

网络安全透视

与你的技术供应商考虑端到端网络安全时的100个要求

约翰·萨福克

高级副总裁 | 全球网络安全官
华为技术有限公司

2014年12月



作者

在此，我想要感谢那些对本文档做出重大贡献的人：刘海军、南建峰、王唯践、David Francis、Andy Purdy、Debu Nayak、Peter Rossi、Andy Hopkins、罗明、薛勇波、李花兰、Wout van Wijk、William Plummer、Ludovic Petit、Ulf Feger、牟德俊、杨光磊，以及其他直接或间接对本白皮书做出贡献的人，恕不一一列举。

约翰·萨福克

目录

2014年12月

1. 执行概要.....	1
2. 引言.....	2
3. 捕捉和精炼问题的方法论.....	4
4. 设计强健的网络安全方案需要考虑的问题和事情.....	5
4.1 战略、治理与控制.....	5
4.2 标准和流程.....	7
4.3 法律法规.....	8
4.4 人力资源.....	9
4.5 研究和开发.....	10
4.6 验证：不假定任何事情，不相信任何人，检验所有东西.....	13
4.7 第三方供应商管理.....	14
4.8 制造.....	15
4.9 安全地交付服务.....	17
4.10 问题、缺陷和漏洞解决.....	18
4.11 审计.....	19
5. 关于华为.....	20

1 执行概要

在我们2013年10月发布的白皮书《构筑公司的网络安全基因——一套综合流程、政策与标准》¹中，我们详细描述了我们在全面建立端到端网络安全流程的方法。我们说过，我们借此机会将客户告诉我们的与安全相关的前100件事情记录下来。实际上，任何人都可能向其技术供应商提出那些问题，了解他们的网络安全方法。本白皮书是一个清单，详细讲述了前100件事情，聚焦于技术购买商向其技术供应商提出的问题。

其目的是根据别人向华为提出的问题以及我们针对一系列的“标准”和最佳实践所做的评估提出建议，让购买者可以在招投标时系统地分析供应商的网络安全能力。

为了撰写这前100个要求，我们参考了很多的资料。

- 首先也是最重要的是，我们认真倾听了客户的心声。他们的问题和关注点是什么？他们的担心是什么？他们自己的要求，他们的行业或者国家的要求是什么？
- 作为全球ICT行业的领军企业，华为的业务遍及大规模通信基础设施、云计算、企业和消费者解决方案等所有东西。我们拥有来自150000员工、科学家和工程师的丰富知识——我们利用他们的知识和激情来做好这件事。
- 最后，我们浏览了1200多份“标准”、文章或者“最佳实践”，以确保一定程度的一致性。

我们认识到，在很多国家，与网络安全相关的法律和行业要求越来越多。政府和规则制定者开始将网络安全义务和网络安全失败的后续责任转嫁给国家关键基础设施供应商和计算机或信息技术服务供应商，这种现象确实不再罕见了。越来越多的公司不得不详细阐述其应对网络安全的方法，并详细说明他们对其自身的技术供应商和服务供应商所做的分析和评估。

服务供应商可以说“我不知道”或者“我原以为他们是优秀的，有能力的”，这样的时代正快速走向终点。技术购买者不对其所有供应商使用一致的评估问题的时代马上就要终结了。在一个全球相互交织的世界，威胁可能来自任何地方，而且也确实如此。这前100个要求是一个开始，让你开始评估供应商的网络安全能力，减少自身的风险。至关重要的是，我们相信，在要求高质量的安全保障方面，购买者的要求越高，购买者越一致，ICT供应商对安全进行投资、提高其安全标准的可能性就越大。

本白皮书大部分篇幅阐述了根据我们的研究，我们认为你在选择技术供应商时应该考虑的100件事情。我们把它们分成了几个章节，包括：战略、治理与控制，标准和流程，法律法规，人力资源，研究和开发，验证，第三方供应商管理，制造，安全地交付服务，问题、缺陷和漏洞解决以及审计。

每个章节都详细讲述了许多你应该考虑向你的技术供应商提出的要求。我们也提供了一些额外的理据，说明为什么这可能很重要的原因。其中一些问题可能会在以下方面对你们自己的组织有所帮助：内部审计人员要看什么，你自身的治理可能要考虑什么，以及你的董事会和审计委员会可能会问些什么问题。

¹ <http://pr.huawei.com/en/news/hw-310599-cyber.htm>

最后，我们向标准组织发出请求：

- 首先，我们应该团结起来，减少不同标准之间的交叉和重复。
- 第二，我们要将这些各种各样的标准进行重建，让它们建立在一个一致的构建模块之上：举个例子，治理与控制应该是所有含有此要求的标准中相同的构建模块，而不是很多标准有稍微不同的模块。
- 第三，我们需要尽可能地多关注结果性措施，而不是界定输入或者任务。

我们鼓励尽可能多的公司、政策顾问、供应商和买家思考这最初的Top100作为第一版，并提出改进建议。本着这种精神，我们很高兴地宣布，东西方研究所（EWI）已经同意采用首版Top100，并利用其广博的知识和网络，引导版本的刷新和定制化。我们希望Top100的概念能够成为买家方法的一个组成部分，能够有助于ICT行业进一步推动改进产品和服务的安全设计、开发和部署。

2 引言

在我们2013年10月发布的白皮书《构筑公司的网络安全基因——一套综合流程、政策与标准》²中，我们详细描述了全面建立端到端的网络安全流程的方法。我们说过，我们借此机会将客户告诉我们的与安全相关的前100件事情记录下来。实际上，这个清单中的一些问题，任何人都可以向其技术供应商提出，了解他们的网络安全方法。

我们给这个清单取名叫“逆向信息征询书”。其实它就是客户与他的供应商见面时，应该问供应商的一个潜在的网络安全要求清单——换言之，我们将流程倒着走了，我们让客户问我们，作为供应商，我们是如何处理网络安全的。

这第三份白皮书记录了前100个要求和我们制定这些要求所采取的方法。

首先，我们来讨论这样一个问题：是什么原因导致网络安全相关的一整套国际标准、规范和实践如此难以制定、达成一致并得到执行呢？难道是因为做这件事情得不偿失？当你看到网络犯罪带来的巨大损失的时候，你就知道显然不是这样的。是因为还没有被企业或者是政府提上日程吗？不管是关于网络犯罪的国际政府会议的数量，还是关于数据遭到破坏、知识产权被盗以及因为拒绝服务攻击而导致的在线服务中断的重要媒体报道，都在告诉你不是这么回事。也许是因为这个挑战的规模实在太大了，我们无从下手，也许是因为有太多的关于“标准”、“最佳实践”和“指南”的看法了。我们当然认为这是其中一个因素，正如我们在上一份《白皮书》中所说的：“标准的问题在于它们并不标准”。最后，你们在分析现有标准的时候会发现，它们都倾向于聚焦企业或政府部门，有些聚焦最终用户，很少标准，如果真有的话，真正聚焦硬件和软件生产商——供应商。

² <http://pr.huawei.com/en/news/hw-310599-cyber.htm>

事实上，由于技术的广度，我们永远也无法达成“单一标准”。但是我们可以做的是关注那些在很多标准、准则和最佳实践中经常提到的关键要求（可能措辞有所不同），并让它们聚焦供应商应该共同采取的措施，以改进其产品安全。

在本白皮书中，我们旨在详细描述我们的客户和其他利益相关方问得最多的关于网络安全的非技术性问题。在这里，“最多”还指那些引起对话、审视或者后续问题最多的一些问题。我们采用“诗的破格”的方法把这些提给我们的问题进行了处理，把它们转化成一般性的问题。我们还加了一些反映最新事件的问题，比如斯诺登泄密事件，并且填补了问题之间的空白，使得文章的每个部分都衔接紧密。

我们把这些问题的提出来，以持续地增强知识，促进正在进行的讨论，并对评估网络安全中“什么是好的”这样的工作做出贡献。

在详细叙述这些问题时，我们并不试图将它们按优先次序进行排列，也没有把它们套到某个特定的框架或者方法论上。实际上，对华为的每个核心流程，我们都详细地阐述了这个问题：它们大致位于华为流程的哪些地方？

本质上来说，这个清单不可能对每个行业而言都是全面的，也不可能覆盖所有法律和技术标准。这不是我们的目的。我们的目的是根据别人向华为提出的问题以及我们对“标准”和最佳实践课题的评估提出建议，让购买者可以在供应商答标时系统性地分析其网络安全能力，在寻找满足其即期和长期技术需求的最佳供应商时，让他们能够使用这些信息增强其信息征询书（RFI）和建议征询书（RFP）的质量。

我们真挚地认为，在要求高质量的安全保障方面，购买者的要求越高，购买者越一致，ICT供应商对安全进行投资、提高其安全标准的可能性就越大。

团结一致，我们可以增强技术产品和服务中安全考虑的质量，从而让我们可以齐心协力地做更多的事情，通过信息和通信技术（ICT）的使用去丰富人们的生活。



3 捕捉和精炼问题的方法论

为撰写前100个要求我们参考了很多资料：

- 首先也是最重要的，我们认真倾听了客户的声音。他们的问题和关注点是什么？他们的担心是什么？他们自己的要求，他们的行业或国家的要求是什么？通过这些我们有幸请到数以千计的访客参观我们的深圳总部，向他们展示我们的价值观、能力、政策和方法——这些活动激发了很多问题和思索，我们在此感谢这些客人的真知灼见。
- 作为全球ICT行业的领军企业，华为的业务遍及大规模通信基础设施，云计算、企业和消费者解决方案等所有东西。我们拥有来自150000员工、科学家和工程师的丰富知识——我们利用他们的知识和激情来做好这件事。

作为一家公司，华为热切支持国际主流标准，并为这些标准的制定积极做出贡献。截至2012年底，华为加入了150多个行业标准组织，如，3GPP IETF、IEEE、ITU（国际电信联盟）、OMA、ETSI（欧洲电信标准化协会）、TMF（电信管理论坛）、ATIS、Open Group等。华为向这些标准组织总共提交了5,000多个提案，在这些组织中占180多个席位，支持形成一致的国际标准方面的努力。在标准和框架方面，我们为新兴的美国国家标准与技术研究所框架（NIST）的制定做出了贡献，支持加强ISO27001标准，我们也是ITU和3GPP工作和概念的积极贡献者。在撰写这前100个要求时，我们参考了这些材料的很多内容。

- 最后，我们浏览了1200多份“标准”，文章或者“最佳实践”，以确保一定程度的一致性。

虽然我们确实希望你们中的大多数人会把此文件做为参考，但是这前100个要求并不是一个全面的购物清单式的问题清单，上面列出了你向你的供应商提出的问题。提问很容易，但是理解答案，确保答案的精确性、实证性和可审计性还是需要技能的。

最后，我们要向标准组织发出一些请求：

- 首先，我们应该团结起来，减少不同标准之间的交叉和重复。
- 第二，我们要将这些各种各样的标准进行重建，让它们建立在一个一致的构建模块之上：举个例子，治理与控制应该是所有含有此要求的标准中相同的构建模块，而不是很多标准有稍微不同的模块。
- 第三，我们需要尽可能地多关注结果性措施，而不是界定输入或者任务。

我们非常乐意接受你们关于本前100个要求的反馈——需要增加、删除或修改什么——这样的话，将来我们可以制定一个版本，把你们的输入包含进去。

4 设计强健的网络安全方案需要考虑的问题和事情

我们认识到，在很多国家，与网络安全相关的法律和行业要求越来越多。政府和规则制定者开始将网络安全义务和网络安全失败的后续责任转嫁给国家关键基础设施供应商和计算机或信息技术服务供应商，这种现象确实不再罕见了。这是一个两难的困境，因为一旦出现大量数据丢失或服务中断之类的情况，政府或者规则制定者很可能会质问服务供应商他们的网络安全方法是什么（假设这是一个安全事故）。越来越多的公司不得不详细阐述其应对网络安全的方法，并详细说明他们对其自身的技术供应商和服务供应商所做的分析和评估。而网络安全就其最广泛的定义来说，是复杂的，从而加剧了这一困境——从法律到制造、从服务到人力资源、从治理到研究与开发——世界上几乎没有人有如此的广度和深度，因此，极少人知道要问什么问题，要找什么证据。

服务供应商可以说“我不知道”或者“我原以为他们是优秀的，有能力的”，这样的时代正快速走向终点。技术购买者不对其所有供应商使用一致的评估问题的时代马上就要终结了。在一个全球相互交织的世界，威胁可能来自任何地方，而且也确实如此。这前100个要求是一个开始，让你开始评估你供应商的网络安全能力，减少自身的风险。

在这一章里讲述了我们认为你在考虑供应商的安全能力时应该考虑的前100个要求。不是所有要求在任何时候都适用；不是所有要求都适用于你所在组织的所有层级；不是所有要求都适用于所有的采购活动。我们希望通过这个清单做到的是，你们能够更好地理解在选择供应商时需要考虑什么，希望你们可以使用清单中的部分要求，把你们自己的要求补充进去，从而推动所有技术供应商提高对安全的关注。

这些问题划分成与我们2013年10月发布的第二篇白皮书大致相同的章节。在该白皮书中，我们全面介绍了我们的网络安全方法。

在读这前100个要求时，你可能会认为其中一些问题可以合并。对此我们也苦思良久，并试图将问题写得非常明确。我们合并得越多，失去焦点的风险就越大。有些问题也非常微妙，其后续问题转移到了生命周期或流程的下一个阶段，从而问了一个稍微不同的问题。因此，你们可以随意对问题进行修改，因为我们最大的愿望就是提高所有技术供应商的安全考虑的质量。

4.1 战略、治理与控制

如果董事会和高级管理者都不认为网络安全是一个优先事项，那组织的员工也不会认为它是优先事项。确保网络安全融入到组织的组织设计、治理与内控框架是设计、开发和交付良好网络安全的开始。

要求	还要考虑到…
<p>1. 供应商是否有正式的风险管理战略和方法？如信息和网络安全风险？</p>	<ul style="list-style-type: none"> • 若没有战略，就不太可能分配投资或资源。 • 组织要知道组织运作（包括使命、功能、形象、或者名誉）、组织资产、和个人的网络安全风险。 • 缺乏战略会导致随意性的结果，质量和安全没有一致性和可重复性。 • 只有战略而没有一套行之有效的方法，那么战略就会成为空谈。
<p>2. 你的供应商有没有合适的治理、组织设计、政策和流程来支撑他们的战略？并定期更新他们的战略以适应最新的网络安全环境和要求？</p>	<ul style="list-style-type: none"> • 如果网络安全被嵌入到组织的治理和基层中去，那它对于比如财经委员会或者战略委员会之类的重要性就是相似的。 • 明确可见的董事委员会、政策文件、标准和关键审计控制点都说明它被嵌入到组织中，而且被认真对待。 • 如果这对董事会和高级管理层来说不重要的话，那对员工也不会是重要的。所以它必须是可见的。
<p>3. 供应商有什么样的治理架构可以表明网络安全是企业的一项战略和运营重心？是否有一个专门的网络安全董事委员会，它是如何运作的？</p>	<ul style="list-style-type: none"> • 一个由董事会高级成员领导的专门委员会说明这是公司的优先事项，而不仅仅是委托给技术员工的技术性活动。 • 如果该委员会包含重要的董事会成员，这展现了高层的决心，因为他们是唯一可以带来根本性变化的人。 • 如果这个委员会是设定网络安全战略和方法整体方向的决策机构，这表明董事会积极参与网络安全工作。 • 如果董事会成员接受汇报，在出现问题时进行评审，参与危机管理，这表明他们熟悉运作上的实际情况 • 如果高层管理者清楚地表达了在战略目标和重点工作、可用资源和整体容忍度上面的期望，并且分配实现结果的责任，这可以确保每个人都理解网络安全的重要性。
<p>4. 供应商如何确保网络安全在它的业务中得到进行了应对？董事会成员如何知道企业中发生的事情，他们如何担责？</p>	<ul style="list-style-type: none"> • 应该有一个清晰的链接来展示最高级的董事委员会如何监管其策略的执行。 • 公司应该能够展示从策略深入到业务最深层（接近客户）以及反向的综合衔接。 • 供应商能够提供证据证明董事会成员和高级管理者在采取网络安全行动方面有清晰的个人责任吗？还是他们仅仅只是作为委员会成员列席？
<p>5. 供应商采用什么方法来确保他们的企业的各个部分都考虑了安全的影响？这些是如何以一种一致的、可重复的方法在进行？</p>	<ul style="list-style-type: none"> • 网络安全是每个人的事，解决网络安全必须人人参与。能够展示公司“全员”参与去决定什么事情会发生，什么不会，从而确保安全成为企业基因的一个部分。 • 网络安全越集中到总部的一小部分人头上，就越会成为只是这一小部分人的问题。端到端意味着必须有端到端的资源参与其中。 • 公司的其他部门如何看待这个企业战略方向并将这一信息作为他们风险管理和运作流程的输入的呢？
<p>6. 供应商采取什么方法向网络安全活动提供资源？是通过一个集中的专门团队去做还是公司各个部分，包括区域的安全资源，都参与其中？</p>	<ul style="list-style-type: none"> • 这是谁的问题？如果这不是我的问题，而且我的绩效中不包含对安全的最佳方法，那我就不会应对这个挑战。组织设计和供应商嵌入安全的方法决定了它是否真的是公司的一个整体战略还是一个由少数人来应对的附加物。 • 公司应该能够展现，在主要职能部门，风险管理和网络安全是怎样融入到其活动中的，包括流程和资源的融入。 • 公司还应该能够展现在其内部企业流程中是如何监控和处理本地安全要求的。
<p>7. 每个公司都有安全事故，供应商如何从他们的安全事故中吸取经验教训？他们的高层管理者如何进行评审从而使得吸取的经验教训都嵌入到他们所做的事情中去？</p>	<ul style="list-style-type: none"> • 一个“瞎”的董事会是可怜的董事会。人们常说，只有组织的最高层才能激发行为和和方法的最大变化。如果他们看不到这些安全方面的缺点或事故，他们就不会理解他们客户所看到的，也不知道他们要在公司中必须要亲自改变什么东西。 • 公司应该能够展示例行向董事会级别的委员会汇报安全事故，从中吸取的教训和事故之后的改进情况

要求	还要考虑到...
8. 供应商的内部IT系统是否曾是网络攻击的受害者，他们从中学到了什么从而改进他们的产品和服务？	<ul style="list-style-type: none"> • 一个公司从自身的安全挑战吸取经验教训的能力使其能够更好地理解他的供应商可能面临的挑战，了解如何从风险角度缓解这些挑战。 • 一个公司应该能够展现在网络安全方面，它是如何“自己是对症下药”的。

4.2 标准和流程

要生产质量一致的产品，需要可重复的质量流程和标准，也需要你的员工和供应商采用相似的方法。网络安全也是一样：如果你的流程是随意的，或者你对网络安全标准的方法是随意的，最终产品的质量和安全性也会是随意的。

要求	还要考虑到
9. 供应商是否采取并支持在网络安全广泛意义之内的任何全球标准？他们遵从什么标准，在什么标准组织担任高级角色或积极地参与了活动？	<ul style="list-style-type: none"> • 如果企业文化是能采用国际标准，就采用国际标准，愿意在业务流程中融入最佳实践，那它很可能与网络安全的最新思想协调一致。 • 一个公司参加了支持网络安全标准制定和应用的标准团体，这表明该公司愿意采用最佳实践和标准。 • 你的供应商是否对适用于你公司的技术标准表示支持和接受呢？ • 为了加强独立软件测试的可信度，你可能需要探索供应商是如何采用业界最佳测试实践的（比方说通用准则），并在标准化方面做出努力以期加强内部网络安全测试的能力和数量。
10. 供应商如何决定应该遵循什么样的最佳实践和标准（或法律）？有什么样的流程进行决策并解决法律和标准之间的冲突，他们如何让其保持最新？	<ul style="list-style-type: none"> • 标准和最佳实践的问题是：“优秀”是旁观者眼中所看到的。一个能够同步到最新需求的机制向客户表明他们得到了最新需求。要真正地采用最广泛的观点、标准和想法意味着公司必须持续评估别人如何应对这个挑战，并把新的改良的思想和要求融入他们的运营中。 • 公司应该能够展现一个综合的方法，在全球进行扫描，寻找最佳实践、标准、规范等，把它们固化到一套公司政策、程序和基线之中。
11. 为了遵从一系列的技术标准，供应商有什么团队或者能力来支持这些广泛的管理和技术标准，包括密码算法？	<ul style="list-style-type: none"> • 你需要将这个要求清单扩展，识别一系列具体的管理/流程标准，如ISO27000,以及行业内的技术标准，如X.805,PCI,OWASP. • 供应商要能够适应现有的标准，并且愿意随着标准的修改和新标准的制定而改变他们的技术，让你感到满意。 • 密码学/加密技术是一个专业领域，有时受本地法律的约束。你的供应商要有专门致力于密码学/加密技术的资源，并且了解法律和技术要求。

4.3 法律法规

法律是复杂、多变而且一直在变化的。大家知道，一个国家有某个法律，并不意味着该法律一定执行了；即使执行了，其执行方式可能不同，或者对同样的法律或规范有不同的解释。法律、规范、标准和国际控制增加了供应商和企业的复杂性和风险。

要求	还要考虑到
<p>12. 供应商如何评估并试图理解他们所运营的国家的安全、隐私法律和要求？他们如何把这些信息用于其产品和服务的设计、开发、和运行和维护？</p>	<ul style="list-style-type: none"> • 不同国家不一致的法律给全球性企业带来了明显挑战。除此之外，法律和规范的问题还在于“解释可能会不同”。公司要有一个机制来评估和确保得到最新的法律法规，使客户知道他们得到的产品是满足最新要求的产品，这很重要。要真正地考虑最广泛的观点、标准和想法意味着公司必须持续评估别人如何应对这个挑战，并把新思想和要求融入他们的运营中。 • 公司应该能够展现一个综合的方法，在全球进行扫描，寻找最佳实践、标准、规范等，把它们固化到一套公司政策、程序和基线等。 • 法律虽然很多变，但却很重要。公司应该能够展示它如何在产品开发和过程中以一种一致的、可重复的方式应对不清晰或者冲突的法律。 • 法律与技术标准或要求一样重要。供应商应该能展示其如何满足一个国家或地区的法律要求，尤其是在个人隐私和数据保护领域。 • 日常业务活动是遵从流程的。因此，若能够展示在产品和服务设计中考虑了合规要求，这表明对所有要求有一个全面的方法。
<p>13. 供应商如何确保他们的流程与本地法律和要求一致？若某个本地法律与他们的政策、标准或流程相冲突，他们如何处理？你的供应商是否就它和政府的关系做出过公开的声明？</p>	<ul style="list-style-type: none"> • 法律就是法律，你的供应商要能够证明他们的设备和服务是遵从法律要求的，这很重要。 • 要保证总部能听到本地的声音，这是每个在别的国家运营的公司都会遇到的挑战。供应商应该要能够证明这样的声音如何融入到总部的思想和产品开发中去。 • 公司应该能够说明，在本地法律优先的前提下，它如何处理相互冲突的法律和要求。 • 供应商应该能够明确声明是否有任何义务向别的政府提供信息/数据。 • 供应商应该披露他们与任何政府在国家安全、植入“后门”、弱化加密或安全保护方面的关系。 • 供应商应该能够明确说明将把数据保存在哪里，数据受什么法定管辖。
<p>14. 供应商如何确保他们的流程和产品遵从产品所部署国家的出口管制和运营法律（包括加密）？</p>	<ul style="list-style-type: none"> • 一个公司应该能够展示其贯穿销售、服务、合同商务和产品设计流程的综合管理、政策和程序，而且这些流程能够满足特殊的法律要求--不论是贸易合规、许可证管理还是出口管制等。 • 一个公司应该能够证明有恰当的控制点以确认关键的要求得到了执行。 • 如果他们做不到这些，客户就会冒着这样的风险：不得不替换掉违反法律的设备或服务。
<p>15. 供应商针对知识产权的公司政策是什么？</p>	<ul style="list-style-type: none"> • 一家公司应当能够制定一系列政策、程序和方法，详细说明其如何应对许可、知识产权和跨文化差异之类的问题。在很多国家都存在道德和法律方面的挑战，但是对这些挑战的应对应该一致，并且应将其融入到公司经营方式中去。你应该确保供应商有内部行为准则或者商业行为准则政策。
<p>16. 供应商如何确保他们的销售团队只销售符合本地法律法规，包括任何出口管制或贸易制裁规定的产品和服务？</p>	<ul style="list-style-type: none"> • 销售团队的职责就是销售产品，销售是他们的原动力，并且销售对于企业的成功至关重要。他们也许会认为，规则和制度会妨碍销售。此外，购买者也许不一定有最强的采购资源，因此，供应商必须能够证明他们的流程是如何保护购买者的。 • 一个供应商能够展示其有一套综合流程，包含了销售、法律和交付或支持，而且这套流程与购买者的内外部要求对齐，这一点很重要。
<p>17. 供应商如何评审合同，确保其中包含了关于他们的网络安全能力的准确信息？</p>	<ul style="list-style-type: none"> • 项目和合同通常是非常复杂的、也是长期的，并且包括来自众多公司多个部分的输入件。供应商应当能够展示，为了实现购买者的目标，达成了哪些共识并写入了合同？包括法律法规。
<p>18. 鉴于所有的高技术公司都使用其他供应商的技术，供应商应该要能够清晰描述所采用的许可和控制机制。</p>	<ul style="list-style-type: none"> • 你希望你的供应商使用的第三方部件是有适当许可的，从而让你感到放心。这样就能够避免下游环节的潜在冲突，导致可能需要替换硬件或软件，从而造成代价高昂的中断。

4.4 人力资源

很多公司都说他们的员工是他们最重要的资产，确实如此。但是，从安全的角度来说，他们也可能是一个挑战。员工雇佣、培训、激励和绩效管理的方式常常是成败的关键——不仅仅是在网络安全方面，在公司整体战略的交付上也是如此。

要求	还要考虑到
19. 供应商的全员网络安全意识教育中是否包含了管理层？如果是，是怎么做的呢？他们的高层管理者和董事会是否接受了持续的法律合规培训？	<ul style="list-style-type: none"> 将意识教育看做一件对管理团队——包括中层管理团队——来说重要的事情，这很重要。否则员工将会忽视意识教育。因此，管理层要重视意识教育并且身体力行，参与全员意识教育培训。 若供应商能够展现出“我们都致力于此”、“这是我们大家的事情”，那成功的几率就更大。 公司日常运作的决策者和监管者对法律遵从的理解会影响公司的稳定和持续运作。他们应该有网络安全法律方面的知识。
20. 从内部威胁的方面来说，并不是所有职位的风险都是相同的。在网络安全方面，供应商是否识别了“敏感”或“关键”岗位？	<ul style="list-style-type: none"> 必须要确保给客户提供服务的关键岗位上的人是可信的，并且有基本的保护性措施。 建立对这种关键岗位的识别机制，聚焦此类岗位的潜在风险，并对此类岗位进行有效管理，这可以展现一个供应商的成熟度。 举个例子，对你的核心ICT有直接访问权限，可以直接改变产品软件的岗位，对产品和服务产生的威胁会更严重。
21. 对“敏感”或者“关键”岗位员工的招聘与审查，供应商采用什么方法？供应商有没有进行背景检查，离职审查并签署合适的合同条款呢？	<ul style="list-style-type: none"> 这显示出对人员素质和诚信的一贯方法。它能够识别内部人员威胁带来的风险，展示缓解这些风险的方法 若供应商能够展现这点，这说明供应商对网络安全采用了全面的方法。
22. 供应商有什么样的流程和机制定期进行与员工和分包商职责一致的网络安全意识和专项培训？他们如何知道员工参加了培训？	<ul style="list-style-type: none"> 供应商如何将网络安全转变成融入其企业文化精髓的被所有员工接受的基本文化呢？供应商建立了哪些基本体系和流程来保证这一点？ 网络安全是长期的要求，这意味着每个人的知识必须经常更新。如果你的供应商的知识不能与时俱进，这可能意味着没有重心并且没有做好准备。 在考察你的供应商的时候，值得一看的是他们是否有定期的培训和意识提升活动，是否使用很多全球性的和地方性的培训和意识提升工具，是否在功能性领域做一些额外的工作——也就是在具体领域进行更详细的培训。实质上，组织的人员、合作伙伴要接受足够的培训以履行他们信息和网络安全相关的义务和责任，并且与相关政策、程序和协议保持一致。
23. 供应商是否有任何聚焦提高“敏感”或“关键”岗位员工能力与理解的政策？	<ul style="list-style-type: none"> 这意味着对敏感或关键岗位会有不同的更加严格的要求。公司应该能展现客户所面临风险不只是知识，还有经验和价值观，比如诚实。
24. 很多国家都有反贿赂和腐败的法律。在这方面，供应商如何在这方面处理他们的员工？	<ul style="list-style-type: none"> 供应商必须能展现它怎样让它的员工知道关于防止贿赂和腐败的各国法律和国际认可的最佳实践。 供应商如何以一种一致的方式向员工宣传和融入公司的价值观和“是非”观念？
25. 供应商是否有一个机制，让员工认为某些事情可能不符合政策、法律或法规时可以通知管理层（以合适的方式）？	<ul style="list-style-type: none"> 公司员工可以看到管理者所看不到的一些事情。相应的通知机制的建立可以促使公司及早发现并进行改进。一个自我学习、闭环优化的系统需要展现公司如果处理不符合其流程的事情，员工通常需要使用这样的机制，把他们认为不对的事情说出来。

要求	还要考虑到
26. 供应商的员工的退出策略是什么？他们如何利用从中所获得的知识来改进其政策、程序和文化？	<ul style="list-style-type: none"> 员工离开的原因有很多；一些是因为对看到的東西的感觉不舒服。某些反馈可能暗示了安全问题。供应商应该能够展现他们吸收对其公司运营方式、政策和流程的各种形式的输入——包括来自即将离职员工的心声，作为解决问题，优化业务的一种方式。
27. 供应商是否有一个正式的网络安全问责指南？	<ul style="list-style-type: none"> 供应商要能够展示他们怎么平衡奖惩，从而在客户、公司和员工间形成良好的安全文化。 如果一个员工明知故犯违反公司网络安全政策，应该要清楚有什么政策和流程可以采用，对他的潜在惩罚措施是什么。
28. 对员工采取问责措施时，供应商如何追究他们的经理或主管的责任？也就是说，他们有没有处理任何管理或监督的问题？	<ul style="list-style-type: none"> 对一个公司来说，证明管理者对他们团队的绩效和行为起着一定作用，这很重要——他们不能只是责备别人影响他们团队的绩效和行动。一个公司应该能展现他们如何确保个人、管理者和团队的责任以及激励和惩罚之间的平衡。

4.5 研究和开发

公司不想使用他们稀有的资金从这样的公司购买高技术产品：没有严格的研发流程，不能够交付一致的高质量和安全的产品。他们也不想看到供应商做这样的投资决定：是投资一个新产品还是投资保证所有产品安全。跟质量一样，网络安全也不能附加在产品之上。公司需要展示其投资下一代产品的决心，还要有长期的决心去增强其研发的方法，进行安全设计、开发和部署。

要求	还要考虑到
29. 供应商是否有一套正式的嵌入了网络安全要求的研发流程，它们是否基于任何业界标准或最佳实践？	<ul style="list-style-type: none"> 如果一个公司不能展示一套成熟的研发流程与方法，它就没有坚实的基础去嵌入质量与网络安全。随意的流程会造成随意的质量和安全结果并带来更高的风险。 在安全方面没有一个完美的模型，也没有一个全球的标准，所以公司要能够展示它如何利用来自各个渠道的知识和最佳实践。
30. 供应商的研发流程如何支持网络安全要求并评估其有效性，包括动态的威胁环境。他们使用什么机制确定哪些是强制要求，哪些只是优秀实践？	<ul style="list-style-type: none"> 很多人认为网络安全是质量的一部分，也确实如此，但是它又有一些不同的因素——尤其是在威胁的动态性和攻击入口的变化上。供应商应该要能够展示一个闭环的方法，将安全要求嵌入研发，发现新问题或知识，测试安全结果的有效性。如果无效，那就必须改变，然后回头再把新的或改良的知识和经验嵌入进去，增强网络安全。
31. 世界各地的客户有不同的，有时甚至是相互冲突的安全和功能要求，供应商是否有一套综合流程来承载一个客户需求，直到关系结束，并评估能发生和应该会发生什么？	<ul style="list-style-type: none"> 不同国家的法律法规、社会文化和用户喜好不同，从而形成了不同的客户要求。一套固定的、不灵活的流程并不能满足客户和司法管辖方面的特定需求。缺乏适当的管理会导致这样的结果：客户得到的不是他所期望的甚至可能与他想要的功能正好相反。供应商应该要能够展现对不同甚至是相互冲突的需求的有效管理。
32. 供应商有没有一个产品生命周期管理策略，可以确保产品在其生命周期内在安全方面得到维护？这个策略告诉你什么，他们是怎么使用这个策略的呢？	<ul style="list-style-type: none"> 作为一个潜在客户，你想要确保你所要购买的产品有合适的使用周期（比方说3-5年）从而可以收回你的采购成本。供应商应该能够详细说明他们怎么管理一个产品或者一系列相关产品的生命周期。实际上，他们应该要让你满意：你购买的产品不会在短期内过时或者不能升级。 如果安全要求与其他方面的要求，例如：功能、可靠性、性能等方面的要求相冲突，供应商如何决定哪个要求是首要要求呢？

要求	还要考虑到
33. 供应商应该详细描述他们的主要产品开发流程是如何运作的, 如何从技术和质量的视角评审进展、并进行持续提升。并请详细说明在流程中嵌入了哪些评审、检查点、GONO-GO决策点?	<ul style="list-style-type: none"> • 大多数的技术都很复杂, 那么了解你的供应商如何将多个技术评审、业务评审、安全评审、质量评审以及检查点融入到他们的流程中可以让客户感到放心: 供应商从未忽视其目标和成功结果。
34. 现代软件非常复杂。通常包含了数百万行的代码以及成千的来自不同供应商的部件。供应商有什么样的程序和技术来确保在正确的时间使用了正确的部件?	<ul style="list-style-type: none"> • 开发流程可能设计得非常好。然而如果缺乏有效的IT管理平台的支持, 公司规范和客户要求可能很难在流程中得到执行。如果构成一个完整计算机系统的各种相关元素没有包含在“配置管理”中, 或者没有适当地管理, 那系统就无法连贯运行, 你无法追踪和追溯在哪里使用了什么。
35. 配置管理是一个系统工程过程和支撑技术, 用于建立和维持产品生命周期内其性能、功能和物理属性所要求的一致性。在复杂的技术环境中, 这个机制是维持一致的、高质量、安全的代码的基石, 你的供应商的方法是怎样的?	<ul style="list-style-type: none"> • 公司要能够展示其系统性的“配置管理”或控制系统, 避免技术元素被恶意篡改或错误的部件嵌入到产品开发和编译过程中。 • 这还应该包括版本控制、变更管理、第三方工具和部件管理。
36. 职责分离对限制威胁和潜在破坏非常重要, 在研发中, 特别是对于软件工程师, 供应商是如何进行职责分离的?	<ul style="list-style-type: none"> • 知道如何减少内部人员带来的威胁, 这很重要。职责分离是很重要的一部分。供应商要能够标出他们的研发角色, 以及每个角色可以参与的研发流程的环节。从安全的角度来说, 限制个人可以访问的环节、行动、产品和源代码可以降低风险。
37. 很多技术公司在他们自己的代码中嵌入了第三方软件和开源软件, 供应商是如何跟踪和管理他们每个产品中的这些软件的?	<ul style="list-style-type: none"> • 虽然你的供应商的代码和计算机技术可能是按照高标准来制造的, 但是他们使用的其他供应商的技术可能有弱点。知道问题在哪里, 涉及到谁的软件/硬件是评估风险和采取补救行动很关键一部分。
38. 开源和第三方软件通常在很多网站可以找到。供应商如何知道他们下载的软件是合法且不含恶意软件、后门的?	<ul style="list-style-type: none"> • 如果供应商不对其使用的软件部件及其采购来源进行严格管控, 这说明他们缺乏质量管理。如果他们有很严格的流程来确保他们只从知名的网站下载源代码, 这是降低风险的一个要素。 • 有些“流氓”网站可能会有被篡改的源代码和被植入的恶意软件, 因此, 供应商必须非常谨慎。
39. 在你的供应商使用第三方软件之前, 有什么样的流程确保在接受使用前以及部署后已知漏洞都已经解决了?	<ul style="list-style-type: none"> • 对于买卖双方来说, 一个很好的格言就是: ABC模型: 不假定任何事情; 不相信任何人; 检查所有的东西。你应该检查你的供应商是否验证了其在你所购买的产品中嵌入的第三方软件中所有的已知漏洞在他发货之前都得到了解决。这应该是一个持续的过程, 因为在产品发布之后也可能会不断发现新的漏洞。 • 如果供应商把第三方部件嵌入进其产品中, 供应商应该与其自身的供应商确认这个第三方软件是否有生命周期管理流程覆盖?
40. 供应商如何确保第三方软件、开源部件或者公共软件程序中的缺陷在所有使用到的地方都得到了修复?	<ul style="list-style-type: none"> • 通常一个第三方部件会被使用到多个供应商的产品或者位于不同地点的同一个产品。因此要解决一个第三方漏洞, 要求你的供应商知道使用了这个部件的所有产品, 否则, 该漏洞就有可能没有在所有产品中得到解决。
41. 供应商是否在他们的产品中使用了多种开发语言和工具? 如果是, 他们如何对这些工具分类, 这些工具是否是最新版本, 是否还有支持?	<ul style="list-style-type: none"> • 你的供应商可能使用来自多个第三方的很多工具、软件和代码。由于公司会合并、失败, 也会改变他们的战略, 你的供应商会变得比较脆弱。因此, 你应该要求你的供应商有一个正式的流程按照质量、架构和产品开发路标来评审、批准和阻止第三方产品和部件的使用。 • 你的供应商要能够展示其战略和机制, 保证只有能够提供支持服务、安全的第三方工具和部件会嵌入到他们的产品中。

要求	还要考虑到
42. 供应商需要描述他们对端到端研发流程进行跟踪和追溯的方法和他们所使用的软件工具--他们使用了哪些开源或第三方软件。	<ul style="list-style-type: none"> 事情总有出错的时候，人们可能会做坏事。如果你的公司发生了一些事情，系统崩溃了，或者以任何方式被篡改了，你会给供应商多长时间来找到问题？一天、一周还是一个月？复杂的技术可能包含成千的部件和几百万行的代码。你应该要确保你的供应商可以追溯其卖给所有公司的所有产品中使用的的所有部件，确保你可以追溯你购买的所有产品。供应商也要能够追溯所有参与的人员，他们在什么时间进行了什么操作，以及针对该项工作的授权。
43. 复杂的产品通常有数百万行的代码，供应商的研发过程中是否有自动化的代码扫描环境来自动对代码进行扫描以发现好的/差的编码实践？	<ul style="list-style-type: none"> 好的工程尽可能地把工作自动化，从而“保证”质量和推动一致性。你的供应商要有很多自动化的工具和技术，动态地扫描你的产品，以发现很多问题——理想情况下，这应该要自动反馈到供应商的质量管理体系中。 自动化不能解决所有的事情，也不能发现所有的问题，所以需要一套混合的方法来确保公司不会太依赖于纯粹基于技术的验证。
44. 供应商需要描述决定产品是否能发布上市的机制和授权流程。	<ul style="list-style-type: none"> 让你自己对审批流程的严格程度感到放心。你会从很多ICT团队听说，也许从你自己的公司也听说了，他们说某件事情95%完成。你的供应商要能够以各种方式证明产品是100%完整的，这应该由非项目团队成员来评审。 应该有证据证明有多重技术和质量保障或安全审查，而且最终批准的权力也不在软件工程师手中——你不能自己给自己的家庭作业打分。
45. 在产品开发过程和生命周期中，会有缺陷被发现，供应商是如何跟踪所有的缺陷并确保所有可能使用了该组件的产品中这个缺陷都被修复了？	<ul style="list-style-type: none"> 作为客户，你不想再三发现同样的问题，你也不想同样的问题出现在不同的产品中。因此，你需要知道你的供应商如何追踪缺陷和问题，这种追踪是如何融入到研发、培训以及其他领域中的？
46. 供应商需要描述他们如何最大程度地提高网络安全能力。他们是否有能力中心或安全技能中心？它是如何运作的？	<ul style="list-style-type: none"> 你的公司里面，不是每个人都可以成为全方面的专家。在大型的复杂技术工程上，也是如此。因此，供应商要能够评估其安全能力的广度和深度，确保合适的团队有这个重要技能和专长，你需要知道这是如何开展的。
47. 威胁不断在演进，供应商如何对此进行监控，并在产品设计、开发和部署阶段进行考虑？	<ul style="list-style-type: none"> 如果你的供应商总是在开车时看后视镜，他们可能会撞到墙。你想要让自己放心：你的供应商是向前看的，预测将要出现的问题，并在产品设计和开发中有针对性地应对这些问题。 供应商应该能够展示他们考虑了来自各个渠道的威胁或攻击，他们应该能够展示这些是如何融入他们的设计和其他要求中去的。
48. 供应商需要详细说明相关技术是如何支持他们的流程的。例如，在测试中，他们在测试中如何使用威胁库，或者他们是否建立了测试用例库？	<ul style="list-style-type: none"> 虽然你的供应商可能在流程和标准上说得很好，但是要有效率 and 效果，他们则需要以得到支持和集成的公司技术为基础。你的供应商是这样的吗？ 你的供应商的每个流程或者每个部门应该有一整套集成的技术平台来支持他们的运作和供应商的业务目标。
49. 供应商需要描述他们对版本的管理方法。有些供应商针对所有国家的所有客户有一个单一的代码库；有些有一个基础的代码库，然后针对具体的区域或国家和具体客户有一些分支。这两种核心方法都有优点和缺点。他们使用的是哪种？	<ul style="list-style-type: none"> 是发布一个全球的产品版本，还是针对每个国家或客户发布一个产品版本，无法确定哪个是正确的模式。如果全球只有一个产品版本，那就会失去灵活性，那么你的供应商可能不会采纳你的要求；如果你有数百种不同的产品，功能大致一样，那么供应商的成本就会上升，效率会降低。关键是知道你的供应商如何找到这个平衡点和如何管理他所选择的方法附带的挑战。

4.6 验证：不假定任何事情，不相信任何人，检验所有东西

一个强健的研发流程对于交付高质量和安全的产品的最基本。研发可能会因面临着要尽快地发布新产品的压力，而没有进行适当的测试和验证。建立一个多层的“多手”和“多眼”的独立验证方法可以减少不安全产品得以扩散的风险。端到端的检查和制衡流程确保了没有捷径可走，保护了客户投资和服务。

要求	还要考虑到
50. 供应商是否有网络安全实验室，在研发流程之外，在产品发布上市之前进行独立测试（也就是由非本产品的开发人员进行测试/验证）产品？	<ul style="list-style-type: none">研发团队有他们自己的业务目标，他们应该要在进展、成本和安全之间找到平衡点。独立于研发团队的实验室能够关注安全目标的达成情况，而且不受研发团队的影响。这个方法与职责分离所提供的保护是一致的。对供应商来说，很重要的一点是能够展示他们重视在产品发布之前，把产品做好。
51. 供应商的研发或市场人员是否能忽视实验室的发现？	<ul style="list-style-type: none">从质量和诚信的角度来说，有一些没有参与到项目中的人来确保产品遵从所有的质量和安全要求，这很重要——这些人不应受组织任何其他部分的影响，这些人应该有否决权。回到治理上面来说，内部实验室发现的问题是否有向高级管理层进行汇报？
52. 供应商可能有内部实验室进行渗透测试、静态和动态代码扫描以确保代码符合网络安全设计和编码要求吗？他们是否利用评估报告推动产品团队改进？	<ul style="list-style-type: none">这样的实验室的目标是聚焦安全，所有跟安全相关的东西。要求你的供应商展示这个团队的广度和深度可以让你对其安全方法的健壮性放心。但是，为了推动质量改进，公司应该要能够展示其在验证或测试过程中发现的问题不仅仅用于改进已经测试的产品，而且还用到公司研发组织的改进上。
53. 供应商的产品是否接受在其总部控制之外的其他独立安全验证？如果是，是什么验证，是如何运作的？	<ul style="list-style-type: none">测试团队之间的适当竞争，多种多样的工具、技术和方法可以提高安全测试流程的全面性和健壮性。这些流程越严格，你的供应商在这些流程上的投入越大，越能展示他们对长期安全和质量的战略倾向。
54. 供应商是否允许客户或政府在其的内部或外部实验室用他们自己的员工或安全顾问来测试他们的产品？	<ul style="list-style-type: none">你的供应商允许外部各方验证其产品质量的开放程度展示了他们对其方法的自信和信任。如果门总是关着，你可能会质疑：他们真的是认真对待质量和安全吗？
55. 如果客户或政府想要使用一个第三方的独立安全实验室或者采用通用准则（CC）认证（或类似的方法），你的供应商将会这样做或者将会考虑这样做吗？	<ul style="list-style-type: none">如果你的供应商愿意采取多种独立评估方法，甚至是跟外部各方一起采取多种方法，这向你展示了他们的安全承诺。你会发现作为一家公司，你会希望可以灵活地基于项目的风险和合同的大小选择评估方法。
56. 供应商的总部（或者业务集团），如果有的话，是否控制或干涉内部或外部实验室的独立性？供应商总部或他们公司是否有权力在客户或政府之前查看和修改任何报告或评估结果？	<ul style="list-style-type: none">有时候，供应商可能会面临着发布产品的压力，或者因为合同的原因，想要展示出某种形象。如果你的供应商宣称对他们产品的独立测试，他们要能够向你展示他们这个流程的发现是如何不受任何形式的影响或不会因为发布或其他压力而被篡改的。评估报告不应该在发送给客户或者其他的合适的利益相关方之前被公司更改，除非是为了避免无意造成的潜在漏洞被泄露。
57. 供应商总部的研发员工是否可以访问外部实验室使用的任何工具、流程或脚本？他们会对测试进行预估从而影响测试结果吗？	<ul style="list-style-type: none">如果供应商的总部知道实验室是如何评估好坏的，其总部有没有可能伪装他们的产品，让实验室的工具认为产品是好的？有一个严格的保密方法可以说明，任何测试实验室的目的只是提高质量和安全，别无其他。

要求	还要考虑到
58. 供应商的其中一个实验室或验证中心发现了一个缺陷或潜在漏洞，有什么流程来确保研发会解决该问题，在以后的产品中不再发生？	<ul style="list-style-type: none"> 我们大家都看到过一些例子，我们收到报告说出现了问题，但是之后没有任何改进。供应商要能够向你展示他们是如何系统地处理每个问题或缺陷的。他们要能够展示发现的问题，以及为了解决这些问题所采取的措施。 重要的是，他们要展示他们知道问题发生的真正原因是什么，采取了什么措施来改变流程、培训或者是模板等等，从而使问题不再发生。
59. 供应商的实验室或验证中心是否有能力在问题修复/打补丁之后对软件进行重新测试，确保问题真的被修复了，而没有增加一丁点儿其他的东西进去？	<ul style="list-style-type: none"> 质量和安全不是一个测试就能保证的。技术、威胁以及产品的使用都在变化。实验室和第三方必须有在产品发生变化或得到修复之后对产品以及变化本身进行重新测试。
60. 供应商如何把从验证中心学到的东西系统地融入到他们的业务流程中？	<ul style="list-style-type: none"> 供应商的内部、外部以及客户的测试可能发现具体的产品问题，此外还可能发现系统性的问题。如果你的供应商使用一个全面的集成的方法，他们要能够展示他们是如何利用这些知识，并解决潜在问题的。

4.7 第三方供应商管理

很多大型高科技公司都从第三方公司购买硬件部件、软件部件、交付支持和安装服务。如果第三方的技术或流程有安全弱点，这可能大大增加供应商产品和服务中的弱点，因为它们是嵌入在客户将会收到的产品中的。端到端的网络安全意味着供应商必须与他们自己的供应商一起合作，采用最佳实践的网络安全方法。

要求	还要考虑到
61. 供应商是如何对他们的供应商进行网络安全管理的？供应商是否建立相关安全标准并传递给他们的供应商？供应商所建立的标准多久进行更新，确保跟上最新的思想？	<ul style="list-style-type: none"> 对供应商自己的供应商的安全管理是不可或缺的。供应商必须将自身的和其客户的网络安全要求传递给他们的供应商，否则他们可能会接收到含有内在安全弱点的部件。 供应商应该要能够展示它是如何遵从产业安全标准或者建立安全准则，并把相关的标准传递给其供应商的。建立的标准要保持更新确保其涵盖了最新的想法和安全知识。 供应商如何评估其自身的供应商在安全活动中提供了有充足技能的充足资源？供应商要求其自身的供应商组建专门的安全团队吗？ 供应商是否有专门的角色、组织或流程将网络安全要求、标准、知识传递到其自身的供应商，并确保没有遗漏呢？
62. 供应商对他们的供应商有什么样的采购流程要求？	<ul style="list-style-type: none"> 供应商的所有供应商都可以满足所有安全要求是不太可能的。供应商有必要对其自身的供应商进行安全“认证”和审查，确保他们减少了使用安全方面较弱的供应商的风险。 要求其自身的供应商做安全“认证”可以帮助其自身供应商提高他们的安全能力，满足供应商提出的成为合格供应商的标准，因为供应商的项目需要其自身供应商跟他们一起合作来共同应对网络安全挑战。 公司应该能够展示它有一个健壮的、聚焦安全的选择供应商的流程，这个流程包含了如何对供应商的绩效进行评估、监管和改进。
63. 供应商是否与他们的核心技术供应商有合同条款或安全协议，提供了他们必须满足的一套综合的、风险告知（risk-informed）的要求？	<ul style="list-style-type: none"> 供应商自己的供应商必须知道对他们的安全期望是什么。安全协议是向供应商传递安全要求及法律责任的一个好方法。安全协议可要求供应商加强安全管理，让他们为其提供的所有产品的安全负合同责任。 公司应该能够展示它如何使用合同或者协议来确保它的产品中使用的所有部件，不管部件来自哪个渠道，都遵从安全程序和要求。

要求	还要考虑到
64. 供应商有什么样的流程来评估他们的供应商对安全条款或协议的遵从？供应商是否有一个计分卡或其它度量方法来促进他们履行责任，并驱动他们提高绩效？	<ul style="list-style-type: none"> • 供应商自己的供应商可能会变，安全问题随时可能发生。 • 供应商应该要能够展示它如何与它的供应商以合作的方式来进行绩效管理，如何一起合作解决问题。这可能包含了打分卡、审计和检验。
65. 供应商是否要求他们的供应商在发现他们产品漏洞时通知他们？供应商如何处理这个信息？他们是否有漏洞管理流程？	<ul style="list-style-type: none"> • 在任何产品或者部件中都能发现漏洞。一个负责任的公司应该以一种及时和一致的方式披露其产品中的漏洞。 • 供应商必须能够处理任何漏洞信息，因此应该能够展示一个端到端的漏洞管理流程，不管是谁把问题通知到他们的。
66. 如果他们的供应商不遵从、不想遵从或不能遵从供应商提出的网络安全要求，他们采用什么样的方法？	<ul style="list-style-type: none"> • 网络安全要求的遵从显然是有成本的，但收益不一定是明显的、直接的。 • 如果供应商自己的供应商不遵从他们网络安全要求，供应商采用什么样的方法来鼓励其供应商与他们合作一起应对网络安全挑战？如果其供应商不合作，他们采取什么措施？
67. 供应商是否遵从国际最佳实践标准，如海关商贸反恐联盟 (C-TPAT) 和运输资产保护协会 (TAPA)？他们通过认证了吗？	<ul style="list-style-type: none"> • 对于哪个标准最好，全世界可能有不同的观点，但是供应商应该能够展示它对全球广泛认可的标准的遵从和认证。 • 大家可能都知道，标准可能不完美，但是供应商应该能够展示他们能够超越标准，提供额外的保护和措施。
68. 供应商你是否对他们的供应商的安全实施现场审计？审计范围是什么？供应商需要描述如何与他们的供应商合作，解决审计发现的问题。	<ul style="list-style-type: none"> • 每个供应商和它自身的供应商都需要关注他们客户的需求。审计和检验帮助供应商保持聚焦，他们还要确保按要求交付。以合作的方法了解各自的需求有助于沿着正确的方向提高绩效。

4.8 制造

产品的制造商必须从很多供应商采购部件。他们必须确保在生产过程的每个阶段都没有引入安全风险。

要求	还要考虑到
69. 在制造方面供应商遵从什么国际标准和最佳实践？	<ul style="list-style-type: none"> • 生产中心有很多复杂的流程和工作。它们涉及到从质量到环境方面的很多标准。供应商要能够展示它如何在生产流程中应用全面的方法，采用最佳国际标准和方法。
70. 供应商应该描述其制造流程并提供这些细节：他们如何评估这个流程，包括上下游流程来发现任何受感染或者伪造产品的存在？	<ul style="list-style-type: none"> • 在制造过程中，部件有很多机会受到感染或者破坏，可以是在部件到达供应商的生产中心之前，也可以是在产品生产好了发货给客户之后。供应商要能够详细说明他们在全任一地方是如何处理备件和逆向回运产品的。要考虑的一个重要事情就是存储介质可能包含来自客户的个人数据。
71. 供应商如何确保他们从其供应商那里购买的部件就是他们在生产中心接收的部件，就是他们所期望的部件？	<ul style="list-style-type: none"> • 供应商要考虑到任何可以被破坏或感染的高技术部件可能已经被篡改了——他们的工作应该基于“不信任”的模式，而不是“信任一切”的模式。供应商如何开展这项工作的？

要求	还要考虑到
72. 供应商如何确保部件不会在他们的生产中心被他们自己的员工篡改?	<ul style="list-style-type: none"> 内部威胁问题是真实存在的。正如供应商需要验证和确保来料的完整性一样，他们也必须能够展示流程和管控措施，确保即将离开生产中心的货物没有被自己的员工篡改。
73. 在供应商的产品生产完成之后，发货之前，他们如何防止产品被篡改?	<ul style="list-style-type: none"> 生产完成但是尚未发货的产品提供了理想的篡改机会。供应商如何在其工厂和仓库保护产品，防止篡改呢?
74. 供应商如何确保客户收到的产品与它们离开其生产中心的时候是一模一样的呢?	<ul style="list-style-type: none"> 供应商接下来要考虑的这样的可能性：产品离开工厂的时候是安全的，但是可能在到达客户之前被篡改——在选择物流公司时要评估和考虑物流相关的全面流程。
75. 供应商如何做好部件的需求计划以确保他们尽可能常常拥有最新的部件?	<ul style="list-style-type: none"> 由于漏洞随时可能被发现，过度供应可能意味着在你的库存里有一些部件含有漏洞——即时生产可以降低这个风险。要有效做到这点，就应该把综合的销售预测自动与制造关联起来。
76. 如果客户的某个具体的软件加载到了他们的最终设备上，供应商如何确保被加载的软件就是研发授权的软件，没有被篡改呢?	<ul style="list-style-type: none"> 你想要你的供应商能够展示端到端的集成，能够展示硬件和软件在一个地方完成一道工序然后在另外一个地方完成另外一道工序，中间是没有篡改的空隙和或机会。
77. 供应商如何确保生产中心的人无法在产品上加载恶意软件呢?	<ul style="list-style-type: none"> 在生产过程中对软件进行保护非常重要。供应商应该能够展示如何约束这个环节，详细描述这类角色是否被划分为关键岗位，且要接受额外的监控以防止来自内部人员的威胁风险。
78. 在供应商的生产中心，他们如何确保所有的测试端口在产品离开时都默认关闭了，而且在离开生产中心后无法访问?	<ul style="list-style-type: none"> 生产设备经常需要访问产品测试端口。如果这些端口没有严格的管理，在生产结束时他们是开着的，那么就可能提供了机会，让黑客可以在产品安装时利用这些端口。你的供应商应该要能够展示所有的测试端口是如何自动关闭的，而且这是系统生产流程的一个部分。
79. 在生产过程中，供应商如何确保非授权人员不知道设备最终发往哪个客户，这样他们就不能篡改具体客户的设备?	<ul style="list-style-type: none"> 虽然生产中心的威胁更多地可能是针对一个或者一些具体的产品，但是必须要采取一切措施防止贿赂或恶意意图的情况，把某个具体客户的设备作为目标。供应商应该限制知道哪个具体产品发往哪个客户的人员。可以使用约定代码之类的技术，而不使用客户的名字。
80. 当客户因为订多了产品或者是取消合同而把产品以“未使用”的状态退回来时，供应商如何确保产品在它们退回前没有被篡改?	<ul style="list-style-type: none"> 供应商应该展示他们即使在产品返回时也是采用“不信任”的模型。他们的程序和流程应该假定产品受感染或者被篡改，应该再次验证产品的完整性。
81. 当一个坏件要被退回来的时候，供应商有什么流程确保产品在被发送到供应商的逆向中心之前，磁盘或者存储器件不含有客户数据?	<ul style="list-style-type: none"> 技术设备通常含有存储部件。因此由于错误或故障而产生的逆向退货可能会含有客户数据。供应商必须知道当地的数据保护法。 供应商需要能够展现他们的逆向和报废流程是如何运作的，如果不能进入存储介质去删除数据并保留数据删除的证据，他们将采取什么行动?
82. 若坏件在供应商的一个维修中心维修好了，他们如何确保所有的可替换部件还是原装的？（也就是没有被用人假部件替换）如何确保产品不含恶意软件？供应商会重新测试他们的产品吗？	<ul style="list-style-type: none"> 供应商在它的思维和流程中必须采用“不信任”模型。一个流程的很多阶段都可能会引入缺陷。当货物被维修或者被再次分发送时，供应商应该展示他们如何降低以下风险的：被篡改部件的渗透、使用伪造部件、恶意软件和错误配置。 对坏件进行验证能够防止被篡改、被植入或者被伪造的产品经过坏件逆向流程进入供应链。

要求	还要考虑到
83. 供应商是否有追溯部件的能力和流程？哪里都可能发生问题：供应商的硬件或者软件，从供应商的人员到第三方都可能发生问题。在发生问题的时候，他们如何能够追溯“谁”、“什么”、“为什么”、“什么时间”和“在哪里”这些与问题相关的信息。	<ul style="list-style-type: none"> • 一个准确而快捷的追溯系统可以协助快速定位问题源头，确定问题范围，这样供应商就能通知相关方采取措施防止问题扩散。 • 正向和逆向追溯的能力也有助于供应商识别问题的根因，识别能够采取的改进措施，防止相同的问题在将来再次发生。

4.9 安全地交付服务

如果在部署和支持产品时的流程不安全，那在设计产品时注重安全就没有什么意义。客户只是想确保当设备在支撑他们的业务时，它的运行和维护是安全的。

要求	还要考虑到
84. 供应商的服务工程师对安装好的和运营的客户设备和服务有什么样的接入权限？只要他们想，他们可以在任何时候接入任何设备吗？	<ul style="list-style-type: none"> • 供应商应该能够说明客户永远可以控制任何第三方访问其技术和服务的权限。因此供应商要能够展示一系列的流程和政策，指导它的员工哪些他们是可以做的哪些是不可以做的以及相关问责措施。 • 客户常常实施“明示书面许可”的原则，并要求有审计措施来确保对其政策的遵从。
85. 供应商采用什么方法来保护系统默认账号或者客户给他们用来做支持和维护工作的系统账号呢？	<ul style="list-style-type: none"> • 供应商政策和程序的其中一部分内容应该能够展示他们如何对待这些访问凭证，如何保护它们，什么时间归还，以及要做的独立验证和审计。
86. 对于他们的工程师的电脑或工程技术，供应商有什么样的控制措施？比如，供应商的工程师可以下载自己的软件到他们的电脑上吗？	<ul style="list-style-type: none"> • 如果员工的电脑被黑客攻入了，或者是感染了恶意软件，恶意人员能够通过员工的电脑窃取客户信息或者攻击客户的网络。因此供应商应该要详细说明他们所采取的保护和监控员工电脑的措施。
87. 供应商有什么样的流程和控制措施来确保他们的工程师只为每个客户使用正确的软件？	<ul style="list-style-type: none"> • 客户的技术常常非常复杂，包含了来自很多供应商的技术，有时候这些部件的集成要求一套具体的软件一起有效运行。供应商应该能够展示他们对你的技术做的任何更改或升级与作为客户的你所批准的软件一致，包括正确的版本和发布级别。
88. 供应商如何确保他们的服务或支持工程师不能篡改安装的软件，也无法安装含有漏洞的软件或恶意软件？	<ul style="list-style-type: none"> • 作为买家，你想知道你的支持工程师没有恶意/无意地给你留下一些你没有要求的東西，因为恶意的攻击者可能会替换硬件部件或者加载未经审批的软件来破坏产品的完整性，植入恶意软件或有漏洞的软件。 • 采用“不信任”模型，供应商应该能够展示他们如何防止恶意攻击者在软件部署或者升级过程中篡改产品或者部件。
89. 供应商应该详细描述在以下方面采取的方法：硬件加固、软件和硬件审查、针对特定客户的安全产品（如防火墙）。	<ul style="list-style-type: none"> • 要有很好的成文的最佳实践来指导你的供应商和你自身的ICT团队来“加固”（加强它以防止攻击）你所购买的设备。你所购买的设备可能也含有一系列的安全能力和特性。 • 任何安装、支持或维修活动都采用并遵从这个最佳实践，并且确保相关的功能正确地打开和关闭，从而让你自己放心。

要求	还要考虑到
90. 当供应商为了问题定位不得不抓取数据时，他们获得了客户的正式授权吗？他们仅抓取授权范围内的数据吗？他们如何管控所抓取的数据并保护个人数据呢？	<ul style="list-style-type: none"> 在技术设备中进行问题定位活动时可能会要求访问设备中的数据。要有一套双方协商一致的政策和程序在必要时确保对个人用户数据和商业数据的保护。
91. 如果供应商的支持工程师无法现场解决这个问题，抓取的数据需要发送到另外一个国家进行审视，如何对此进行控制，以确保遵从客户要求和当地法律的？	<ul style="list-style-type: none"> 有时复杂的故障一线工程师难以在现场解决，需要位于其它地方的研发工程师进行故障定位。 供应商和作为客户的你要就如何处理数据达成一致，例如，如果所需要的支持不在你所在的国家，你的供应商能够给你提供哪些灵活性？
92. 当不再需要为问题定位所抓取的数据时或者授权过期时，供应商处理数据的流程是什么？	<ul style="list-style-type: none"> 数据是客户的资产，仅能在授权的时限和范围内使用，服务结束时必须删除，防止这些数据被用于服务之外的其他目的。你的供应商是怎么做的呢？并如何确保真的做了呢？
93. 审计日志是证明在系统上发生了什么事情的一个重要证据。供应商怎么确认他们的审计日志含有所有的相关信息？	<ul style="list-style-type: none"> 供应商应该能够展示它记录和保护准确的审计日志的方法。 使用业界广泛认可并使用的审计软件可以让结果更为客观和可靠。
94. 客户依赖他们的供应商来保持业务连续性，尤其是在危机时刻，例如：服务中断、自然灾害。在困难时刻，你的供应商有什么样的装备，有多强的意愿来支持你？要求他们举些真实例子。	<ul style="list-style-type: none"> 供应商是否与其客户有定期的沟通渠道来与客户一起讨论网络安全要求、路标和计划，以求最大程度满足客户的网络安全战略，包括在困难时刻。 电脑使用者的风险无时不在，即使发生灾难时也会有风险，因为威胁制造者不会放过每一个机会。通常，你的供应商有丰富的国际知识、工具和资源，这些可能对它的客户有所帮助。例如，应对频繁的拒绝服务攻击，可能会要求快速地扩张设备，使用新的或不同的技术，你会想要你的供应商展示提供帮助的意愿，并且展示灵活性。 自然灾害确实会发生，你的供应商可能在维持你的业务连续性上发挥着重要作用。寻求他们的承诺，让他们在这些困难时刻帮助你，你也许能够据此来评估他们是否会为了你的业务成功而做出长期努力。

4.10 问题、缺陷和漏洞解决

不言而喻，在安全方面，没有100%的保证。因此，公司有效响应问题的能力，以及从错误中吸取教训对客户和供应商都是非常重要的。

要求	还要考虑到
95. 供应商是否有PSIRT/供应商CSIRT（产品安全事件响应团队/供应商计算机安全事件响应团队）或类似的团队？请详细说明他们的运作以及如何联系他们。这个团队需要遵循什么样的流程和要求？	<ul style="list-style-type: none"> 问题不可避免。当问题发生的时候，你想知道，供应商能够及时收到关于任何实际的或者感知的安全问题的通知。你要有追踪安全事故直到问题解决的机制，从而让自己放心。 产品安全事件响应团队在履行其职责时要遵从一套通过审批的流程，这很重要。

要求	还要考虑到
96. 供应商有什么样的机制跟客户的CSIRT或协调组织打交道，这样他们可以把问题通知到你的公司，并共同努力快速地解决问题？	<ul style="list-style-type: none"> 你的公司可能想要一个从一个内部中心点（一个PSIRT/供应商CSIRT）到多个点的多种联络机制。你的供应商应该展示他们在采用多种模型时的能力和灵活性。
97. 供应商是否有与安全研究团体合作的方法？	<ul style="list-style-type: none"> 一个不懂得倾听的组织也不会学习。供应商需要跟各种各样可能发现其产品问题的公司和个人合作。你的供应商这方面的工作是如何高效专业地开展的呢？
98. 如果发生重大事故，供应商如何确保客户能够并将会适时地得到通知，确保其公司里可以获得适当的资源来对事故做出响应？供应商应该能够清楚地描述其升级流程。	<ul style="list-style-type: none"> 如果你的组织内部发生重大安全事故，你希望你的供应商有一个可以快速通知你的机制，同时供应商的内部也有事故处理流程包括其内部升级流程，从而让你放心。 实际上，大多数企业不可能让有技能的资源闲置在那里。供应商如何证明他们理所当然会让其高级管理者知道这种情况，并可以而且会分配必要的支撑资源来解决问题。

4.11 审计

光说不做没有价值，说起来容易，描绘的蓝图也很漂亮——但是你说过你会做的事情，你会做吗，会是以你之前同意的方式，按照你同意的时间范围、成本、质量、和安全要求来做吗？你怎么知道是这样做的呢？严格的审计起到了关键作用，向你的客户和利益相关方保证，合适的政策、程序和标准得到了执行以交付所要求的业务结果。

要求	还要考虑到
99. 供应商有什么样的流程和机制来做内部安全审计和报告，确保相关的董事委员会能看到组织的真实风险态势、事故状况和后果，而不仅仅只是知道汇报给他们的那些？	<ul style="list-style-type: none"> 如果有正式的内部、外部、客户和第三方对网络安全活动的审计，这表明董事会愿意接受真实的反馈。 能够展示这些表示你的战略、政策和标准是“活”的，能够适应新的威胁和情况。 向董事会/委员会就网络安全活动、进展、和绩效做正式的汇报，这说明这项工作正常业务活动的一部分，而不是一个“项目”或者一个“特别”的活动。
100. 供应商有能够让外部利益相关人或者他们所委派的组织进行审计的机制吗？	<ul style="list-style-type: none"> 对关键利益相关人展示开放、透明的态度，并且接受外部审计和审查，这表明了决心，展示了不断学习的企业文化。 你对外部审查越开放，你得到的改善建议就会越多。



5 关于华为

华为的产品与解决方案覆盖170多个国家和地区，服务于世界超过三分之一的人口。我们有150,000名员工，平均年龄32岁，海外员工本地化平均比例为79%。截至2013年底，华为共获得281个LTE商用合同和162个EPC商用合同，其中110个LTE网络及88个EPC网络已经商用发布。

华为通过不断的创新保持在行业中的领先地位，拥有电信行业最有价值的知识产权组合之一。华为尊重和保护他人知识产权。华为每年将超过10%的销售收入投入到研发，45%的员工从事研发，2013年研发费用支出为307.34亿元人民币，占收入的12.9%。近十年投入的研发费用超过1519亿元人民币。

截至2013年12月31日，华为累计申请中国专利44,168件，外国专利申请累计18,791件，国际PCT专利申请累计14,555件。累计共获得专利授权36,511件。相比数量，华为更加关注知识产权的商业价值和质量。从2010年至今，华为已有466项3GPP LTE核心提案获得通过，位居业界第一。在FTTH（光纤到户）、OTN（光传送网）、G.711.1（固定宽带语音）等技术领域持有的专利处于全球领先地位。知识产权保护对华为持续成功至关重要。因此，华为坚决拥护对知识产权的保护。

华为在全球有16个研究所，28个联合创新中心和45个培训中心。约65%的营业额来自于海外。华为使用的70%的物料来自于中国大陆之外的供应商，其中美国的供应量最大，占32%（2013年从美国公司的采购额为72.37亿美元）。

华为为全球超过75个国家的120多个运营商提供管理服务，累计获得超过340个管理服务合同，帮助客户实现卓越运营。华为已经建立了基于云的IT解决方案，并与400多个伙伴合作，加快云计算技术在多个行业的商业应用。截至2013年底，我们已经在全球为客户建设了330多个数据中心，其中包括70个云数据中心。

2013年，华为终端整体发货量1.28亿台；其中全球手机发货近6000万台，移动宽带终端4450万台、家庭终端2440万台。消费者业务在全球智能机发货量达到5200万台，同比增长超过60%。



华为支持主流国际标准，并为这些标准的制定积极做出贡献。截至2013年底，华为已经加入了全球170多个行业标准组织和开源组织，包括3GPP、IETF、IEEE、ITU（国际电信联盟）、OMA、ETSI（欧洲电信标准化协会）、TMF（电信管理论坛）等。2013年华为向这些标准组织提交提案累计超过5,000件，在这些组织中在任185个职位，支持形成一致的国际标准方面的努力。

截至2013年12月31日，公司的员工持股计划参与人数为84,187人。员工持股计划将公司的长远发展和员工的个人贡献有机地结合在一起，形成了长远的共同奋斗、分享机制。这让我们能够有长远的眼光，保证在风险、激励和战略之间达成平衡。员工知道如果自己不能很好地服务客户，或者进行不当的活动，他们的股权和奖金将会受到影响。

Copyright © 2014 华为技术有限公司 版权所有

您可以为内部参考的目的复制和使用本文件。本文件未授予任何其他许可。

本文件“按原样”提供，不作任何明示或暗示的保证。任何保证均明确予以否认，包括但不限于不侵权、商用性以及特定目的适用性的保证。华为不负责保证所呈现信息的精确性。本文件提供的任何信息可能会被纠正、修改和改变，恕不另行通知。使用或信赖本文件所提供信息的风险自行承担。本文件提供的所有关于第三方的信息均来源于公开资源或他们发布的报告和报表。

、HUAWEI、华为、 是华为技术有限公司的商标或者注册商标。

本文档提及的所有其他公司的名称和商标均为其各自所有人的财产。