert, führt oft zu sofortigem Handlungsbedarf.

In Interviews mit dem obersten operationellen Management, in dem diese die Sicht und Einschätzung von ernsten Störungen erklärt haben, zeigt die Erfahrung, unabhängig von der Größe des Unternehmens, das dies zu einem Sicherheitsbedarf führt, den diese vorher nicht in Betracht gezogen hatten und der rasche Antworten erfordert.

Es können Aktionspläne, basierend auf einer Kombination von zwei Expertisen, die einen einfachen und direkten Ansatz verwenden, erstellt werden: Jener des Professionisten selbst, zur Verfügung gestellt vom operationellen Management und jener der Sicherheitslösungen, zur Verfügung gestellt von Sicherheitsexperten.

1.4 Allgemeiner Überblick zur Verwendung von MEHARI

Ganz klar, die Hauptausrichtung von MEHARI ist die Risikoerhebung und –minderung. Seine Wissensdatenbank, Mechanismen und Werkzeuge sind für diesen Zweck geschaffen worden.

Ebenso kann, nach Meinung der Entwickler der Methode, der Bedarf für die Verwendung einer strukturierten Methode zur Risikoanalyse und –verminderung, abhängig von der Organisation, sein:

- eine permanente Arbeitsmethode – mit Richtlinien für eine spezialisierte Gruppe,
- eine Arbeitsmethode parallel zu anderen Sicherheitsmanagementpraktiken,
- eine Arbeitsmethode, die gelegentlich verwendet wird um geregelte Praktiken zu ergänzen.

Aus dieser Sicht, stellt MEHARI Ansätze und Tools zur Verfügung die es ermöglichen Risikoanalyse dann durchzuführen, wenn sie benötigt wird.

MEHARI unterstützt Sicherheits- und IT-Verantwortliche (CISOs, Risikomanager, Auditoren, CIOs, etc.) bei Ihren Managementaufgaben und kann über die Internetseite von CLUSIF als ZIP-Datei geladen werden. Diese Datei enthält die Wissensdatenbank und die dazugehörigen Referenzhandbücher.

3. MEHARI UND ISO/IEC 27000 STANDARDS

Eine oft gestellte Frage ist: Wie MEHARI mit anderen internationalen Standards, speziell ISO/IEC 27000, zusammen arbeitet.

Der Anspruch hier ist eine Erklärung wie MEHARI, im Sinne der Kompatibilität und Ziele, sich in den ISO Standards 27001, 27002 und 27005 einfügt.

1.5 Die jeweiligen Ziele von ISO/IEC 27001, 27002, 27005 und MEHARI

1.5.1 Ziele von ISO/IEC 27002:2005

Dieser Standard verlangt von einer Organisation die Identifizierung ihrer Sicherheitsanforderungen aufgrund von drei Hauptquellen:

- Risikoanalyse
- Gesetzliche, regulative, in Statuten verankerte oder vertragliche Anforderungen
- Der Satz von Grundregeln, Zielen und Anforderungen, die auf die Informationsverarbeitung zutreffen, die die Organisation aufgebaut hat, um ihren Betrieb zu unterstützen.

Mit dieser Basis können Kontrollziele, unter Verwendung, der im Kapitel „“code of practice for information security management” aus dem Standard zu findenden Liste oder jedem anderen Satz von Kontrollzielen, gewählt und implementiert werden. (§4.2)

Hinweis: im Bereich von 27002: 2005, wird festgehalten, dass der Standard „Richtlinien und generelle Grundsätze für das Einleiten, das Einführen, das Beibehalten und das Verbessern des Informationssicherheitsmanagements" liefert. Das bedeutet, dass der ISO-Standard als Ausgangspunkt gesehen werden kann. Jedoch fordert ISO/IEC 27001 (§1.2), dass jede Ausnahme gerechtfertigt werden muss und es vertretbar ist Kontrollziele zu setzen. (Appendix A - A.1).

Der ISO 27002 Standard stellt eine Zusammenstellung von Richtlinien zur Verfügung, die von einer Organisation genutzt werden sollen. Er merkt jedoch an, dass die Liste nicht vollständig ist und dass ergänzende Maßnahmen benötigt werden können. Es wird jedoch keine Methodik für die Schaffung eines vollständigen Sicherheitsmanagementsystems empfohlen.

Andererseits beinhaltet jeder Teil der ‚best practices’ Einführungen und Kommentare, die eine große Hilfe, für die zu erreichenden Zielen, sein können.
Hinweis: Der ISO Standard hält in seinem Bereich fest, dass er eingesetzt werden kann um “zu helfen, Vertrauen in die innerorganisatorischen Aktivitäten aufzubauen”. Dies ist nicht zufällig beinhaltet und hebt einen wesentlichen Aspekt hervor, den die Verfechter des Standards fördern: Die Bewertung (sogar Zertifizierung), aus einer Informationssicherheitssicht, von Partnern und Lieferanten.

1.5.2 Ziele von ISO/IEC 27001:2005

Das klare Ziel von ISO/IEC 27001 ist “ein Modell zur Verfügung zu stellen und ein unternehmensweites **Informationssicherheitsmanagementsystem (ISMS)** zu verwalten“, welche „entweder intern oder von Dritten, inklusive Zertifizierungsstellen, verwendet werden“.

Das Bewertungs- und Zertifizierungsziel legt einen starken Fokus auf formale Aspekte (Dokumentation und Aufzeichnung von Entscheidungen, Anwendbarkeitsbescheinigungen,

Aktenvermerke, etc.) und Kontrollen (Überprüfungen, Audits, etc.) und ist sehr stark an der Qualität orientiert.

Es ist klar, dass die Grundlage der Annäherung an Sicherheit eine Risikoanalyse impliziert, um die Risiken zu untersuchen, denen die Organisation ausgesetzt sein kann und angemessene Maßnahmen zu setzen, die die Risiken auf einen annehmbaren Wert verringern.

Der ISO/IEC 27001 Standard gibt vor eine Risikoanalysemethode anzuwenden, diese ist aber nicht Teil des Standards und es gibt keine Vorschläge, außer das PDCA Modell (Plan-Do-Check-Act) zur kontinuierlichen Verbesserung des ISMS einzusetzen.

Auch die Empfehlungen oder ‚best practices' die zur Risikoverringerung verwendet werden können, sind an jenen im ISO/IEC 27002:2005 ausgerichtet, während eine damit verbundene Liste von Kontrollzielen in den Anhängen zur Verfügung gestellt wird.

Entsprechend dem ISO/IEC 27001, ist die Basis **zur Bewertung des Sicherheitsmanagementsystems** nicht so sehr die Kenntnis oder die Überprüfung, ob eine getroffene Entscheidung angemessen und an die Bedürfnisse der Organisation angepasst ist, sondern viel mehr zu prüfen, dass wenn die Entscheidung getroffen wurde, ob das Managementsystem derart ist, dass ein Auditor sicher sein, dass diese Entscheidung tatsächlich umgesetzt ist.

1.5.3 Ziele von ISO/IC 27005:2008

Die Ziele dieses Standards sind nicht eine Risikomanagementmethode zu konstituieren, sondern ein minimales Rahmenwerk festzulegen und Anforderungen für die Risikoerhebung, die Identifizierung der Bedrohungen und Schwachstellen zur Risikoabschätzung und deren Niveau zu beschreiben um danach die Möglichkeit zur Behandlung von abgeleiteten Pläne und Maßnahmen auszuwählen, die auf eine Bewertung und Verbesserung der Situation abzielen.

Der Standard hält fest, dass eine Risikoerhebungsmethode gemäß diesen Anforderungen gewählt werden muss um inkonsistente oder vereinfachte Methoden zu vermeiden, die dem Ziel des Autors dieses Standards widersprechen.

1.5.4 Ziele von MEHARI

MEHARI ist ein konsistenter Satz von Werkzeugen und methodischen Eigenschaften für das Sicherheitsmanagement und verbundenen Bewertungen, die auf einer genauen Risikoanalyse basieren. Die fundamentalen Aspekte von MEHARI:

- sein Risikomodell (qualitativ und quantitativ),
- die Betrachtung der Effizienz etablierter oder geplanter Sicherheitsmaßnahmen,
- die Möglichkeit der Bewertung und Simulation des sich aus zusätzlichen Maßnahmen ergebenden Restrisikos,

sind obligatorische Ergänzungen zu den Anforderungen der ISO/IEC 27000 Standards und im speziellen des ISO/IEC 27005 Standards.

1.5.5 Vergleich der Ziele von MEHARI und den ISO/IEC 27001 und ISO/IEC 27002 Standards

Die Ziele von MEHARI und den zuvor erwähnten ISO Standards sind vollkommen unterschiedlich.

- MEHARI zielt darauf ab, Werkzeuge und Methoden zur Verfügung zu stellen, die am besten geeigneten Sicherheitsmaßnahmen für eine bestimmte Organisation auszuwählen und wenn diese Maßnahmen eingesetzt werden das Restrisiko zu bestimmen.
- Die ISO Standards stellen ‚best practices' zur Verfügung, die natürlich sehr nützlich sind, aber nicht zwingend zu den Bedrohungen der Organisation passen. Sie können sehr gut eingesetzt werden um die Aspekte Reifegrad der Sicherheit, Informationssicherheitsplanung, unabhängige interne Einheiten und externe Partner abzudecken.

Das „**Security services reference manual**" von MEHARI stellt tatsächlich detaillierte Punkte, zur Erstellung eines Sicherheitsregelwerkes, zur Verfügung und kann mit ISO/IEC 27002 verglichen werden. In diesem Punkt ist es klar, dass MEHARI einen breiteren Bereich als die ISO Normen abdeckt. Es deckt wesentliche Aspekte der Sicherheit, als nur die der Informationssysteme, ab.

1.6 Kompatibilität zwischen diesen Ansätzen

Der Ansatz von MEHARI ist mit dem aus ISO/IEC 27002 kompatibel. Da, obwohl sie nicht dieselben Ziele haben, es ziemlich einfach ist die Ergebnisse der Analysen aus MEHARI in ISO/IEC 27002 Indikatoren auszudrücken.

MEHARI gibt die Antwort auf den Bedarf aus beiden ISO 27001 und 27002 Standards, eine Risikoanalyse durchzuführen und einen Maßnahmenkatalog zu erstellen.

1.6.1 Kompatibilität mit ISO/IEC 27002:2005 Standards

Jedoch sind die Kontrollziele oder ‚best practices' von ISO hauptsächlich generelle, Verhaltens- oder organisatorische Maßnahmen, während MEHARI zusätzlich den Bedarf für technische Maßnahmen fordert, deren Effektivität gewährleistet werden kann.

Trotz dieses Unterschiedes stellt die Schwachstellenprüfung von MEHARI Umsetzungstabellen zur Verfügung die es erlauben die Ergebnisse der Kontrollen in ISO 27002:2005 Indikatoren umzuwandeln. Dies ist für jene von Bedeutung, die ihre Übereinstimmung mit dem Standard prüfen müssen.

Es ist hier zu erwähnen, dass die Auditfragen von MEHARI verwendet werden können, um eine effektive Schwachstellenanalyse durchzuführen. Dabei werden die betroffenen Verantwortlichen für den Betrieb einbezogen und die Möglichkeiten jeder Sicherheitsmaßnahme zur Risikominimierung festgelegt.

1.6.2 Kompatibilität mit ISO/IEC 27001 Standard

Es ist leicht MEHARI in den PDCA (Plan-Do-Check-Act) Prozess von ISO/IEC 27001 zu integrieren, speziell in der Phase ‚PLAN' (§4.2.1), da MEHARI vollständig die Taskbeschreibung zur Einführung der Basis eines ISMS abdeckt.

In der der Phase ‚DO' (§4.2.2), welche bestimmt ist um ein ISMS einzuführen und zu verwalten, stellt MEHARI die anfänglichen Elemente zur Verfügung, die gebraucht werden um

die Behandlung von Risiken zu etablieren. Dies ist verbunden mit der Priorisierung und der dazugehörigen Klassifizierung der Risiken und der Entwicklungsindikatoren.

Für die Phase ‚CHECK' (§4.2.3), stellt MEHARI Elemente zur Verfügung, die es erlauben die Restrisiken und eingeführten Verbesserungen bei den Sicherheitsmaßnahmen festzustellen. Jede Änderung des Umfeldes (Einflussfaktoren, Bedrohungen, Lösungen und Organisation), die möglicherweise durch ein Audit festgestellt wurde, kann im Vergleich zum Initialaudit, das mit MEHARI durchgeführt wurde, zu einer Überarbeitung der Sicherheitspläne führen.

Während der Phase ‚ACT (§4.2.4)' ruft MEHARI implizit zur Kontrolle und der kontinuierlichen Verbesserung der Sicherheit auf, um die Ziele der Risikominimierung zu erreichen. In diesen drei Phasen ist MEHARI zwar nicht Herz der Prozesse, trägt aber zu deren Realisierung und Sicherstellung der Effektivität bei.

1.6.3 Kompatibilität mit ISO/IEC 27005:2008 Standard

Der Rahmen der von dem neuen Standard vorgeben wird ist voll auf die Risikoverwaltung gemäß MEHARI anwendbar, z. B.:

- Die Prozesse zur Risikoanalyse, -erhebung und -behandlung (abgeleitet von ISO 13335),
- Die Identifizierung der primären und unterstützenden Vermögenswerte – plus der damit verbundenen Klassifizierung aus der Umfeldanalyse,
- Die Identifizierung der Bedrohungen mit ihrem Niveaus (natürliche Gegebenheiten), die MEHARI in der Beschreibung der Risikoszenarien präzisiert,
- Die Identifizierung und Quantifizierung der Effektivität von Sicherheitsmaßnahmen (oder –kontrollen) bei der Behebung von Schwachstellen,
- Der Kombination dieser Elemente bei der Erhebung des Schweregrades von Risikoszenarien mittels einer 4-stufigen Skala,
- Die Möglichkeit direkt für die Risikominderung benötigte Sicherheitsmaßnahmen auszuwählen.

Deswegen ist MEHARI nicht nur leicht in den ISMS Prozess, wie er von ISO/IEC 27001 vorgegeben wird, zu integrieren sondern stimmt voll mit den Anforderungen des ISO/IEC 27005 für eine Risikomanagementmethode überein.