

中国计算机审计研究报告

中国审计学会计算机审计分会

2016

信息系统审计 法规知识选编(下)

REPORT SERIES OF
IT AUDIT RESEARCHES IN CHINA

中国审计学会计算机审计分会
《信息系统审计法规知识选编》课题组



中国时代经济出版社

中国计算机审计研究报告

中国审计学会计算机审计分会

2016
1302.27
5
12

信息系统审计 法规知识选编 (下)

REPORT SERIES OF
IT AUDIT RESEARCHES IN CHINA

中国审计学会计算机审计分会
《信息系统审计法规知识选编》课题组

 中国时代经济出版社

图书在版编目 (CIP) 数据

信息系统审计法规知识选编: 全2册 / 《信息系统
审计法规知识选编》课题组编. —北京: 中国时代
经济出版社, 2016. 6

ISBN 978 - 7 - 5119 - 2563 - 3

I. ①信… II. ①信… III. ①信息系统—审计法—基
本知识—中国 IV. ①D922. 27

中国版本图书馆 CIP 数据核字 (2016) 第 070852 号

书 名: 信息系统审计法规知识选编 (全2册)

作 者: 《信息系统审计法规知识选编》课题组

出版发行: 中国时代经济出版社

社 址: 北京市丰台区玉林里 25 号楼

邮政编码: 100069

发行热线: (010) 63508271 63508273

传 真: (010) 63508274 63508284

网 址: [www. cmepub. com. cn](http://www.cmepub.com.cn)

电子邮箱: [sdjj1116@163. com](mailto:sdjj1116@163.com)

经 销: 各地新华书店

印 刷: 北京市荣海印刷厂

开 本: 787 × 1092 1/16

字 数: 870 千字

印 张: 51

版 次: 2016 年 6 月第 1 版

印 次: 2016 年 6 月第 1 次印刷

书 号: ISBN 978 - 7 - 5119 - 2563 - 3

定 价: 135.00 元

本书如有破损、缺页、装订错误, 请与本社发行部联系更换

版权所有 侵权必究

目 录

(下 册)

第三章 信息系统应用控制审计法规知识	(413)
第一节 应用系统架构审计	(413)
(一) 电子政务总体设计	(413)
214. 电子政务顶层需求分析	(413)
215. 电子政务系统总体设计	(417)
216. 电子政务体系结构	(419)
217. 电子政务业务流程设计	(423)
218. 业务要素特征应用架构	(424)
(二) 信息化应用架构审计	(425)
219. 中央跨部门共建项目应用架构	(425)
220. 政务信息系统技术支撑规范	(426)
221. 政务信息系统应用架构	(437)
222. 企业信息系统应用架构	(440)
223. 电子商务信息系统应用架构	(442)
224. 应用系统技术架构	(444)
225. 应用系统集约化架构	(451)
226. 应用架构控制审计	(455)
第二节 应用系统控制审计	(457)
(一) 业务控制审计	(457)
227. 业务流程控制审计	(457)
228. 应用输入控制	(458)
229. 应用处理控制	(458)
230. 应用输出控制	(459)

(二) 应用软件规范控制	(460)
231. 软件立项控制	(460)
232. 软件需求控制	(462)
233. 软件开发控制	(468)
234. 软件设计控制	(468)
235. 数据库设计控制	(470)
(三) 应用功能控制审计	(473)
236. 数据输入控制审计	(473)
237. 数据处理控制审计	(475)
238. 数据输出控制审计	(477)
第三节 信息资源建设管理	(479)
(一) 政务信息资源目录体系	(479)
239. 政务信息资源目录体系总体框架	(479)
240. 政务信息资源目录体系技术要求	(483)
241. 政务信息资源核心元数据	(485)
242. 政务信息资源分类	(494)
243. 政务信息资源技术管理要求	(505)
(二) 政务信息资源交换体系	(507)
244. 政务信息资源交换体系总体框架	(507)
245. 政务信息资源交换体系技术要求	(509)
246. 政务信息资源交换体系数据接口规范	(513)
247. 政务信息资源交换体系技术管理要求	(519)
248. 电子政务主题词表编制规则	(524)
(三) 会计核算软件数据接口国家标准	(532)
249. 企业会计核算软件数据接口国家标准	(532)
250. 行政事业单位会计核算软件数据接口国家标准	(532)
251. 总预算会计核算软件数据接口国家标准	(533)
252. 商业银行会计核算软件数据接口国家标准	(533)
253. 企业资源计划软件数据接口国家标准	(534)
(四) 行业信息资源规范	(536)
254. 国家审计信息化数据规划	(536)
255. 国家审计计算机审计方法体系	(540)

第四节 信息共享业务协同	(543)
256. 政府信息公开	(543)
257. 政务部门信息共享	(544)
258. 信息共享协同审计	(546)
259. 业务协同控制审计	(547)
260. 信息公开的监督	(548)
第四章 信息系统网络控制审计法规知识	(550)
第一节 网络规划控制审计	(550)
(一) 电子政务网络规划	(550)
261. 国家电子政务网络规划	(550)
262. 国家政务外网网络架构	(551)
263. 电子政务网互联互通架构	(553)
264. 电子政务网络建设标准	(553)
265. 综合布线工程设计规范	(569)
266. 路由器安全技术要求	(570)
(二) 政务网络规划审计	(576)
267. 不再审批新建专用网络	(576)
268. 网络结构控制审计	(577)
269. 网络外部连接审计	(579)
270. 网络运行状况审计	(581)
271. 网络设备配置审计	(581)
272. 网络结构控制常见问题	(582)
第二节 存储处理控制审计	(583)
(一) 存储处理系统	(583)
273. 不同结构的存储系统	(583)
274. 存储方式与技术路线	(584)
275. 不同存储方式的控制	(586)
(二) 备份恢复系统	(588)
276. 备份与灾难恢复规范	(588)
277. 灾难恢复	(589)
278. 灾难恢复需求的确定	(591)
279. 灾难恢复策略的制定	(592)

280. 灾难恢复策略的实现	(595)
第三节 机房系统控制审计	(599)
281. 机房设备布置规定	(599)
282. 电子计算机场地组成	(599)
283. 机房承重结构控制	(601)
284. 建筑物电子信息系统防雷	(602)
285. 机房供配电系统控制	(606)
286. 低压配电设计	(608)
287. 机房消防系统控制	(608)
288. 机房空气调节系统控制	(610)
289. 机房电气技术控制设计规范	(613)
290. 机房监控和安全防范控制	(617)
291. 机房给水排水系统控制	(618)
292. 机房电磁屏蔽设计规范	(619)
第五章 信息系统安全控制审计法规知识	(621)
第一节 信息安全等级保护	(621)
（一）信息安全等级保护制度	(621)
293. 信息安全等级保护的职责	(621)
294. 信息安全等级划分与保护	(622)
295. 信息安全等级保护的实施	(623)
296. 信息安全等级保护备案	(624)
297. 信息安全等级保护产品选择	(626)
298. 信息安全等级保护测评	(627)
299. 信息安全等级保护整改	(628)
300. 信息安全等级保护整改指南	(629)
301. 信息安全技术体系建设总体要求	(631)
302. 电子政务项目安全可控	(632)
（二）信息安全风险评估制度	(632)
303. 信息安全风险评估	(632)
304. 风险评估整改	(634)
305. 信息安全残余风险评估与应对	(634)
306. 信息系统安全性审计	(635)

第二节 信息安全等级保护管理体系	(639)
(一) 安全管理机构	(639)
307. 安全管理机构岗位设置	(639)
308. 安全人员配备	(640)
309. 授权与审批	(641)
310. 检查沟通与合作	(642)
311. 审核和检查情况	(643)
(二) 安全管理制度	(644)
312. 建立完善信息安全管理制度的	(644)
313. 管理制度的制定与发布	(646)
314. 管理制度的评审与修订	(647)
(三) 人员安全管理	(648)
315. 人员录用	(648)
316. 人员离岗	(649)
317. 人员考核	(650)
318. 安全意识教育与培训	(650)
319. 外部人员的访问管理	(652)
(四) 系统建设安全管理	(652)
320. 信息系统安全定级	(652)
321. 信息系统安全方案设计	(655)
322. 信息安全产品采购与使用	(656)
323. 自行开发信息系统建设	(658)
324. 外包软件开发	(659)
325. 信息系统建设工程实施	(660)
326. 信息系统建设工程测试验收	(661)
327. 信息系统交付	(663)
328. 信息系统备案	(664)
329. 信息系统安全等级测评	(665)
330. 信息系统安全服务商选择	(667)
(五) 系统运维安全管理	(668)
331. 环境管理	(668)
332. 资产管理	(669)

333. 介质管理	(671)
334. 设备管理	(672)
335. 监控管理和安全管理中心	(674)
336. 网络安全管理	(675)
337. 系统安全管理	(676)
338. 恶意代码防范管理	(678)
339. 密码管理	(680)
340. 变更管理	(681)
341. 备份与恢复管理	(682)
342. 安全事件处置	(684)
343. 应急预案管理	(686)
第三节 信息安全等级保护技术体系	(687)
(一) 物理安全控制	(687)
344. 物理位置选择	(687)
345. 物理访问控制	(688)
346. 防盗窃和防破坏	(689)
347. 防雷击	(690)
348. 防火	(691)
349. 防水和防潮	(692)
350. 防静电	(693)
351. 温湿度控制	(693)
352. 电力供应	(694)
353. 电磁防护	(695)
(二) 网络安全控制	(695)
354. 网络结构安全	(695)
355. 网络访问控制	(697)
356. 网络安全审计	(698)
357. 网络边界完整性检查	(699)
358. 网络入侵防范	(700)
359. 恶意代码防范	(701)
360. 网络设备防护	(701)
(三) 主机安全控制	(703)

361. 主机身份鉴别	(703)
362. 主机安全标记	(705)
363. 主机访问控制	(705)
364. 主机可信路径	(706)
365. 主机安全审计	(707)
366. 主机剩余信息保护	(708)
367. 主机入侵防范	(709)
368. 主机恶意代码防范	(710)
369. 主机资源控制	(711)
(四) 应用安全控制	(712)
370. 应用程序身份鉴别	(712)
371. 应用程序安全标记	(713)
372. 应用程序访问控制	(713)
373. 应用程序可信路径	(715)
374. 应用程序安全审计	(715)
375. 应用程序剩余信息保护	(716)
376. 应用程序通信完整性	(717)
377. 应用程序通信保密性	(717)
378. 应用程序抗抵赖	(718)
379. 应用软件容错	(719)
380. 应用程序资源控制	(720)
(五) 数据安全控制	(721)
381. 数据完整性	(721)
382. 数据保密性	(722)
383. 数据备份与恢复	(722)
(六) 安全等级保护整改	(724)
384. 等级保护整改工作要求	(724)
385. 等级保护整改目标和内容	(725)
386. 等级保护整改流程和目标	(726)
387. 等级保护管理整改	(728)
388. 安全技术措施	(729)
389. 网络交换机安全技术要求	(730)

390. 防火墙安全技术要求	(732)
(七) 安全等级保护标准	(736)
391. 安全等级保护 4 类标准	(736)
392. 安全保护等级划分标准说明	(739)
393. 安全等级保护基本要求说明	(740)
394. 安全等级保护实施指南说明	(743)
395. 安全等级保护定级指南说明	(745)
396. 安全等级保护管理要求说明	(747)
397. 安全等级保护通用安全技术标准说明	(750)
398. 安全等级保护安全设计技术要求说明	(751)
399. 安全等级保护安全工程管理要求说明	(753)
400. 安全等级保护测评要求说明	(756)
401. 安全等级保护测评过程指南说明	(757)
第四节 信息安全国家标准	(760)
402. 网络通信的信息安全技术要求	(760)
403. 信息技术设备安全	(760)
404. 服务器安全技术要求	(761)
405. 安全审计要求	(763)
406. 备份与故障恢复	(766)
407. 数据安全	(767)
408. 数据库安全	(773)
第五节 信息系统安全法律责任	(774)
409. 违反信息安全等级保护的法律责任	(774)
410. 违反信息系统安全保护的法律责任	(775)

第三章 信息系统应用控制审计法规知识

第一节 应用系统架构审计



(一) 电子政务总体设计

214. 电子政务顶层需求分析

2007 年 9 月,《电子政务系统总体设计要求》(GB/T 21064—2007):

5 系统总体设计要素

5.1 需求分析

5.1.1 业务组织结构

业务组织结构将标识出系统的使用者,是业务功能的部属单位。对业务系统中所涉及的组织结构的分析应包括组成范围、工作职责及各组织单元之间的关系。

5.1.2 系统业务功能

系统业务功能是系统能力的重要体现,是用户直接可见的部分,也是系统分析设计的基础。

系统业务功能要素中包括系统应具有的各项功能要求、业务流程以及系统的处理范围,说明如下:

a) 将功能分类,形成功能集合或功能子系统,并逐步整理各项功能,分类方法可以组织结构或功能的关联性为依据;

b) 按业务流程表述业务与人的信息、处理的过程、所需的数据、涉及的角色以及输出的结果;

c) 通过上述分析,确定系统的处理范围,标识出系统具有的功能以及

涉及的外部角色，外部角色可以是外部系统、各种类型用户或外部设备。

5.1.3 部门业务关系

通过对业务流程的分析，明确部门间的业务协同关系。部门间的协同关系主要表现为指示与汇报、请求与服务、信息共享与交换。应给出协同业务名称、协同类型、协同发起部门、协同响应部门以及协同描述等，说明如下：

- a) 协同业务名称，标识各协同关系；
- b) 协同类型，如指示与汇报、请求与服务、信息共享与交换等；
- c) 协同发起部门，即服务的请求方、信息的发送或提供方；
- d) 协同相应部门，即服务的响应方、信息的接收或读取方；
- e) 协同描述，从业务应用的角度简要描述服务的内容或共享信息的作用。

5.1.4 系统信息资源

全面分析系统引入或产生的信息资源，包括信息资源清单、数据描述、接口要求、数据流程及信息管理要求等，说明如下：

- a) 信息资源清单，包括信息资源名称、分类、来源及主要用途等；
- b) 数据描述，对主要数据内容进行简要描述，包括名称、数据类型、格式、单位、范围等，可引用其他文档（如：数据字典、通信协议标准、用户接口标准）；
- c) 接口要求，包括信息传输、WEB 页面、API 调用等接口方式及限定条件；
- d) 数据流程，包括系统对引入信息的数据使用过程，以及系统产生信息的数据加工过程；
- e) 信息管理要求，包括信息的采集、更新，管理的职责、方式和要求。

5.1.5 安全保密要求

系统的安全保密遵循电子政务保密标准体系的要求，应包括以下几个方面：

- a) 系统安全要求；
- b) 信息安全等级要求；
- c) 系统容灾备份要求；
- d) 系统应急使用要求；
- e) 系统使用限定；
- f) 数据存储与传输的保密约束。

5.1.6 系统性能要求

5.1.6.1 性能指标

系统性能将影响系统使用的效果、系统资源的需求和系统设计的策略，应给出明确的性能指标规定。系统性能包括系统工作效率指标、信息共享能力、信息维护能力、系统使用能力等，说明如下：

- a) 系统工作效率指标，可包括系统启动时间、各种响应时间、业务周转时间等；
- b) 信息访问能力，可包括信息访问最大用户数、信息交互用户数等；
- c) 信息维护能力，可包括信息的准确率、完整率、更新周期、更新及时率等；
- d) 系统使用能力，可包括持续使用时间、容量、吞吐量或速率等。

5.1.6.2 性能指标详细说明

性能指标的详细说明如下：

- a) 启动时间，即启动系统或应用所需的时间；
- b) 响应时间，即系统响应一项规定的操作所需的实践，可包括平均响应时间和最大响应时间；
- c) 周转时间，即从发出一条指令开始到一组相关的功能完成，所经历的等待时间，可包括平均周转时间和最大转轴时间；
- d) 信息访问最大用户数，即允许对系统同时进行信息访问的最大用户数量；
- e) 信息交互用户数，即发生信息交互关系的用户数量；
- f) 信息准确率，即信息正确的项数与信息总项数之比；
- g) 信息完整率，即信息已采集项数与应采集项数之比；
- h) 信息更新周期，即需随时间变化的信息对其进行修改的时间间隔；
- i) 信息更新及时率，即在规定的周期内及时更新的项数与需更新总项数之比；
- j) 可持续使用时间，即保持连续不断使用的最短时间；
- k) 容量，如允许用户数、数据存储量、信道容量等；
- l) 吞吐量或速率，即在给定的实践周期内成功执行的数量。

5.1.7 系统设施与环境要求

5.1.7.1 系统设施要求

系统设施要求包括使用或引入到系统中的硬件、软件及系统设备连接方

式要求。对系统设施进行规划的依据是系统业务功能、系统信息资源、安全保密要求及系统性能要求，应指明它们之间的导出关系。

a) 系统使用或引入到系统中的硬件要求，包括：

- 1) 计算机与服务器；
- 2) 输入/输出及存储设备；
- 3) 网络与通信设备；
- 4) 自动服务设备；
- 5) 其他所需的设备。

应给出每种设备的类型、数量、特征及能力要求。

b) 系统使用或引入到系统中的软件要求，包括：

- 1) 操作系统、数据库管理系统；
- 2) 通信及网络软件；
- 3) 实用软件；
- 4) 输入和设备模拟器；
- 5) 测试软件等。

需要时可提出系统物理连接方式要求，包括连接的地理位置、设备配置和网络拓扑结构、网关等。

5.1.7.2 系统环境要求

系统运行必需的环境要求包括系统在运输、存储、操作过程中必须经受的环境条件，如：

- a) 自然环境条件，风、雨、温度、湿度、烟雾等；
- b) 诱导环境，运动、撞击、噪音、电磁辐射等。

对于车载式、活动式系统或基础设施类系统必须提出系统环境要求。

5.1.8 系统质量要求

系统质量方面的要求包括以下内容：

- a) 适应性要求，系统运行所依赖的数据环境（如现场的位置、数据记录的参数等）；
- b) 可重用性要求，可被多个应用使用的要求；
- c) 可靠性要求，系统不发生故障及故障发生后的处置要求；
- d) 维护性要求，发生问题后易于改正的要求；
- e) 可移植性要求，易于改进以适应新环境的要求；
- f) 易用性要求，易于学习和使用的要求。

5.1.9 标准与规范要求

为了使系统符合电子政务整体框架的要求并能有机集成,必须规定应遵循的技术标准体系,如工程管理、网络建设、信息共享、支撑技术、信息安全等方面的标准化要求。

在规定通用标准和规范的同时还需规定特殊体系结构的约束(必须采用标准构件、已有构件或用户提供的构件)、特殊设计或实现标准的实用要求。

5.1.10 系统验收要求

应规定系统验收时的接收条件和检验方法,确保系统建设的质量。

a) 系统接收条件可包括:

- 1) 通过具有认证资格的第三方测评;
- 2) 通过一定周期的典型用户试用;
- 3) 通过规定周期的系统试运行;
- 4) 通过制定级别的评审或审查。

b) 再进行测评、试用、试运行、评审或审查时,可采用以下检验方法:

- 1) 演示:运行依赖于课件的功能操作的系统或部分系统,不需要使用仪器、特殊的测试设备或进行事后分析;
- 2) 检测:使用仪器或其他特殊的检测设备运行系统或系统的组成部分,以便采集数据供事后分析使用;
- 3) 分析:对从其他检验方法中获得的积累数据进行处理,例如测试结果的归纳、解释、推断;
- 4) 审查:对系统构件、文档等进行可视化检查;
- 5) 特殊的检验方法:系统的任何特殊合格性方法,如特殊工具、技术、过程、设施、验收限制及标准样例的使用。

215. 电子政务系统总体设计

2007年9月,《电子政务系统总体设计要求》(GB/T 21064—2007):

5 系统总体设计要素

5.2 系统体系结构设计

5.2.1 技术体系框架

信息系统涉及网络、通信、计算机、系统软件、应用软件等各种相关技术,技术体系框架从总体上描述不同类型技术构建信息系统的规则和方法,标识出各服务领域及其接口,实现开放系统的分离原则。技术体系框架需要

反映以下一些共性内容：

- a) 服务领域的层次结构；
- b) 服务领域的主题内容与组成；
- c) 服务领域之间的相互关系；
- d) 与外部的接口。

5.2.2 系统设计策略

系统设计策略指为达到系统性能、安全保密能力以及为提供所需的可靠性、可重用性、维护性和可移植性等质量特性而选择的方法，或关键技术实现及其他影响系统组成成分的设计决策。这些策略是系统设计必须遵循的原则，在进行系统总体设计时应首先确定。给出设计策略的同时还需说明设计策略与依据的需求之间的符合性。

系统设计策略一般应包括：

- a) 性能实现设计策略；
- b) 安全保密设计策略；
- c) 可靠性设计策略；
- d) 质量特性实现设计策略；
- e) 关键技术设计策略等。

5.2.3 系统构成

对系统进行分解，划分为若干子系统或硬件构件和软件构件，并将系统功能、性能等需求逐步落实到每个子系统或构件中，分解后的构件存在着关联关系，确定系统组成时应明确以下内容：

- a) 子系统或硬件构件和软件构件的构成及其功能；
- b) 构件间的静态关系、关系的种类及必要说明；
- c) 系统构建的获取途径，如新开发的构件、重用的构件、集成的构件、采购的构件等。

5.2.4 系统运行模式

系统运行模式从技术角度反映目标系统的运转方式。构件之间的运行模式是构件之间的动态关系，如执行控制流、数据流、动态控制序列、状态关系、时序关系、中断处理、异常处理、并发执行等。运行模式可包含以下内容：

- a) 系统初始化模式；
- b) 系统管理模式；