浅谈信息系统安全集成服务能力建设

翟亚红[1]，吴　治[1,2]，段静辉[1]，彭琳赓[1]

（1.中国网络安全审查技术与认证中心，北京 100020；
2.辽宁省先进装备制造业基地建设工程中心，辽宁 沈阳 110001）

摘　要： 网络安全已是国家战略。从事信息系统安全集成服务企业的服务能力，对于信息系统建设具有重要的影响。安全集成服务认证作为一项自愿性认证受到广大IT企业的认可。在从事安全集成服务认证审核中，发现依然存在一些共性方面的问题。剖析安全集成服务内涵，总结分析企业在安全集成服务能力方面存在的问题及产生问题的主要原因，对于企业安全集成服务能力提升提出一些建议。

关键词： 信息系统；安全集成；服务能力

中图分类号： TP399　　**文献标识码：** A　　**DOI：** 10.19358/j.issn.2096-5133.2020.10.007

引用格式： 翟亚红，吴治，段静辉，等. 浅谈信息系统安全集成服务能力建设[J]. 信息技术与网络安全，2020，39(10)：33-37.

Discussion on the construction of information system security integrated service ability

Zhai Yahong[1], Wu Zhi[1,2], Duan Jinghui[1], Peng Lingeng[1]

(1.China Cybersecurity Review Technology and Certification Center, Beijing 100020, China;
2.Liaoning Advanced Equipment Manufacturing Base Construction Engineering Center, Shenyang 110001, China)

Abstract: Network security is a national strategy. The service capability of enterprises engaged in information system security integration service has an important impact on the construction of information system. Security integration service qualification, as a voluntary certification, is recognized by the majority of IT enterprises. In the audit of security integration service qualification, we found that there are still some common problems. This paper analyzes the connotation of security integration service, summarizes and analyzes the problems existing in the security integration service capability of enterprises and the main reasons for the problems, and puts forward some suggestions for improving the security integration service ability of enterprises.

Key words: information system; security integration; service capability

0 引言

安全集成服务认证作为一项自愿性认证，由中国网络安全审查技术与认证中心（以下简称：网安中心）负责，自2012年至今已经过将近十年的发展。信息安全服务[1]现有7个方向，分别是信息安全风险评估、信息系统安全集成、信息安全应急处理、信息安全灾难备份与恢复、软件安全开发、信息系统安全运维、网络安全审计。截止到2020年6月底，获得安全集成服务认证企业近两千家，是各类安全服务企业申请并取得证书数量最多的一类服务。

随着信息技术的发展，特别是网络安全技术的不断发展，安全集成服务认证依据自ISCCC-SV-003：2011《信息系统安全集成服务认证规则》发展至CCRC-ISV-C01:2018《信息安全服务规范》，安全集成服务专业能力已受到前所未有的重视。在认证审核的过程中，无论是对于已获证企业的监督审核，还是对于新申请企业的初次审核，从满足审核依据的要求方面，仍然存在着各种不同程度的问题；从国家安全战略方面，安全集成服务企业自身安全服务能力需要持续提升，从而促进网络安全建设能力水平，有利于提升整体网络安全防护能力。

本文首先分析安全集成服务内涵；其次分析安

www.pcachina.com

全集成专业评价要求，并总结认证审核发现最为典型的三方面问题，提出安全服务能力评价模型；最后针对企业安全集成服务能力持续建设提出一些建议。

1 安全集成服务内涵

1.1 安全集成的定义

信息系统安全集成服务是按照信息系统建设的安全需求，采用信息系统安全工程的方法和理论，将安全单元、产品部件进行集成的行为或活动。可从多个层面来理解安全集成的定义：第一个层面信息系统[2]，对于信息系统的定义，在此不再赘述；第二个层面安全，即信息系统安全[3]，包括了信息系统安全体系[4]、信息系统安全管理目标、信息系统安全需求、信息系统安全设计、信息系统安全技术、信息安全标准与法律法规等；第三个层面集成，是指一些孤立的事物或元素(这里具体指安全单元、产品部件)通过某种方式集中在一起，产生联系，从而构成一个有机整体的过程；第四个层面技术和方法，包括需求调研、方案设计、建设实施、安全测试和运行维护过程的技术和方法；第五个层面工程项目，主要内涵在于项目管理[5]，涉及质量管理[6]和信息安全管理[7]方面。

1.2 安全集成服务的内涵

对于安全集成的理解已在前面进行详述，安全集成服务其内涵体现于服务，即对于一个项目，必然存在着信息系统的建设方和信息系统的承建方，承建方凭借其自身的专业技术能力向建设方提供专业的服务，双方通过签订合同或协议，约定各自权利、义务、责任，明确在给定的费用和时间约束规范内，完成一项独立的、一次性的工作任务。承建方(安全集成企业)通过完成这个工作任务，实现建设方信息系统安全建设目标。

从审核的角度来看，如何确认企业所提供的业绩(案例)属于安全集成类项目，第一，从合同(包括合同的有效组成部分，例如投标文件、技术协议等)约定来看，这个项目属于服务类的项目，包括了安全服务在内的系统集成类项目(单一设备采购、独立软件开发、独立产品研发项目不宜作为安全集成项目)；第二这个项目一定是有其建设过程的，即可以从信息系统生命周期[8]角度理解，应该至少能够区分集成准备、方案设计、建设实施和安全保障四个过程；第三在这个项目的建设过程中，企业应用了其自身所具有的集成服务能力，能够体现于项目建设形成的过程文档和项目建设的成果。

2 安全集成专业评价

2.1 安全集成专业评价要求

依据 CCRC－ISV－C01：2018 附录 B 信息系统安全集成服务资质专业评价要求，提出安全集成服务专业能力在集成准备、方案设计、建设实施、安全保障四个过程应该具备的能力要求，详见表 1 所示。

表 1 评价指标数量

过程	要点	一级	数量	二级	数量	三级	数量
集成准备阶段	需求调研与分析	*	6	*	5	*	3
方案设计阶段	方案设计	*	9	*	6	*	3
建设实施阶段	实施集成	*	8	*	6	*	3
	监督管理	*	1	–	–	–	–
	系统测试	*	5	*	4	*	2
安全保障阶段	系统试运行	*	7	*	4	*	2
	验收	*	2	*	2	*	2
	运行维护	*	3	*	2	*	1

对于安全集成专业评价要求，各个级别在服务过程和服务要点方面的要求基本是涵盖的，指标数量的区别主要体现对于服务能力要求程度的不同。以系统测试要求为例说明，对于三级企业要求基本具备系统测试能力，目的是通过测试验证完成合同约定的服务内容，达成系统安全建设目标；对于二级企业要求在具备测试能力的基础上，能够规范地开展测试，形成测试方案、记录、报告等；对于一级企业则提出了更高的要求，即能够制定系统安全性测试方案，模拟攻击场景，对系统安全性进行测试，体现了对企业在人员、工具、测试方法、测试深度、测试规范性等综合能力方面的要求。

2.2 安全集成专业审核典型问题及分析

总结近两年安全集成服务审核案例，归纳企业在安全集成专业能力方面三个方面的典型问题，并逐一对问题出现的原因进行分析。

第一，表现在技术服务要求方面。对于初次申请企业，流程和规范方面常见问题具体表现在三方面，一是所制定的流程和规范适用范围不是安全集成服务，例如是适用于软件开发，或者系统集成实施等；二是所制定的流程和规范其内容不全面，

www.bcachina.com

未能覆盖安全集成服务全过程要素；三是所制定的流程和规范，具体内容方面过于宏观，不能有效地指导项目执行，规范要求与项目执行实际脱节。对于监督审核企业，流程和规范方面常见问题具体表现在三方面，一是所提供的流程和规范缺少定期的评审和修正；二是所提供的流程和规范，对照项目执行过程文档，发现要求在项目实施过程中未能被充分应用；三是规范的体系化建设方面，未能及时地修订相关指导书或是未能结合技术发展新制定相关指导书。分析以上问题，其主要原因在于三个方面，首先是对于规范条款要求的理解不到位，尽管网安中心通过组织培训，编制自评估表及自评估指导书等多种方式对规范条款要求进行解读，但在知识的接收和传导环节依然难以充分有效；其次是企业安全集成服务能力部分不足，整体安全集成服务能力的构成包括人员、工具、组织级管理、项目级管理以及特殊能力要求等多方面，部分能力的不足或缺失，直接反映在规范方面要求的缺失；第三是体系化建设方面不健全，安全集成流程和规范自身的体系化建设不完善，以及与组织级质量管理体系、信息安全管理体系等未能够充分有效地融合。

第二，表现在项目过程管理要求方面。这个方面的问题反映在项目组和公司的职能部门两个层面，常见问题具体表现在两方面，一是在安全集成服务实施过程中该形成的文档未形成或未保存或有遗失；二是在安全集成服务实施过程中所形成的文档内容不全或不符合公司要求或不满足审核要求。分析以上问题，其主要原因在于三个方面，首先从项目组来看，表现在人员能力方面不足，公司级管理重在对于项目经理的管理，而易忽视对于项目组成员的管理，职能部门人员对于项目的参与程度不够，往往流于形式，对于项目组成员，尤其是新进成员，缺少有效培训，在项目执行过程很难按照规范执行。其次是公司对项目组绩效考核评价的导向问题，重结果轻过程的要求，导致了项目组在项目执行环节的管理问题，公司级职能部门对于项目监管缺失或者失效，直接导致了项目过程管理的问题。此外，特别说明一下监督审核中一个常见问题，即在监审过程中，由于管理的原因，未能够充分地将企业的安全集成能力充分展现出来。这个问题的原因主要是企业人员变化，特别是规模大的企业具有人员多、项目多等特点，监督审核的目的在于查验企业服务技术能力的维持情况，而每次企业申报项目材料的技术人员往往因项目不同而变化，因而可能造成申报材料少交、漏交情况，导致企业真实服务能力水平不能完全体现，当然出现这种情况归根到底还是企业管理方面的原因。

第三，表现在技术能力要求方面。这方面的问题主要反映在方案设计、集成实施和系统测试阶段，常见问题具体表现在三方面，一是对于安全需求调研不充分，如等级保护防护需求，等级保护进入2.0时代，无论对于新建系统，还是改扩建系统，等级保护的安全防护需求都应该进行调研；二是在设计环节，未能明确设计的依据(如国家标准、行业规范等)，未能编制有效的施工手册和作业指导书；三是系统测试不全面，未能有效地覆盖合同建设内容，系统测试的深度不够，不能达成测试的目的，对于一级企业，包括渗透测试在内的安全性测试能力尚有一定的不足。分析以上问题，其主要原因在于三个方面，首先是认识方面的原因，对于安全集成技术能力的本质认识不到位，从审核的角度关注的是企业自身所具有的技术能力，而不是集成其他企业的，未建立或者是未能有效地建立长效的技术能力提升体系；其次是基于商务的或者技术方面的原因，只完成合同明确约定的服务内容或者是建设单位明确提出的要求，但是鉴于从事的是“安全”事业，那么无论建设单位是否明确提出，作为承建方都有义务完成国家、行业法律法规和技术标准规定的要求，例如等级保护制度的要求；第三是人员能力、设备等资源能力的欠缺，专业技术人员是企业发展的基础，人员能力是企业服务能力的直接体现，因此对于专业技术人员能力的培养是十分重要的。从事信息安全服务应用自动化的工具设备是提升服务能力效率最直接的方式，因此，对于工具设备的配置和使用，特别是有能力的服务企业，对于工具的自主研发也是十分重要的。

2.3 安全服务能力评价模型

为促进提升安全服务企业安全服务能力，同时持续改进安全服务能力评价水平，基于对安全服务能力核心要素的识别，构建安全服务能力评价模型，如图1所示。

该模型适用于目前包括安全集成服务方向的8个信息安全服务方向。由图1可见，安全服务能力评价等级划分为一级、二级和三级，安全服务能力

www.bcachina.com

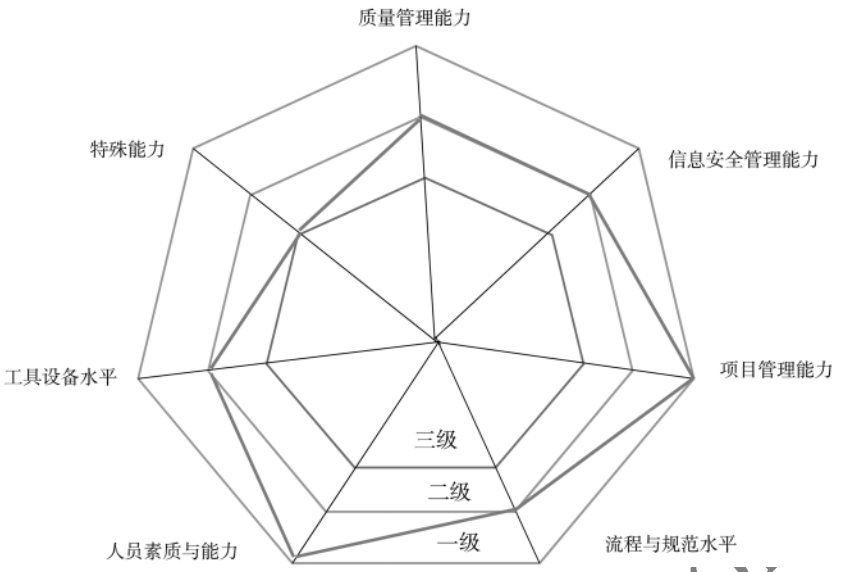

图 1 安全服务能力评价水平

核心要素包括质量管理能力、信息安全管理能力、项目管理能力、流程与规范水平、人员素质与能力、工具设备水平、特殊能力。对于特殊能力作为不同方向的差异化能力要求。

3 安全集成服务能力建设几点建议

3.1 多体系融合方面的建议

安全集成服务涉及 ISO9001 质量管理体系、ISO27001:2013 信息安全管理体系、ISO20000-1:2011 信息技术服务管理体系等多体系，因此，安全集成服务首先应是在某管理体系覆盖范围中，其次能够按照管理体系的要求良好运行，第三，多体系作为上层结构，安全集成服务在执行层与体系要保持一致。安全集成服务是一种组织行为，因此，在企业中安全集成服务需要各职能部门按职责分工，共同协作，才能得以保证。

3.2 与国家网络安全法规、标准结合方面的建议

安全集成服务技术能力建设，必须重视国家网络安全法规、国家和行业相关技术标准。如等级保护制度。等级保护2.0是网络安全的一次重大升级，等级保护对象范围在传统系统的基础上扩展到云计算、移动互联、物联网、大数据等。企业更加需要组织技术人员加强关键基础设施防护、等级保护等相关法规，尤其是国家、行业现行技术标准的培训和学习。在安全集成服务全过程中准确应用相关规范、技术标准。例如需求分析需要关注系统安全保护等级，安全设计引用等级保护基本要求，安全功能方面的设计至少满足相应等级要求，产品和技术的选择满足网络安全审查要求等。

3.3 系统测试能力提升方面的建议

系统测试能力是安全集成服务能力中的一项重要要求。但这个方面往往是企业比较容易忽视或不够重视的。测试能力是一个企业对安全集成结果进行自测的一项技术。加强系统测试能力提升主要可以从三个方面入手，第一人员方面，配置专职的测试人员；第二工具方面，配置专用的测试工具(商用、开源)，并加强对工具的安全管理；第三指导书方面，建立系统测试方面的指导书、测试方案模板、测试计划模板、测试记录模板、测试报告模板等，并能够持续地改进完善。

4 结束语

安全集成服务技术能力本质上是企业所拥有的安全集成技术知识，这些知识附着在人员、设备、信息和组织中。企业安全集成服务能力建设就是需要建立适合企业自身发展的能够不断积累企业知识的长效机制。只有安全集成行业总体能力水平提升，才能更有助于在信息系统建设环节有效提升系统安全建设的水平，才能有效提高信息系统安全防护水平，从而促进国家整体网络安全防护能力的提升。

参考文献

[1] 中国网络安全审查技术与认证中心.CCRC-ISV-C01:2018 信息安全服务规范[S].北京：中国网络安全审查技术与认证中心，2018.

www.pcachina.com

[2] 上海社会科学院信息所.信息安全辞典[M].上海:上海辞书出版社,2013.
[3] 林国恩,李建彬.信息系统安全[M].北京:电子工业出版社,2010.
[4] 冯登国,孙锐,张阳.信息安全体系结构[M].北京:清华大学出版社,2008.
[5] 项目管理协会.项目管理知识体系指南[Z].北京:电子工业出版社,2005.
[6] 国家质量技术监督局.质量管理体系标准[S].北京:中国计量出版社,2001.
[7] 谢宗晓,郭立生.信息安全管理体系应用手册:ISO/IEC 27001 标准解读及应用模板[M].北京:中国质检出版社,2008.
[8] 范红.信息安全风险评估规范国家标准理解与实施[M].北京:中国标准出版社,2008.

(收稿日期:2020-07-02)

作者简介:

翟亚红(1974-),女,本科,高级工程师,主要研究方向:网络安全、安全服务审核等。

吴治(1978-),男,博士,高级工程师,主要研究方向:网络安全、安全服务审核等。

段静辉(1976-),男,博士,高级工程师,主要研究方向:网络安全、安全服务审核等。

(上接第 27 页)

Reasoning with neural tensor networks for knowledge base completion[C]. NIPS, 2013.
[9] BORDES A, USUNIER N, GARC′IA-DUR′AN A, et al. Translating embeddings for modeling multi-relational data[C]. NIPS, 2013.
[10] WANG Z, ZHANG J, FENG J, et al. Knowledge graph embedding by translating on hyperplanes[C]. Proceedings of the Twenty-Eighth AAAI Conference on Artifificial Intelligence, 2014.
[11] LIN Y, LIU Z, SUN M, et al. Learning entity and relation embeddings for knowledge graph completion[C]. AAAI, 2015.
[12] BOUMA G. Normalized (pointwise) mutual information in collocation extraction[C]. Proceedings of the Biennial GSCL Conference, 2009.
[13] BOLLACKER K D, EVANS C, PARITOSH P, et al. Freebase: a collaboratively created graph database for structuring human knowledge[C]. Sigmod Conference. ACM, 2008.

(收稿日期:2020-07-08)

作者简介:

缪琦(1998-),男,本科,主要研究方向:大数据挖掘。

杨昕悦(1996-),女,硕士,主要研究方向:知识图谱。

www.pcachina.com

版权声明

经作者授权，本论文版权和信息网络传播权归属于《信息技术与网络安全》杂志，凡未经本刊书面同意任何机构、组织和个人不得擅自复印、汇编、翻译和进行信息网络传播。未经本刊书面同意，禁止一切互联网论文资源平台非法上传、收录本论文。

截至目前，本论文已经授权被中国期刊全文数据库（CNKI）、万方数据知识服务平台、中文科技期刊数据库（维普网）、JST 日本科技技术振兴机构数据库等数据库全文收录。

对于违反上述禁止行为并违法使用本论文的机构、组织和个人，本刊将采取一切必要法律行动来维护正当权益。

特此声明！

《信息技术与网络安全》编辑部

中国电子信息产业集团有限公司第六研究所