基于 ITIL 的气象信息管理研究和应用

胡利军,庄科旻,杨 豪,黄思源
(宁波市气象网络与装备保障中心,浙江 宁波 315012)

摘 要:随着气象业务的不断发展,信息基础设施、现代化设备、业务系统不断升级、完善、优化,系统运维和服务能力要求也随之不断提高,为解决原有 IT 运维管理运行效率低下、用户满意度不高的弊端,在气象业务 IT 运维管理中引入 ITIL(信息技术基础架构库)规范。基于 ITIL 开发业务管理系统,制定相关的业务处理流程,加强日常服务管理,实现服务管理的流程化和规范化,提高 IT 运维人员服务水平。在做好日常 IT 服务管理的基础上,开展基于 ITIL 网络信息安全管理方面的研究工作,进一步提高安全防护水平,增强安全管理能力。系统投入业务使用后,有效地提高了业务运维效率、服务管理能力,保障了系统的安全性和可靠性,提高了用户的满意度,在做到业务留痕的同时,建立了信息管理数据库。

关键词:信息技术基础架构库;信息管理;规范化;流程化;信息安全
中图分类号 TP315 **文献标识码**:A **文章编号**:1673-629X(2019)07-0175-04
doi:10.3969/j.issn.1673-629X.2019.07.035

Research and Application of Meteorological Information Management Based on ITIL

HU Li-jun, ZHUANG Ke-min, YANG Hao, HUANG Si-yuan
(Ningbo Meteorological Network and Equipment Support Center, Ningbo 315012, China)

Abstract: With the development of meteorological business, IT infrastructure, modernization equipments, and business systems are continuously upgraded, improved, and optimized. Thus the requirements of system maintenance and service capability are also continuously improved. To improve the IT maintenance efficiency and users' satisfaction, the ITIL (information technology infrastructure library) is introduced in business management. We develop business management system based on the ITIL, formulate relevant business process, strengthen daily service management, realize the process and standardization of service management, and also improve the service level of IT maintenance personnel. Meanwhile, on the basis of daily IT service management, network information security management based on ITIL is carried out to further improve the level of security protection and enhance security management capabilities. After the system is put into use, it effectively improves the maintenance efficiency, standardizes the service level, ensures its security and reliability, and improves the users' satisfaction. At the same time, we record the relevant operations and establish the information management database.

Key words: ITIL; information management; standardization; process; information security

0 引 言

随着数据中心 IT 基础设施升级迭代,现代化建设项目的推进实施,业务信息系统开发应用,服务管理的要求也随之不断增强。尤其在网络信息安全不断加强和重视的情况下,如何利用先进的技术和有效的管理手段,加强信息系统管理、提高业务服务水平显得尤为重要[1]。在气象信息 IT 运维服务管理方面,引入 ITIL(IT 基础架构库),开发了“基于 ITIL 的气象信息管理平台”。实现了气象业务 IT 系统服务管理的规范性、有效性和持续性,做好各类信息系统的管理、事件的处置、档案管理和业务留痕等,同时在网络安全防护[2]、事件处置方面进一步规范高效。文中主要涉及两部分内容:规范化、流程化的运维管理[3],和 ITIL 在等级保护信息系统安全管理方面的应用。

1 IT 服务管理

1.1 运维管理

系统运维包括系统的日常维护、保障系统运行两

收稿日期:2018-08-12 **修回日期**:2018-12-17 **网络出版时间**:2019-03-21
基金项目:国家自然科学基金(41675110)
作者简介:胡利军(1973-),男,硕士,高工,CCF 会员(97601M),研究方向为计算机信息处理。
网络出版地址:http://kns.cnki.net/kcms/detail/61.1450.TP.20190321.0917.050.html

层含义,与业务增长量、基础设施数量、安全等级的要求成正比,业务增长越快、设施数量越多、安全等级越高,对系统运维的保障能力要求也越高[4]。在业务规模越来越大,网络设备、安全设备、服务器资源和业务系统的不断增多,人员又比较紧张的情况下,面对环境、需求的不断变化,对如何采取有效的运维方式、进行规范高效的管理提出了要求[5]。业务运行中,采用商业软件和自主开发程序相结合的方式进行监控管理,同时在气象信息服务管理中引入 ITIL 规范。

对于应用 ITIL 管理 IT 服务的研究,国外起步较早、应用范围较广,在提高服务质量、降低 IT 服务交付和支持成本,以及协同 IT 和业务需求方面取得了很大成功;而国内 ITIL 用于运维管理方面的研究虽有多年的时间,但具体应用在业务上较少。面对管理规范化、服务高效持续的需求,引入 ITIL 规范,开发了信息管理系统,以进行 IT 基础设施的软硬件配置管理,紧急事件处置、问题处理、服务可持续性管理等,以及根据信息系统等级保护的需求实现信息安全管理。

对日常 IT 业务运维中出现的事件、问题、配置、变更和发布等流程进行研究,规范日常业务管理,在流程化、规范化管理的基础上提高服务质量,以用户为中心,在尽可能少影响业务的前提下,快速地恢复服务,保证最佳的效率和服务的可持续性[6]。

在 ITIL 实践策略中,开发的系统平台包括配置管理、事件管理、问题管理、变更管理和发布管理等模块,文中以“事件管理”为例来介绍基于 ITIL 的管理流程。

1.2 事件管理

运维时既要做到妥善快速处理,又要做到留痕、有迹可循,需要对发生的事件进行识别、记录、分类等,按事件的轻重缓急进行解决处理[7]。根据 ITIL 的规则,对业务运行中发生的事件进行电子化、流程化管理[8]。事件处理流程分两类,“一般事件处理流程(见图 1)”和“特殊事件处理流程”,以“一般事件处理流程”为例。

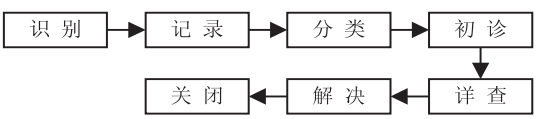

图 1 一般事件处理流程

通常情况下,值班人员接到报告后,首先进行“事件识别”,了解发生事件的初步信息,通过系统平台在数据库中记录,包括事件管理涉及数目、确认的时间、发生的时间、发生地点、事件信息提供者、有关事件的服务、与事件有关的软件和硬件、事件详情、事件类别,以便对该事件后续进展进行有效整理和趋势分析;然后,根据事件处置的紧迫性、对业务的影响程度来对事件进行“分类”,确定处理优先级。

分类时,同时确定事件的处理提交对象,“网络管理员”、“系统管理员”或“安全管理员”等。负责处理的人员按照事件处理流程来处理,同时查找数据库中相关事件和已知解决方法等类似记录以寻求对策。一旦确定了处理方法,及时处理事件,恢复业务正常运行;若暂无相应解决方法,则提交上一级技术部门、技术外援寻求帮助,进一步调查和诊断,直至事件处理结束。事件处理完毕,经与提交事件的用户确认后,关闭事件。

关闭前,在系统平台上对整个事件的发生、处理详情等情况进行记录。“事件记录”,要做到被处理事件的记录完整性,包括日期、时间、地点、处理者、状态、事件优先级、事件现状、事件解决的时间、关闭的时间等;已解决的事件,要将平台数据库中“事件的状态”从“解决中”、“未解决”等状态及时更改为“已解决”,此时平台中“状态”的颜色也由“红色”变为“黑色”;事件处理过程中,要做好事件的进展跟踪和用户间的沟通交流。

1.2.1 事件优先级确定

对事件处理的优先级进行分类[9],处理优先级通常取决于事件对业务的影响程度和处理紧迫性(见表 1)。

表 1 事件的影响程度和处理紧迫性

等级	影响程度	处理紧迫性
最高级	业务完全停止	立即解决
高级	关键性问题	当天解决
中级	有轻微影响	短期内解决
低级	基本没影响	可列入解决计划

结合事件影响和紧迫性程度对事件优先级(见表 2)进行裁定,当事件处理优先级为“1”时,说明该事件急迫需通过特殊程序及时处理。

表 2 优先级

优先级		影响			
		最高级	高级	中级	低级
紧迫性	最高级	1	1	2	3
	高级	1	2	3	4
	中级	2	3	4	5
	低级	3	4	5	5

涉及高危漏洞、特殊节点时段的安全事件优先级为“1”,接到该类事件报告后,按特殊流程进行处理,直接进入初诊阶段,进行事件诊断,确认事件的真实性。然后进行“事件详查”,寻找处理该事件的方法,根据应对措施、处理方法“解决事件”;最后“关闭事件”,对事件进行总结记录。

1.2.2 事件处理事例

根据 ITIL 的规则,对业务运行中发生的事件进行

电子化、流程化管理。例如处理新一代多普勒天气雷达回波有干扰杂波事宜,如图 2 所示。

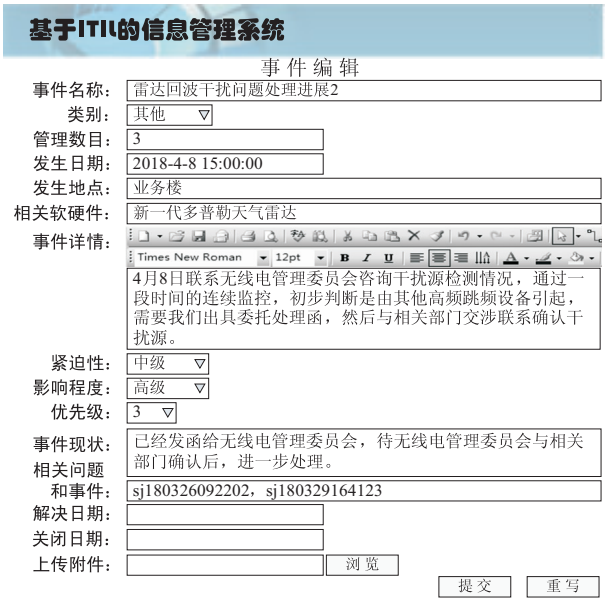

图 2　事件处理图例

“事件识别”:运行监控室接到电话,雷达回波产品有杂波干扰。对事件进行核实,初步识别并提交给运维人员。

“事件记录”:记录事件并编号“sj180326092202”,表示处理时间在 2018 年 3 月 26 日 9 点钟,同时记录下发生日期、时间、地点、处理者,此时事件的状态为“未解决”。

“事件分类”:杂波问题,短时间不易解决,需要排除是雷达本身的原因,还是受外界的干扰,短时间内无法处理,但对雷达回波产品的分析产生了影响。对业务的影响程度为“高级”,紧迫性为“中级”,根据表 2 可看出该处理事件“优先级”为 3,在短期内处理好该事情即可。

“事件初诊”:对该事件进行初步诊断,查找回波杂波产生的相关信息,确认事件的真实性,起始时间和杂波的影响程度。杂波干扰出现的时间不固定,基本上在白天产生,晚上没发生杂波现象。

“事件详查”:联系厂家,对雷达回波杂波问题进行排查。确认雷达本身没有问题,与外界干扰有关。与相关部门联系,查找干扰源,同时告知用户产生杂波的初步原因及处理进展。

“解决事件”:经跟踪检测和判断,杂波由其他高频跳频设备引起,需要函告相关部门确认,该事件编号为“sj180408173019”,与前面“sj180326092202”事件关联,多个关联事件间可以相互间跳转。

“关闭事件”:此时事件的状态为“已关闭”,事件已解决。

事件规范化管理的主要目的是对业务影响最小前提下,采取最佳处置方式,快速解决问题,恢复业务正常运行。系统记录了事件发生、处理、解决的全过程,建立了事件管理数据库,给其他服务管理提供了详实的信息。

2　ITIL 在安全管理中的应用

2.1　防护体系建设

在信息系统运行保障中,为提高业务平台的健壮性和安全性,除做好物理安全和主机安全外,关键还是管理意识和管理模式的提高[10]。按要求建立和落实各类规章、制度、流程,明确责任、及应急处理规范等。为规范管理,在“基于 ITIL 的气象信息管理平台”中,增加了“信息网络安全管理”子系统,根据等级保护的要求实现信息的安全管理[11-12],进一步加强人员、设备、规章制度、政策文件、维保合同、运维情况等内容的管理,建立事件处置应急流程和知识库[13]。

2.2　系统框架

子系统采用 ASP. NET+SQL SERVER 开发技术,系统档案模块前台显示和录入修改功能开发基于 WORDPRESS 实现,内容包括等级保护相关的各类“规章制度”、“协议书”、“合同报告”、“事件管理”、“25 类表格”、“系统档案”等。

系统框架如图 3 所示。

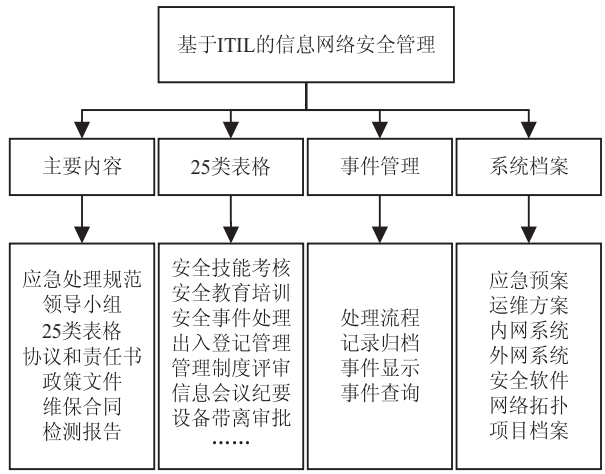

图 3　安全管理子系统框架

在“信息网络安全管理”子系统中,对安全技能考核、安全教育培训、安全事件处理、出入登记管理、操作运维记录、应急预案培训等 25 类内容建立流程和电子化档案[14]。

2.3　安全事件管理

2.3.1　事件流程

当发生的事件处理优先级为“1”时,说明该事件急迫需启动紧急流程特殊处理。网络安全事件优先级一般来说都是“1”,也就是“优先紧急处理”,需要启动应急处置流程(见图 4)。

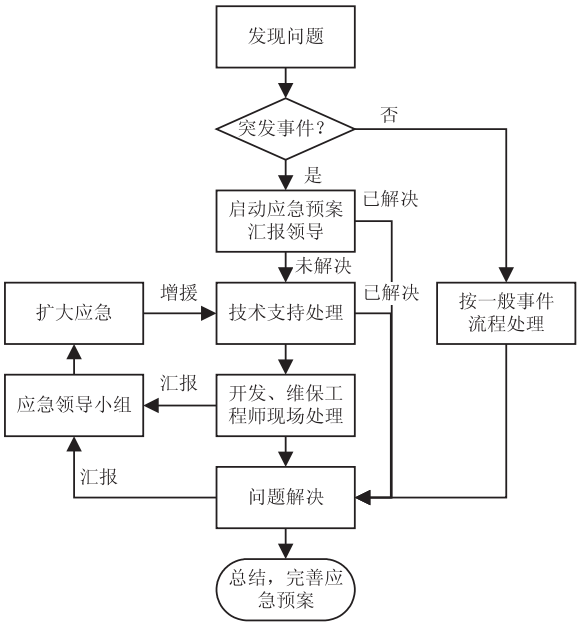

图 4 应急响应流程

2.3.2 特殊流程事例

某日接通知,网站存在安全漏洞。由于涉及网络安全,马上启动应急流程,进行了以下处置:第一时间报告相关领导,关停相关网站服务;经技术分析识别,该漏洞跟页面开发代码有关,通知开发人员进行代码修改、漏洞修补;相关人员立即到岗,落实处置措施,并进行下步详细部署;技术人员继续对网站进行主机漏洞、应用漏洞和后门木马扫描;开发人员快速解决漏洞问题,从接到通知到解决问题,用时在 2 小时内。完成所有相关服务器、系统扫描后,出具报告并上报。最后,梳理完善档案记录,经再次确认后,恢复相关网站和应用。

该事例属于“特殊事例”,优先级为“1”,按紧急流程处理,主要分初诊、解决、关闭三个步骤,最后再进行详情记录。

一件完整的事件记录含事件名称、事件类别、管理数目、发生日期、地点、信息提供者、事件相关服务、相关软硬件、事件详情、事件紧迫性、影响程度、优先级、目前现状、关联问题事项(编号)、解决日期、事件关闭日期、相关事件附件等。

在管理系统中引入 ITIL 准则后,对事件进行流程化、规范化管理,建立了完整的档案。在回顾过往事例时,可以完整地还原一个事件处置的全过程,对后期相关事件的处理提供了参考依据。

3 结束语

将 ITIL 的准则引入到气象信息管理中,结合单位业务运行实际,建立一个基于 ITIL 的信息管理系统[15]。按规范制定事件处置应急流程,提高事件处置的规范性、及时性,以及事件档案保存的完整性;按照 ITIL 的规范以及制定的流程进行日常 IT 业务管理,使 IT 运维人员管理更加方便、高效,更加了解各个环节间的相互关系;提高了 IT 服务用户的满意度、系统的可用性,以及运维人员解决处理问题的能力;建立了流程管理数据库,实现了各类模块管理的记录、查询和显示等功能,达到规范记录、档案保存、业务留痕的目的。

参考文献:

[1] 王 军. 基于 ITIL 的运维管理系统设计与实现[D]. 北京:北京邮电大学,2010.

[2] 孙佑海. 网络安全法:保障网络安全的根本举措——学习贯彻《中华人民共和国网络安全法》[J]. 中国信息安全,2016(12):28-33.

[3] MÜLLER S D,DE LICHTENBERG C. The culture of ITIL:values and implementation challenges[J]. Information Systems Management,2018(1):49-61.

[4] 杨 钰,吴 健. ITIL 中 IT 基础架构管理模型设计与实现[J]. 计算机技术与发展,2007,17(4):250-253.

[5] OIC. System management policy[M]. Japan:OIC Japan International Cooperation Agency,2012:10.

[6] 贺俊彦,刘 然,刘红梅. 基于信息技术基础架构库(ITIL)的气象信息业务统一运维体系的建设与发展[J]. 气象科技进展,2018,8(1):232-236.

[7] 陈喜珠,谢 炜,裴俊豪. 基于 ITIL 的政务云运维管理平台设计与研究[J]. 电信工程技术与标准化,2018,31(4):48-53.

[8] OIC. System management design[M]. Japan:OIC Japan International Cooperation Agency,2011:17.

[9] OIC. Risk management[M]. Japan:OIC Japan International Cooperation Agency,2012:37.

[10] 张瑞冉. IT 服务管理在运维管理中的研究与应用[D]. 北京:首都经济贸易大学,2012.

[11] 李 军,谢宗晓. 信息安全等级保护与信息安全管理体系的比较[J]. 中国质量和标准导报,2017(8):58-63.

[12] 张震华. 基于 ITIL 的公安 IT 运维管理系统的设计与实现[J]. 信息系统工程,2013(2):61.

[13] 刘慧敏. 以 ITIL 为基础的 IT 服务管理应用研究[J]. 计算机技术与发展,2012,22(5):195-197.

[14] 赵晶晶. 网络安全等级保护及实施方案[J]. 电子技术与软件工程,2017(7):224.

[15] 周 霞. 探索 IT 服务管理(ITSM)在胜利油田的应用[J]. 计算机技术与发展,2011,21(3):236-238.