了解信息技术导致的风险以及被审计单位的应对

（来源：《中国注册会计师》， 2018-03-29）

【编者按】在信息化环境下，企业运用信息技术编制财务报表，设计和执行内部控制。注册会计师在对企业的财务报表进行审计时，必须考虑信息技术的影响。同时，信息化也对注册会计师的审计技术和方法带来革命性变化。为了帮助注册会计师应对信息化带来的挑战，中国注册会计师协会资助普华永道中天会计师事务所研究编写了《信息系统环境下的财务报表审计》一书，即将出版。本刊约请作者加以摘编，分期连载，以飨读者。

如果说注册会计师了解被审计单位的信息技术环境以及与财务报告相关的信息系统，目的是为了对被审计单位的信息技术使用情况进行摸底，进而获得与被审计单位信息技术使用与财务报表相关性有关的信息。那么，了解信息技术导致的风险及应对就是为了评估被审计单位的信息技术是否处于一个可控的状态，相关的应对（控制）体系是否已经建立健全，以帮助企业应对相关信息技术风险，为审计策略的选择和审计范围的确定提供依据。

了解被审计单位的信息技术整体环境是对企业信息系统整体管理体系中的相关风险点的识别及应对机制，这一部分是注册会计师了解信息技术导致的风险及被审计单位应对的重要组成部分，对其他具体的信息技术风险及应对有着宏观引导作用，是其他具体的信息技术风险存在和应对的背景和大环境。本文着重讲解企业使用信息技术导致的具体风险及应对体系。

一、了解被审计单位信息技术导致的风险

一般而言，企业通常遇到的与财务报告编制相关的典型信息技术导致的风险包括但不限于以下方面：

1. 程序或数据的访问没有受到合理限制；

2. 自动控制或程序没有合理设计或有效运行；

3. 报表没有被合理设计或有效运行；

4. 对数据的非授权访问；

5. 数据丢失或损坏；

6. 交易处理过程中的错误没有被更正或识别。

以上是一些常见的信息技术导致的风险举例，普遍适用于各个行业的企业。需要说明的是，以上列出的这 6 类风险点是我们在信息技术导致的风险中比较常见的风险，这里并未穷尽所有信息技术导致的风险。注册会计师需要在审计项目中针对各个项目分别进行风险评估和识别工作，以确保审计工作的效率和效果。

注册会计师在进行被审计单位信息技术整体环境的了解过程中，就要有意识的开始进行风险点相关性的识别工作，了解哪些风险类别是和被审计单位相关的风险，哪些是不相关的风险。然后才能针对识别的相关风险评估应对体系，有效的开展审计工作，避免过度审计或审计不足。

二、关于被审计单位信息系统相关风险的应对体系

为了应对上述识别出的信息技术导致的风险，被审计单位通常会从组织架构、人员、技术、流程和程序等方面来进行应对，即设计一套控制体系来应对相应的风险。虽然具体的控制活动根据被审计单位实际情况可能千差万别，但是控制的目的都是为了应对相关的信息技术导致的风险。通常情况下，以被审计单位信息技术整体控制环境为大背景，被审计单位在信息技术导致的风险应对方面的具体控制体系包括信息系统一般控制和应用控制。

（一）信息系统一般控制

如果把某一信息系统比喻为一个机器人，这个机器人根据其设定的程序进行的日常活动即我们所见的业务层面操作/控制（IT Dependencies），这些活动直接或间接的对机器人是否能实现预定的操作目标产生影响。那么，如何保证这个机器人能够按我们所设定的程序进行日常活动？这就必须要使得机器人的制造、更新、维护、访问控制这 4 个环节/方面得到有效的保证。

首先，机器人是按照预设需求制造的，比如我们要制造一个具有清洁功能的机器人，只有把控生产制造环节，才能保证制造出预设功能，而不是其他功能的机器人；同时，由于需求在不断地发生变化，要保证机器人能够不断满足我们的需求变化，我们需要对机器人进行升级或者是修复，从而使其功能与时俱进；另外，在机器人日常运作过程中，我们需要对它是否按正确的方式进行了工作，如果出现了问题怎么处理等进行日常的维护，保证其持续有效地按我们要求的方式活动等，这就是我们日常维护所要关注和保证的事情；最后，也是最重要的，对这个机器人，谁可以操作和改造它，就涉及到一个访问控制的问题，如果随随便便任何人都可以进入其的核心程序对其进行改造，很可能这个产品可能就功能紊乱了，所以把握访问控制是至关重要的。这几个方面就确保了一个按我们所需方式制造、维护、升级和使用的产品。

与之类似，信息系统一般控制就是合理保证系统持续有效地按照我们要求的方式进行运作的一套控制体系。机器人运转原理的制造、更新、维护和访问控制对应到的就是我们信息系统一般控制的系统建设、系统变更、系统日常运行维护、程序和数据的访问四大领域的话题。这四大领域是信息系统最基础也是最核心最为重要的环节，虽然对于业务部门和财务部门来说，可能对这四大领域没有太多感性的认

识，但是，正是这四大领域的存在，才为系统在业务层面支持业务流程奠定了坚实的基础。如果说业务流程层面的自动化流程和控制是信息系统的外延，那么基础层面的信息系统一般控制是信息系统的内核。

根据《中国注册会计师审计准则第 1211 号——通过了解被审计单位及其环境识别和评估重大错报风险》及其应用指南，信息技术一般控制是与多个程序相关且支持应用控制有效运行的政策或程序，应用于主机、小型机和终端用户环境。保证信息完整性和数据安全性的信息技术一般控制通常包括：

1. 数据中心和网络运行控制；
2. 系统软件的购置、修改及维护控制；
3. 程序修改控制；
4. 接触或访问权限控制；
5. 应用系统的购置、开发及维护控制。

上述五项信息技术一般控制分别对应我们所阐述的信息系统一般控制的四大领域，即：

1. 系统日常运行维护；
2. 系统变更；
3. 程序和数据的访问；
4. 系统建设。

在信息系统审计规划阶段，注册会计师仅需要对被审计单位在以上领域的控制活动进行了解，获知被审计单位是否存在相关控制活动，以此为基础制定审计策略，详细的信息系统一般控制审计执行（如果注册会计师决定测试相关控制），将在审计执行阶段完成。

信息系统一般控制为信息系统按照管理预期正常运转的基本控制，为运行其上的应用控制的持续有效性提供保障。正是由于信息系统一般控制的基础性和内核性，信息系统一般控制在审计中具有以下局限性：

1. 信息系统一般控制通常不能直接预防或发现重大错报；

2. 信息系统一般控制通常不能直接对特定财务报表项目认定提供直接证据；

3. 有效的信息系统一般控制本身并不能得出应用控制的可靠性。

（二）信息系统应用控制

信息系统应用控制为业务的持续有效运行和财务报表的编制提供直接或间接基础和支持。每个企业在各个业务流程的应用控制千差万别，需要在财务报表审计过程中，从每个财务报表科目余额或交易的重大财务错报风险出发，在业务流程中识别是否有相关的系统支持存在。即在了解与财务报告有关的信息系统中所提到的对被审计单位对信息技术的依赖领域（IT dependencies）：

1. 系统自动化控制；

2. 系统生成的报表/信息；

3. 系统自动计算；

4. 系统权限管理和职责分离；

5. 系统之间的自动化接口。

我们可以通过一张图来说明财务报表与信息系统风险应对体系的关系。以便于我们更清楚的理解各个部分之间的依赖和支持关系。

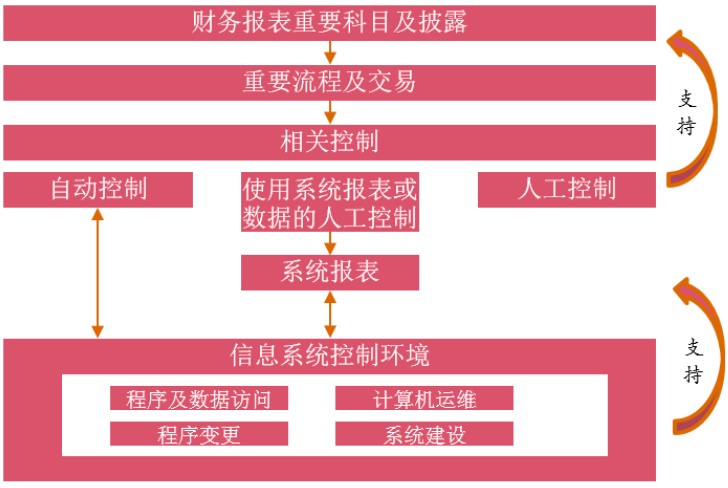

图 1　财务报表与信息系统之间的关系

简言之，财务报表、应用控制和信息系统一般控制之间的关系可以描述为：财务报表形成于各个业务流程和交易过程；而自动控制、依赖于系统的人工控制、及不依赖系统的人工控制这些业务层面的控制活动保证了流程和交易的按我们预期的方式运行；为了保证业务层面的系统相关控制活动（自动控制和依赖于系统的人工控制）的持续有效的运行，信息系统一般控制从建设、变更、运维和访问四个领域提供了坚强有力的保证。

需要说明的是，在审计计划阶段，注册会计师对于信息系统整体控制环境、一般控制和应用控制的了解是对被审计单位及其环境的了解，目的是为了评估被审计单位是否存在系统运行的健康可控的大环境、是否存在支持财务报表的应用控制、是否存在支持信息系统应用控制的信息系统一般控制，从而帮助注册会计师制定审计策略。即，注册会计师在审计规划阶段需要了解清楚被审计单位信息系统相关风险及其应对体系。

从前面的讲解中，我们将企业的信息系统风险及应对体系的关系表示如下：

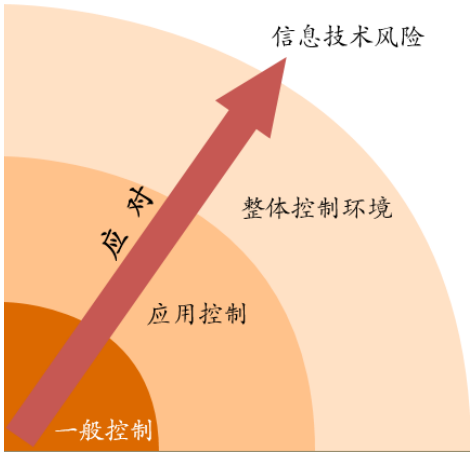

图 2　信息技术使用导致的风险及应对体系

其中，信息系统整体控制环境是控制体系存在的大背景，决定了管理的基调和健康程度；应用控制体系是风险应对体系中直接对业务

流程进行有效支撑的保证；信息系统一般控制是风险应对体系的基础和内核，为应用控制体系的稳健持续有效运行提供保证。三层应对体系共同构成了企业信息技术风险应对的控制体系，三者缺一不可。

在审计规划阶段，对于被审计单位信息系统整体控制环境、一般控制和应用控制的了解，注册会计师通常通过访谈和查看等方式获得相关信息。除非有特殊必要，一般不在审计计划初始阶段对其进行的详细测试工作。对于信息系统一般控制和应用控制的进一步测试工作，将在审计执行阶段进行介绍。

（三）关于信息系统风险的一些常见问题解答

问题一：企业对使用信息系统所带来风险的应对体系与企业内部控制体系之间是什么关系？

答：企业对使用信息系统所带来的风险的应对体系分为三个层面：一个是信息技术整体（控制）环境，是信息技术使用和管理的大环境及基调；一个是业务层面，即我们通常所说的应用控制体系；一个是基础层面，即我们通常所说的信息系统一般控制体系。企业的内部控制体系是企业实现全面风险应对的全面控制体系。前者是后者的有机组成部分，并伴随着企业信息化程度的提升而在内控体系中的地位日益重要，占比日益提升。

问题二：信息系统一般控制和应用控制的实现方式都是自动的吗？

答：不一定。

内部控制的实现方式分为两大类：系统自动实现的自动控制（automatic controls）和人工方式实现的人工控制（manual control）。其中，人工控制又分为纯粹的不依赖系统数据或信息的人工控制和依赖于系统数据或信息的人工控制（IT-dependent manual control）。

信息系统一般控制是对信息系统的建设、变更、访问及运行维护相关风险的应对控制体系。这些控制活动的实现方式可能是系统自动实现的自动控制，例如通过SVN服务器实现变更程序的版本控制；也可能是人工方式实现的人工控制，例如系统中对于账号权限申请的书面审批控制；也可能是基于系统数据而进行的人工控制，例如，相关人员对于系统账号权限的定期复核控制。

应用控制是对业务流程支撑的过程中，依托系统相关的信息或数据所实现的相关控制。具体包括系统自动控制、自动计算、报表和系统数据、系统权限及职责分离和接口。其中，自动控制、自动计算和报表数据通常通过系统自动方式实现，为自动控制；系统权限及职责分离和接口通常是通过自动或者是依赖于系统人工的方式实现。

因此，信息系统一般控制和应用控制不一定全部是自动控制，一般情况下是各种控制实现方式的组合。

（文章链接：http://www.cicpa.org.cn/pdfflash/201803.html，转载请注明。）