

# 浙江省服务贸易协会

## 信息简报

Zhejiang Association of Trade in Services

2014年11月 ◆ 总第33期

### 2015年度服务贸易展会计划表

展会报名端口 <http://www.zats.cn>

点击菜单栏的最后项“报名回执”，选择您感兴趣的展会。

[设为首页](#)  
[加入收藏](#)  
[联系我们](#)

[无形贸易交易平台](#) [协会论坛](#) [会员登录](#) [报名回执](#)

[进出口合同登记](#) | [境内举办对外经济技术展览会许可系统](#)

注意事项：

- 1、部分会展的“报名入口”需要收到密码的企业才能填报
- 2、认真填写，表格无法修改
- 3、地址栏非常重要，填写错误会导致发票无法投递
- 4、“添加人员信息”完成后，请务必点击“完成”按键
- 5、请按照各类会展的简介或文件所示缴费。汇款时注明参加的会展及费用类别（摊位费、



会务费等)

如果代收费方为“浙江省服务贸易协会”，账号及开户行为：376659185457 中国银行浙江省分行

6、请在报名后的第二天点击“已报名清单”查询是否报名成功（增加中……）联系电话：0571-89703132 邮箱：zats2010@126.com

序号	展会名称	城市	时间	展出内容	主办方
1	2015年澳大利亚信息通信技术物流展览会 CeBIT & CeMAT Australia	悉尼	5月5日-7日	信息通信交换、传输技术与设备，通信终端设备、物料搬运及装载设备、仓储设备、物流技术	汉诺威（澳大利亚）展览公司
2	亚洲通讯展 (COMMUNIC ASIA)	新加坡	6月2-5日	信息通信交换、传输技术与设备，通信终端设备等	新加坡资讯通信发展管理局及新加坡媒体发展管理局
3	2015年台北国际电脑展	台湾.台北	6月2日-6日	各类电脑相关及消费性电子软件、硬件、周边设备、零部件、通信器材及网络产品等	台湾对外贸易发展协会
4	2015年第七届巴西国际通讯电子展	巴西.圣保罗	8月25日-27日	各类电脑相关及消费性电子软件、硬件、周边设备、零部件、通信器材及网络产品等	巴西 ARANDA 展览协会
5	俄罗斯通讯展 (SVIAZ EXPO COMM MOSCOW )	莫斯科	5月12-15日	信息通讯	美国克劳斯展览公司及俄罗斯通讯部
6	日本IT展 (JAPAN IT WEEK)	东京	5月13-15日	IT类	日本励展展览公司

7	GARTNER 外包峰会暨展会	佛罗里达	10月5-9日	服务外包	美国 GARTNER 集团
8	德国慕尼黑国际物流及交通运输博览会	慕尼黑	5月5-8日	物流行业相关信息 通讯、电子商务及数据处理	广州搏毅展览有限公司
9	法国戛纳春季/秋季电视节 ( MIPTV/ MIPCOM )	戛纳	4月13-16日/10月13-16日	影视交易	励展集团
10	美国 E3 游戏展	洛杉矶	6月7-9日	游戏类内容	美国娱乐软件协会 ( ESA )
11	日本东京游戏展	东京	9月17-20日	游戏类内容	日本计算机娱乐供货商协会
12	亚洲电视论坛暨影视节目交易展览会( ATF )	新加坡	12月4-6日	影视交易	励展集团
13	第四届中国 ( 北京 ) 服务贸易交易会	北京	5月28—6月1日	服务贸易展示、洽谈和交易	商务部
14	第十三届中国 ( 大连 ) 软件和信息服务交易会	大连	6月18—21日	IT 软件洽谈和交易	商务部
15	第三届中国 ( 上海 ) 国际技术进出口交易会	上海	4月24—26日	技术进出口洽谈和交易	商务部
16	第十二届中外货代物流洽谈会	广州 ( 暂定 )	11月	中外货代和物流一对一洽谈	中国国际货运代理协会

# 国际认证

应会员单位要求，简报增加“国际认证栏目”，并提供协助会员联系权威认证机构的服务。

## ISO27001 标准简介

### 一、信息安全管理概况

在信息及其处理设备高度发达的今天，信息安全的重要性已被充分肯定。

但是，我们仍旧可以听到来自世界各地的信息安全问题：政府网络被黑客轻而易举地进入，公司机密信息出现在报纸上或被人在垃圾桶中发现，财务信息被公布在网站上让所有人浏览，银行资产通过网络系统流向黑客的钱袋……

不管您的组织是怎样的性质，您都不会希望价格表，客户信息，调研信息，市场策略、标书底价、产品研发成果等落入别有用心之人的手中。许多组织发现重要资料泄露的时候已造成了不可挽回的损失，这时候才认识到那看似完美的信息安全防护系统远远达不到专业水平，而且漏洞百出。

在意识到信息的力量、价值及保护信息的重要性后，ISO27001（信息安全管理体系）已经被越来越多的组织认可。该标准提供了一个完整的切入、实施、维护和文件化组织内部的信息安全的框架。

### 二、什么是 ISO 27001 信息安全管理体系

ISO27001 信息安全管理标准要求建立一个完整的信息安全管理体系。该管理体系在组织中建立一个完整的切入、实施、维护和文件化的管理框架。该管理标准提供给组织信息安全管理最佳实践指导。

ISO27001 是组织一个关键的管理工具，它可以用来识别管理和减小对组织信息安全的威胁。企业的信息如产品定价、客户信息、研究成果、市场开发计划或发展战略等是企业赖以生存的宝贵财富。当一个组织与另一个组织合作的时候，对信息的保护尤为重要。当您的组织要把保密的信息与另一组织分享的时候，您应当肯定对方是否能够保证该信息的安全，同样的您也应该保证对方的敏感信息的安全。

ISO27001: 2005, 它包含了 133 个安全控制措施来帮助组织识别在运做过程中对信息安全有影响的元素。这 133 多个控制措施被分成 11 个方面, 成为组织实施信息安全管理实用指南, 这十一个方面分别是:

- 一、安全方针 (Security Policy)
- 二、信息安全组织 (Security Organization)
- 三、资产管理 (Asset Management )
- 四、人员安全 (Personnel Security)
- 五、物理与环境安全 (Physical and Environmental Security)
- 六、通信与运营管理(Communications and Operations Management)
- 七、访问控制 (Access Control)
- 八、系统开发与维护 (Systems Development and Maintenance)
- 九、信息安全事故管理 (Information Incident Management)
- 十、业务持续性管理 (Business Continuity Management)
- 十一、法律符合性 (Compliance)

ISO27001 制定的一个 ISMS 体系实施规范, 并可使用该规范对组织的信息安全管理体系进行审核与认证。通过使用该规范能使组织建立信息安全管理体系

通过 ISO 27001 来实施和认证 ISMS, 并不就一定能保证组织能完全摆脱信息安全遭破坏, 但实施该标准使信息安全被破坏的可能性降低, 因此降低投资和信息安全事故发生后的被破坏的程度。

### 三、建立 ISMS 体系对组织有什么好处

保证信息安全不是仅有一个防火墙, 或找一个 24 小时提供信息安全服务的公司就可以达到的。它需要全面的综合管理。而引入信息安全管理体系就可以协调各个方面信息管理, 从而使管理更为有效。

信息安全管理体系标准(ISO27001)可有效保护信息资源,保护信息化进程健康、有序、可持续发展。ISO27001 是信息安全领域的管理体系标准, 类似于质量管理体系认证的 ISO9001 标准。当您的

组织通过了 ISO27001 的认证,就相当于通过 ISO9001 的质量认证一般,表示您的组织信息安全管理已建立了一套科学有效的管理体系作为保障。

通过进行 ISO27001 信息安全管理体系认证,可以增进组织间电子商务往来的信用度,能够建立起贸易伙伴之间的互相信任,随着组织间的电子交流的增加通过信息安全的记录可以看到信息安全管理明显的利益,并为广大用户和服务提供商提供一个基础的设备管理。同时,把组织的干扰因素降到最小,创造更大收益。

组织按照 ISO27001 标准建立信息安全管理体系,会有一定的投入,但是若能通过认证机关的审核,获得认证,将会获得有价值的回报。

#### **四、引入 ISO27001 标准会给组织带来以下好处:**

企业通过认证将可以向其客户、竞争对手、供应商、员工和投资方展示其在同行内的领导地位。定期的监督审核将确保组织的信息系统不断地被监督和改善,并以此作为增强信息安全性的依据。信任、信用及信心:使客户及利益相关方感受到组织对信息安全的承诺。

60%的组织在过去的两年内信息及信息系统遭到过破坏,建立信息安全管理体系能降低这种风险,通过第三方的认证能增强投资者及其他利益相关方的投资信心。

通过认证能够向政府及行业主管部门证明组织对相关法律法规的符合性。

通过认证能保证和证明组织所有的部门对信息安全的承诺。

通过认证可改善全体的业绩、消除不信任感和拓展业务。

获得国际认可的机构的认证证书,可得到国际上的承认。

#### **五、组织实施 ISO27001 的程序与模式**

ISO27001 中详细介绍了实施信息安全管理的方法和程序,用户可以参照这个完整的标准制定出自己的安全管理计划和实施步骤。ISO27001 可以作为大型、中型及小型组织的确定在大多数情况下所需的控制范围的参考基准。修订后的 ISO27001 充分考虑了信息处理技术尤其是在网络和通信领域应用的近期发展,同时还强调了与业务相关的信息安全及信息安全的责任,扩展了新的控制。例如新版本包括关于电子商务、远程工作和外购等领域的控制。

组织引入信息安全管理标准的关键在于组织的重视程度和制度落实情况。组织在实施过程中一定要注意,ISO27001 里描述的所有控制方式不可能适合组织中每一种情况和组织中的每个潜在用户。因此,需要根据功能要求和组织本身的实际情况进一步开发适合组织自身需要的控制目标与控制措施,就像依据 ISO9001 标准开发质量手册和程序文件一样。

信息安全管理体系可以定义为整个组织或组织的一部分,包括处理、存贮和传输数据所用到的相应的资产、系统、应用程序、服务、网络和技术等。信息安全管理体系是整个管理体系的一部分,建立在业务风险的方法上,以开发、实施、完成、评审和维护信息安全。在 ISO27001 中

信息安全管理体系可能包括：

组织的整个信息系统；

信息系统的某些部分；

一个特定的信息系统；

ISMS 选择上面哪一种范围模式取决于组织的实际需要，一个组织可能需要为其企业的不同部分、不同方面定义不同的 ISMS。例如可以为公司与贸易伙伴的特定的贸易关系定义一个信息安全管理系统。ISO27001 强调管理体系的有效性、经济性、全面性、普遍性和开放性,目的是为希望达到一定管理效果的组织提供一种高质量、高实用性的参照。各单位以此为参照建立自己的信息安全管理体系,可以在别人经验的基础上根据自己的实际情况选择自己引入 ISO27001 的模式，以达到对信息进行良好管理的目的。

组织在实施 ISO27001 时，可以根据组织的需求和实际情况，采用以下几种模式：

- 1 组织按照 ISO27001 标准的要求，自我实施建立组织的安全管理体系，以达到保证组织信息安全的目的。
- 2 组织按照 ISO27001 标准的要求，自我实施建立组织的安全管理体系，以达到保证组织信息安全的目的，并且通过 ISO27001 体系认证。
- 3 组织通过安全咨询顾问，来实施建立组织的安全管理体系，以达到保证组织信息安全的目的。
- 4 组织通过安全咨询顾问，来实施建立组织的安全管理体系，以达到保证组织信息安全的目的，并且通过 ISO27001 体系认证

如果您对 ISO27001 感兴趣或者有任何疑问，请联系：

中国检验认证集团浙江有限公司（CCIC）中国质量认证中心浙江评审中心(CQC)

——浙江省服务贸易协会合作单位

周小波 13958095866 0571-56551768

缪莉 13958164607 0571-56551660

邮箱 isozxb@163.com

## 信息简报 稿件征集中……

浙江省服务贸易协会

邮箱: zats2010@126.com

电话/传真: +86-571-89703132

地址: 浙江省杭州市延安路 466 号浙江经贸大楼南 1611

邮编: 310006

QQ 群: 23142609 & 187270591

**Zhejiang Association of Trade in Services**

**E-mail: zats2010@126.com**

**Tel/Fax: +86-571-89703132**

**Add: South 1611 Zhejiang Trade Building, 466 Yan' an Road, Hangzhou,  
P.R.China**

**Zipcode: 310006**

**QQ group: 23142609 & 187270591**