梅哈里 (MEHARI) 2010

概述

法国信息安全协会

地址： 11, rue de Mogador, 75009 PARIS

电话 : +33 1 53 25 08 80　　传真： Fax: +33 1 53 25 08 88

网址： http://www.clusif.asso.fr

目录

致谢

法国信息安全协会（CLUSIF）特别感谢Jean-Philipe Jouas 先生和MEHARI梅哈里方法编写委员会成员的杰出贡献，以及马晶晶女士对此版本的翻译。

1. 引言

梅哈里方法论最初的设计及不断的发展，是为了协助首席信息安全官(CISOs)管理任务和制定信息安全及信息系统策略，因此本概述的主要面向对象是首席信息安全官。但是，在相同或类似的大环境中，也适用于信息系统审核员（Auditor）、 首席信息系统官（CIOs）或风险管理员（Risk Manager）。

本文的主要目的是描述梅哈里的用途，更详细的方法说明及相关的工具将在法国信息协会CLUSIF其它文件中提供，比如：

— 梅哈里基本原理及详细功能介绍,

— 使用指南：关键性分析，安全服务评估及风险分析，

— 安全服务参考手册，

— 知识库。

梅哈里的首要目标是提供一个针对信息安全领域的风险评估和管理的方法，此方法与ISO/IEC 27005:2008标准的要求及执行工具和要素相一致。

其它目标如下：

允许直接和独立地分析事件情景中描述的风险状况；

提供一套适合短期、中期、长期的系列安全管理工具，适用于各种不同类型和安全成熟度的组织。

鉴于这些目标，梅哈里提供了一致的方法论、适当的知识库，以帮助首席信息安全官，企业管理人员和安全管理人员，以及在风险管理中，实施步骤和行动的相关人员。

梅哈里与ISO27000系列标准的关系，将在本概述的最后章节进行描述。

2. 梅哈里用途

梅哈里首先是风险评估和管理的方法。

实际上，考虑到上面提到的第二个目标，我们建立了梅哈里及其知识库，以便于对风险状况进行更加准确的分析。在必要时，将在事件情景中描述这些风险状况。

尽管如此，安全管理作为一种功能或活动，会随着时间的推移或企业在其领域的纠正行动演变。实施安全步骤之前的第一步，毫无疑问是利用现有的安全措施做一个安全状态小结，并与最佳做法进行比较，以便填补风险缺口。

根据这一状况评估，做出建立安全措施和采取具体行动的决策。这些决策通常在计划、企业规划、参考或安全政策中通过结构化的方式出现。这种方式可以基于风险分析，根据ISO / IEC 27001的需求作为信息系统管理体系（ISMS）的一部分。但是还有许多其他的方法，包括“内部的、行业的或跨行业间的参考（或标准）”。

不过，在这个阶段，还不能真正的称为风险分析，必须确定安全关键性。通常情况下，决策做出前，最终的决策者都将面临一个问题：*“是否有必要拨出相应的预算？”*由于缺乏一个初步的评估和对安全风险的分析，许多安全项目被放弃或延期。

通常在较晚的时候，有时也会在安全措施实施初始，针对企业或组织的风险级别，提出下面这个问题：“组织所有的风险是否已被识别，这些风险是否可以接受？” 这个问题可以在概述或新项目的框架中提出。然后使用风险分析方法进行分析。

基于梅哈里的原理，在每一个发展阶段，必要工具必须是一致的，也就是说，在一定阶段上的所取得的结果以后可以重复使用。

梅哈里方法论中各种工具和模型，旨在对风险进行直接和个体的分析，可以单独使用于所有安全发展阶段，采取不同的安全管理模式，并确保整体决策的一致性。

这些模型和工具（下文将具体介绍）包括：风险分析的方法及相关工具、关键性分析模型及安全措施质量评估。

2.1. *风险分析*

风险分析几乎在所有安全类出版物中被提到，尤其是在ISO / IEC 27000

系列标准中作为安全需求表达的基础，但大多数时候，并没有提到应该用什么方法来进行风险分析。

近15年来，梅哈里以简单原则为基础，提供了一种结构化的方法来评估风险。

一个风险状况将受到以下因素的影响：

— 不依赖于安全的措施，但依赖于组织的核心活动、环境及背景的结构性因素。

— 降低风险的因素，他们直接关系到安全措施的实施。

其实，对于典型的结构性因素，我们只需分析关键性，以确定对风险状况产生后果的最大严重性。但在评估降低风险的因素时，其安全性评估是必不可少的。

梅哈里通过定性和定量的评估这些因素，来判定风险级别。梅哈里集成了工具（评估准则，计算方法等）和知识库（特别是对安全诊断）对ISO27005标准框架进行必不可少的补充。

2.1.1 风险状态系统分析

为了解答上面所提出的问题：*“组织所有的风险是否已被识别，这些风险是否可以接受？”*需要一个结构化的方法来识别所有潜在的风险状况，分析其中最关键的状况，然后再确定行动以降低风险至可接受的级别。

梅哈里所提供的方法和知识库实现了这一目标。在梅哈里的使用过程中，重点是要确保考虑到每个重大风险状况，并涵盖在行动计划中。

该方法基于风险状况和因素的情况特点，提供适当的风险处理方案及援助。

在风险评估过程中，主要有以下两种选择：

使用集合了梅哈里中各种模型结果 (关键性分析的资产结果分类，脆弱性评估)的知识库功能（Microsoft Excel）。这些功能，可以评估当前的风险级别，并提出降低风险的额外措施。

或使用软件应用程序（如 RISICARE），提供了更丰富的用户界面，及最先进、全面、可模拟和高优化的辅助功能。

2.1.2 风险状态局部分析

同样的工具可应用于任何其他安全管理模式中。

事实上，在一些安全管理模式中，风险管理不是主要基础，如在安全诊断策略或安全性的参考架构中，我们可以经常找到一些并不适用的规则。但

在局部风险分析决策中是非常有用的。

2.1.3 新项目中的风险分析

风险分析的模型和机制，可用于项目管理，以分析其风险，并做出相应措施决策。

2.2. 安全评估

该方法包括：安全措施诊断问卷，实际安全措施实施状况。问卷也可以评估降低风险方案和机制的质量级别。

2.2.1 脆弱性评估，风险分析因素

简而言之，在这个阶段，风险模式应考虑到“降低风险的因素”，特别是安全服务的体现。

风险分析时，详细评估这些服务，作为必要的可信、可靠的重要因素，来确保满足其职能。

作为风险分析和处理的方法， 梅哈里的优势之一是：无论分析当前风险级别，还是估计未来风险级别，都是基于对现有或已决定的安全措施质量的评估。

2.2.2 基于脆弱性评估的安全计划

一种办法是直接通过脆弱性评估建立行动计划。

该安全管理程序按照这一办法非常简单：运行评估和决定，对未达质量水平的服务进行改善。

梅哈里诊断问卷可以用于这一办法。

我们提倡结合梅哈里的其它模式，使用关键性分析，这部分将在本概述后面进行详细介绍。

安全风险分析包括：确定安全服务质量目标，或只选择在诊断框架中的相关服务作为审查目标。

2.2.3 知识库-为建立安全性的参考框架提供支持

基于安全服务知识库的评估模型（称为安全服务参考手册），描述了每个服务的宗旨、机制、及在服务解决方案和服务质量评估中所考虑的因素。

梅哈里这种独特的知识基础，可直接作为建立企业和组织中“安全参考框架”的依据。

这种方法通常用于大型独立实体组织或企业。也可用与许多跨国公司的

子公司，或有多个机构和地区代表的中小企业。在这种情况下，很难有效地执行大量评估或风险分析。

构建安全参考框架

梅哈里评估问卷调查，特别是安全服务参考手册和其相应讲解，将为安全管理人员在企业内部进行决策提供一个良好的工作基础。

规则的例外管理

安全参考框架的构造，通常在本地实施时会遇到困难，因此必须对例外的规则加以管理。

可以利用相关的知识库及风险分析手段和方法，通过对突出困难进行目标风险分析，来管理例外请求以处理当地困难。

2.2.4 脆弱性评估模型所涉及领域

从风险分析角度上看（即查明所有风险状况，并处理所有不能接受的风险），梅哈里的范围不仅仅局限于计算机系统。

评估问卷涵盖了除信息和通信系统以外，在一般情况下，组织场所的整体保护，用户的工作环境，监管和法律方面等问题。

2.2.5 评估模型概述

概括来讲，脆弱性评估问卷，提供了一个广泛和一致的安全看法，可用于各种研究方法，在企业任何安全成熟阶段进行深度分析。

2.3. *关键性分析*

在安全方面，无论方针还是策略，最主要的原则是得到领导人的批准。在如何安全投资和关键性级别之间有一个公正的平衡点。

这意味着，对企业安全关键性的正确认识是根本，对关键性的分析值得高度的重视并有严格的评价方法。

关键性分析的目标是回答以下两个问题：

“什么情况可能出现？如果此情况发生，会带来严重的后果吗？”

在安全领域，风险是被视为干扰企业或组织正常运作的后果因素。

梅哈里包括了关键性分析模型，在《关键性分析和分类指南》中描述，通过以下2种结果表现：

— 故障价值尺度；

— 信息分类和信息系统资产。

故障价值尺度

业务流程或企业活动中可能出现的事件故障识别，由以下步骤实现：

— 可能的故障种类描述；

— 影响每个故障严重程度的参数定义；

— 故障严重程度不同级别的参数临界评价。

故障值尺度由以上结果组成。

信息和资产分类

在信息安全领域，称为信息分类和信息系统资产分类。

这种分类包括：对每个信息种类和每个信息系统资产的定义；每个分类标准，通常是可用性，完整性和保密性（但也可能为其他标准，比如可追溯性或证据价值性），该标准代表信息或资产违背行为的严重性。

在信息系统中，信息和资产分类，可以称为故障价值尺度与信息系统资产相关的敏感指标。

安全风险表达

故障价值尺度和信息分类是表达安全风险的两种不同方式。

前者能为首席信息安全官提供更加详细的信息。后者则更全面，在敏感度和损失精确程度的传递上更加实用。

2.3.1 关键性分析：风险分析的基础

显然，这个模型是风险分析的关键，如果没有对潜在的故障、后果的共同协议，不可能对风险级别进行判断。

梅哈里为关键性评估和资产分类，提供了一种客观、理性的方法。

2.3.2 关键性分析：战略行动规划基石

显然，在实施任何形式的安全计划时，关键性分析是很有的必要的。事实上，无论使用任何方法，都将要分配资源，实施行动计划。而且，投资理由将会不可避免地受到质疑。

安全手段（比如保险），可以对风险产生直接的影响，如果没有对潜在的故障达成共同的协议，那么它的预算很可能得不到批准。

这种模型可用于风险分析以外的其它领域。

2.3.3 分类：安全政策的基本要素

我们已经提到的安全性的参考框架或安全政策，以及相关的安全管理方

法。

在实践中，通过一系列规则进行安全管理的企业，使用其规则，将要进行操作的行为，作为一个需要被处理信息的敏感度函数进行区分——这通常被称为信息和信息系统资产分类。

梅哈里的关键性分析模型提供了执行这一分类的方法。

2.3.4 关键性分析：安全计划的基础

在关键性分析过程中，显然需要业务管理人员的贡献，因为往往需要他立即采取行动。

经验表明，当与高层经营管理层进行会谈时，不论企业的规模大小，当他们解释其观点和对严重故障进行评估时，都会存在对安全的需求。这些需求他们可能没有预先考虑到，并且需要快速的响应。

行动计划可以通过两种方式直接建立。一是直接的方式，二是由经营管理者的行业经验及安全专家提供的安全解决方案相结合的方式。

2.4. *梅哈里用途概述*

显然，梅哈里的主要方向是分析和减少风险，以及为此目标所建立的知识库、机制和支持工具。

此外，根据不同的组织，这种分析和减少风险的结构方法论可以称为：

— 一种作为专业小组的指导方针的永久性工作方法

— 一种与其他安全管理措施同时使用的永久性工作方法

— 一种偶尔用来补充其他方法的工作方式

考虑到这一点，在需要进行风险分析设置时，梅哈里提供了一系列概念和工具。

梅哈里由法国安全协会CLUSIF发行，提供了包括知识库、手册、以及不同的模型(关键性-风险-脆弱性)的下载模式，来协助安全管理负责人(首席信息安全官，风险管理员，审计师，首席信息官……)履行其职责。

3. 梅哈里和ISO/IEC 27000系列标准

我们首先要回答一个问题： 面对国际标准，特别是ISO/IEC 27000系列标准，如何对梅哈里MEHARI进行定位？

这样做的目的是要解释梅哈里（MEHARI）如何适应这些标准的目标及兼容方面，更具体的是指ISO/IEC 27001, 27002 和 27005标准。

3.1. *ISO/IEC 27001, 27002 ，27005标准及 梅哈里的不同目标*

3.1.1 ISO/IEC 27002:2005 的目标

该标准指出，一个组织必须从以下三个主要来源确定其安全性要求：

— 风险分析

— 法律，法规，合同要求

— 该组织已发展到支持其业务的原则，目标和适用于信息处理的要求的集合。

以此为基础，控制点可以根据ISO27002标准或其他控制点标准中“ 信息安全管理代码 ”章节(§4.2)的规则进行选择和实施。

注：很显然，在27002 :2005版本的 “范围 ”里，标准规定的“ 启动，实施，维护和改进信息安全管理的指导方针和总体原则 ”即ISO标准中可以作为 “一个起点看待 ”。然而，在ISO/IEC 27001规定 (§1.2) ，任何措施的删减，必须证明是合理的，并且可以接受增加控制目标 (附录A-A.1)。

ISO27002标准为企业提供了一个指导方向。然而，该清单并不完备，一个组织可能考虑另外必要的控制措施，但是，现在还没有任何一种方法可以建立完整的安全管理体制。

另一方面，每个部分的最佳指导的包括总则和预订目标，这可以是一个非常有用的帮助意见。

注：ISO标准在« 范围»中指出，可用于“ 在跨组织的活动中建立信任 ”。这并不是偶然的。相反，这是标准的支持者们所提倡的一个关键特性，那就是从信息安全的观点来说，这是对合伙人以及供应商的一种评估（甚至是认证）。

3.1.2 ISO/IEC 27001:2005的目标

在ISO/IEC 27001中明确的提出了目标：“为建立、管理信息安全管理体系（Information Security Management System，简称ISMS）提供模型 ”以及“用于内部或通过第三方应用 (包括认证机构) ”

这种评估目标和认证导致了对形式(决策文件和登记、适用性声明、记录等等)和控制(审查、审计等等)的强烈关注。 因此，这是一种非常注重质量的方法。

很显然，该方法的基础涉及到对企业或组织关键性和风险的分析，并选择适当的措施，以降低风险到可接受的程度。

ISO/IEC 27001 表明了风险分析的方法必须应用循环模型 (PDCA- Plan规划， Do执行， Check 查核， Act 行动) 进行定义，以建立ISMS.

此外，降低风险的措施，建议(或最好)与ISO/IEC 27002 :2005相一致。相关的控制点清单在附录中提供。

根据ISO/IEC 27001标准，在信息安全管理体系的评估基础中，我们不需要知道或者确定是否做出了相关的决定，或者体现了企业的需要。但是我们需要核实，一旦做了决定，并且确定管理制度后，审查员或认证员是否可以肯定这个决定已得到执行。

3.1.3 ISO/IEC 27005:2008的目标

这个标准的目标不是建立一个完整的风险管理方法，而是设定最低限度框架，并说明要求 。在进行风险评估过程中，确定威胁和脆弱点，其次是风险估算，评估风险级别，然后选择处置方法以及相关的计划和模式(包括安全措施和指标)，以改善现状。

因此，这并不是一套完整的、自给自足的方法 (在标准中甚至提出，应该选择一种方法)，而是为避免选择过于简单，或者与风险管理概念不一致的方法而设定的一个框架。

3.1.4 梅哈里的目标

梅哈里作为一种连贯的，全面的，自给自足的安全管理工具和方法，以详细的风险分析为基础。

梅哈里的基础方面包括：

— 风险模型(定性和定量)；

— 在模型中，安全服务或计划实施成效的定量评估；

— 对残余风险水平的评估和额外措施。

这些是ISO/IEC 27000，尤其是ISO27005标准中强制要求的组件。

3.1.5 梅哈里与ISO/IEC 27002 和 ISO/IEC 27001目标的比较分析

梅哈里的部分初步目标与上述提到的ISO目标不同：

— 梅哈里的目的是提供系列工具和方法，可以为特定企业选择最适合(技术上和经济上) 的安全措施，以及在这些措施实施时，进行残余风险的评估。这并不是ISO标准最初规定的目标。

— ISO标准提供了一套最佳的做法，以判断在信息安全规划中的成熟度，及独立或有合作伙伴的内部关系。这些方法肯定是有益的，但不一定适用于所有组织，。

在梅哈里中，安全服务参考手册提供了详细的内容用于建立安全参考。通过与ISO/IEC 27002进行比较，很明显，梅哈里的服务覆盖面比ISO国际标准更加广泛，涵盖了计算机系统本身以外的安全关键方面。

3.2. 方法之间的兼容性

梅哈里其实与ISO27002是完全一致的，虽然它们没有相同的目标，但它可以更容易的代表在ISO27002 指标方面的分析结果。

梅哈里满足了两个标准 (ISO27001, ISO27002) ，依赖于风险分析，以确定实施措施的需求。

3.2.1 与ISO/IEC 27002 :2005的兼容性

ISO标准的 “控制点” 或 “ 最佳做法 ” 主要是一般的措施 (组织和行为) ，而梅哈里整合这些措施，并强调提高措施成效来减少脆弱性。

尽管存在这些差异，对于那些需要提供符合此标准证据的组织，梅哈里中的相应表格可提供与ISO/IEC 27002：2005标准相一致的结果。

这里值得一提的是：梅哈里中的审核问卷的设计和构成，实现了各级业务管理人员之间对脆弱性分析的有效运行，并推断出每个安全服务能力，降低这些风险。

3.2.2 与ISO/IEC 27001的兼容性

梅哈里可以很容易的融入到在ISO/IEC 27001中定义的PDCA (规划-实施-检查-处置) 循环中去，特别是 “ 规划 ” (§4.2.1) 阶段。梅哈里完全覆盖了建立ISMS基础的描述任务。

“实施” (§4.2.2) 阶段，旨在实施和管理ISMS，梅哈里提供诸如对风险处置计划建立有用的因素，这直接关系到其使用过程中风险分类的优先次序和实现进度指标。

“检查 ”(§4.2.3) 阶段，梅哈里提供了必要的因素，通过安全服务中估计或审核来确定残余风险，并在安全措施中做出改善。此外，环境中的任何变化 (关键性、威胁、解决方案和组织) ，都可以很容易的引起审核员对梅哈里的初步审核结果的重新评估， 因此，安全计划可以随着时间的推移进行修改。

“处置 ”(§4.2.4) 阶段，梅哈里隐性地调用控制并持续改进安全性，从而确保降低风险的目标得以实现。在这三个阶段中，梅哈里不是这一进程的核心，但是它大大促进其执行，并确保其效率。

3.2.3 与ISO/IEC 27005：2008的兼容性

ISO标准所确定的框架是完全适用于MEHARI风险管理的方式，例如：风险分析、评估和处置过程 (在ISO13335中也提及)、对基本资产和支持性资产的定义的确定，和风险级别的分类(或升级) 及关键性的分析。

威胁及水平的识别(自然接触)确定，在梅哈里中的事件情景中有更精确的描述。

现有安全措施有效性的确定和提高，减少了背景脆弱性。

考虑到这些因素，在为事件情景的严重程度评估时，制定了4个级别等级，可以将选定的安全措施，用于降低风险计划中。

因此，梅哈里方法不仅可以轻松的融入到ISMS过程中，如在ISO27001中描述，也可以充分满足ISO27005的需求。