Cyber Security Perspectives

100 requirements when considering end-to-end cyber security with your technology vendors

John Suffolk

Senior Vice President | Global Cyber Security Officer
Huawei Technologies

December 2014

HUAWEI

Authors

I would like to express my gratitude to those who have made a significant contribution to this document: Harry Liu (Haijun), Jeff Nan (Jianfeng), Jupiter Wang (Weijian), David Francis, Andy Purdy, Debu Nayak, Peter Rossi, Andy Hopkins, Jessie Luo (Ming), Wave Xue (Yongbo), Nancy Li (Hualan), Wout van Wijk, William Plummer, Ludovic Petit, Ulf Feger, David Mu (Dejun), Eric Yang (Guanglei), and others who contributed to this paper directly or indirectly. Please accept my apologies if I have neglected to name you and thank you for your contribution.

John Suffolk

TABLE OF CONTENTS

December 2014

1 Executive Summary

In our White Paper, *Making cyber security a part of a company's DNA - A set of integrated processes, policies and standards*, published in October 2013[1] we detailed our comprehensive approach to end-to-end cyber security processes. We stated that we had taken the opportunity to document the Top 100 things our customers talk to us about in relation to cyber security. In essence, that list includes some of the questions anyone may wish to ask their technology vendors when it comes to their approach to cyber security. This White Paper details that Top 100. It is a list that focuses on what buyers of technology should ask their technology vendors.

The purpose is to provide suggestions based on questions posed to Huawei and our assessment of a range of "standards" and best practice so that buyers can systematically analyse vendor cyber security capability when asking for or responding to tenders.

In detailing this Top 100 we have taken reference from many sources:

- First and foremost, we have listened intently to our customers. What are their issues and concerns? What is it that they worry about? What are their requirements, the requirements of their industry or their country?
- As a global leader in the ICT industry covering everything from large-scale telecommunications infrastructure to cloud computing, enterprise and consumer solutions, we possess a wealth of knowledge in our 150,000 employees, scientists and engineers – we have harnessed their knowledge and their passion to get it right.
- Finally, we have scanned over 1,200 "standards", articles or "best practice" to ensure some level of consistency.

We recognise that in many countries the legal and industry requirements relating to cyber security are increasing. Indeed it is not uncommon to see governments and regulators beginning to pass the accountability, and subsequent liability for failure, of cyber security onto national critical infrastructure providers and computer or IT service providers. More and more companies will be forced to detail the approach they take to cyber security and detail what analysis and assessment they undertook on their technology vendors and service providers.

The time for a service provider to say "I didn't know" or "I thought they were good and capable" is rapidly running out. The time where buyers of technology do not use consistent evaluation questions for all of their suppliers is coming to an end. In a globally intertwined world the threat can, and does, come from everywhere. This Top 100 gives you a starting point for beginning to mitigate your own risk when evaluating a supplier's capability on cyber security, and crucially we believe the more demanding the buyer and the more consistent buyers are in asking for high quality security assurance, the more likely ICT vendors are to invest and to raise their security standards.

The bulk of the White Paper details the 100 items we believe, based on our research, you should consider when selecting technology vendors. They are broken down into sections covering: strategy governance and control; standards and processes; laws and regulations; human resources; research and development; verification; third-party supplier management; manufacturing; delivering services securely; issue, Defect and Vulnerability Resolution; and finally audit.

Each section details a number of requirements you should consider asking your technology vendors. We also provide some additional rationale why this might be important. Some of these questions may well help you in your own

[1] http://pr.huawei.com/en/news/hw-310599-cyber.htm

organisations in terms of what the internal auditors may look at, what your own governance might want to consider, and indeed what your Board and Audit Committee may ask.

Lastly, we make a number of pleas to the standards bodies:

- First of all, we should come together to reduce any overlap and duplication between the differing standards.
- Second, the various standards should be reconstructed so that they are built on consistent building blocks: for example, *governance and control* should be the same building block for all standards that require this, not a slightly different module in many standards.
- Third, we need to focus more on outcome measures where this is possible, rather than defining the input or task.

From our part we encourage as many companies, policy advisers, vendors and buyers as possible to consider this initial Top 100 as "version 1.0" and make suggestions on how it could be improved. In that spirit, we are delighted to announce that the EastWest Institute (EWI) has agreed to take this initial Top 100 and, using its extensive knowledge and networks, shepherd the evolution of updated and more tailored versions. We look forward to the Top 100 concept becoming an integral part of a buyer's approach and helping the ICT industry drive to greater improvements in product and service security design, development and deployment.

2 Introduction

In our White Paper, *Making cyber security a part of a company's DNA - A set of integrated processes, policies and standards*, published in October 2013[2] we detailed our comprehensive approach to end-to-end cyber security processes. We stated that we had taken the opportunity to document the Top 100 things our customers talk to us about in relation to cyber security. In essence, that list includes some of the questions anyone may wish to ask their technology vendors when it comes to their approach to cyber security.

We termed this list a "Reverse Request for Information (RFI)". In essence it is a potential list of cyber security requirements that buyers should consider asking their vendors if they can meet – i.e., we have reversed the process, we are asking customers to ask us, as vendors, how we deal with cyber security.

This third White Paper documents the Top 100 items and the approach we took to developing them.

Let us start with discussing what is it about cyber security that makes the development, agreement and implementation of an international set of standards, norms and practices so difficult to achieve. Is it because the prize of doing this is not sufficient to warrant the effort? Clearly that cannot be true when you read about the alleged substantial losses due to cyber crime. Is it because it has not reached the corporate agenda or political agenda? That cannot be the case either given the number of international government conferences on cyber crime and indeed the significant press reporting of data breaches, intellectual property loss and online service disruption due to denial of service attacks. Maybe it is because the scale of the challenge is too great and we do not know where to start, maybe it is because there are too many views on "standards", "best practices" and "guidance. We would certainly agree this may be a contributing factor as we stated in our last White Paper, "the problem with standards is that they are not

[2] http://pr.huawei.com/en/news/hw-310599-cyber.htm

standard". Finally when you analyse what is available they tend to focus on the enterprise or government department and in some instances the end-user, but few if any, really focus on the producer of the hardware and software – the vendor.

The reality is we will never get to "one standard" given the breadth of technology but what we can do is to focus on the key requirements that are often documented (maybe using different words) in many of the standards, codes and best practice, but position them to focus on what vendors should be collectively doing to improve the security of their products.

In this White Paper we set out to detail the most frequent non-technical questions we are asked by our customers and other stakeholders when it comes to cyber security. In this context, "most frequent" also means the ones that generate the most conversation or review or follow-up questions. We have taken "poetic licence" to tweak the questions posed to us to make them generic. We have also added questions to reflect the latest issues, such as the Snowden revelations, and filled in any gaps in the questions to make each section cohesive.

As a contribution to the ongoing debate and work on assessing "what does good look like" in cyber security, we put forward these questions as part of our collective continuing enhancement of knowledge.

In detailing these questions we have not tried to prioritise them or indeed put them into any particular framework or methodology. In essence for each of Huawei's core processes we have detailed the question where it broadly sits within a Huawei process.

This list by its very nature cannot be comprehensive for every industry or cover every law and every technical standard; that is not the purpose. The purpose is to provide suggestions based on questions posed to Huawei and our assessment of the subject of "standards" and best practice so that buyers can systematically analyse vendor cyber security capability when responding to tenders and can use this information to strengthen the quality of their RFIs and Requests for Proposals (RFPs) when seeking the best vendor(s) to meet their immediate and longer-term technology needs.

We fervently believe that the more demanding the buyer and the more consistent the buyers in asking for high quality security assurance the more likely the ICT vendors are to invest and raise their security standards.

Together we can augment the quality of security considerations in technology products and services, and from this we can collectively do more to enrich people's lives through the use of ICT.

3 The Methodology for Capturing and Refining the Questions

In detailing this Top 100 we have taken reference from many sources:

- First and foremost, we have listened intently to our customers. What are their issues and concerns? What is it that they worry about? What are their requirements, the requirements of their industry or their country? In doing this we are blessed with thousands of visitors to our HQ campus in Shenzhen where we demonstrate our values, our capability, and our policies and approach – this stimulates many questions and thoughts and we thank our guests for their insights.
- As a global leader in the ICT industry covering everything from large-scale telecommunications infrastructure to cloud computing, enterprise and consumer solutions, we possess a wealth of knowledge in our 150,000 employees, scientists and engineers – we have harnessed their knowledge and their passion to get it right.

  As a company we are passionate about supporting mainstream international standards and actively contribute to the formulation of such standards. By the end of 2012, Huawei had joined over 150 industry standards organisations, such as the 3GPP, IETF, ITU (International Telecommunication Union), OMA, ETSI (European Telecommunications Standards Institute), TMF (Tele Management Forum), ATIS, and the Open Group, among many others. In total, Huawei submitted more than 5,000 proposals to these standards bodies and we hold more than 180 positions supporting the drive for agreed international standards. In relation to standards and frameworks, we have contributed to the development of the emerging U.S. National Institute of Standards and Technology (NIST) framework, we support the enhancement to ISO27001, and we are an active contributor to the work and concept of ITU and 3GPP. We have referred to much of this material in informing the Top 100.
- Finally, we have scanned over 1,200 "standards", articles or "best practice" to ensure some level of consistency.

However, the Top 100 is not meant to be a comprehensive shopping list of questions that you pose to your vendor, although we do hope many of you will use the document as a reference. Asking the question is easy but skill is also required to understand the answer, ensure the answer is accurate, demonstrable and auditable.

Lastly, we make a number of pleas to the standards bodies:

- First of all, we should come together to reduce any overlap and duplication between the differing standards.
- Second, the various standards should be reconstructed so that they are built on consistent building blocks: for example, governance and control should be the same building block for all standards that require this, not a slightly different module in many standards.
- Third, we need to focus more on outcome measures where this is possible, rather than defining the input or task.

For our part we would be delighted to receive your feedback on this Top 100 – what should be added, removed or modified – so that we can produce a version in the future incorporating your additional input.

4 Questions and Issues to Consider in Designing a Strong Cyber Security Program

We recognise that in many countries the legal and industry requirements relating to cyber security are increasing. Indeed it is not uncommon to see governments and regulators beginning to pass the accountability, and subsequent liability for failure, of cyber security onto national critical infrastructure providers and computer or IT service providers. This is a dilemma, as in the event of say a substantial data loss, or loss of service, it is likely that the government or regulator will question the service provider on their approach to cyber security (assuming it was a security incident). More and more companies will be forced to detail the approach they take to cyber security and detail what analysis and assessment they undertook on their technology vendors and service providers. The dilemma is magnified by the fact that cyber security in its broadest definition is complex – from law to manufacturing, from service to human resources, from governance to research and development – few people in the world have such breadth and depth, and few therefore know what questions to ask and what evidence to look for.

The time for a service provider to say "I didn't know" or "I thought they were good and capable" is rapidly running out. The time where buyers of technology do not use consistent evaluation questions for all of their suppliers is coming to an end. In a globally intertwined world the threat can, and does, come from everywhere. This Top 100 provides a starting point for beginning to mitigate your own risk when evaluating a supplier's capability on cyber security.

In this section you will find the top 100 requirements we believe you should consider when considering the security capability of your vendors. Not all of them will be applicable all of the time. Not all of them will be applicable to all levels of your organisation. Not all of them will be applicable for all purchases. What we hope from this list is that you will gain a greater understanding of what you need to consider when selecting vendors and that you can use some of this list, supplemented with your own requirements, to drive up the focus of security in every technology vendor.

The questions are broken down into broadly the same sections as our second White Paper which we published in October 2013. In that document we published a comprehensive view of our approach to cyber security.

When reading the Top 100 you may well think that some of the questions could be consolidated. We have thought long and hard about this and have attempted to keep the questions quite specific. The more we consolidated, the more we risk losing focus. There is also subtlety in some of the questions where a follow-up question has moved onto the next stage of a lifecycle or process and is asking a slightly different question. Please feel free to change them as you wish as our overriding desire is to augment the quality of security consideration within all technology vendors.

4.1 Strategy, Governance and Control

If cyber security isn't seen as a priority by a Board and senior officials, it won't be seen as a priority by the organisation's staff. Ensuring that cyber security is imbedded into the organisational design, governance and internal control framework of any organisation is the starting point for the design, development and delivery of good cyber security.

The requirement	Additional considerations…
1. Does the vendor have a formal strategy and approach to risk management, information and cyber security risk?	• If there is no strategy it is unlikely that investment or resources will be allocated. • The organisation should understand the cyber security risk to organisational operations (including mission, functions, image, or reputation), organisational assets, and individuals. • The absence of a strategy leads to random results and a lack of consistency and repeatability of quality and security. • If there is a strategy but that is without effective approaches, that strategy will simply become empty promises.
2. Do your vendors have appropriate governance, organizational design, policies and procedures to support their strategies? And regularly update their strategies to adapt to the latest cyber security environment and requirements?	• If cyber security is built into the governance and fabric of "the building", it will then have a comparable importance to say the Finance Committee or the Strategy Committee. • Identifiable and demonstrable Board committees, policy papers, standards and key audit control points all imply that this is embedded in the organisation and therefore taken seriously. • If it is not important to the Board and senior leaders it will not be important to the staff, so this must be demonstrable.
3. What governance structure does the vendor have in place that demonstrates that cyber security is a core strategic and operational focus of the business? Do they have a dedicated Board Committee on cyber security, how does this operate?	• A dedicated committee led by a senior board member will show that this is company priority and not just a tactical activity delegated to the technical staff. • If the committee has key board members on it, as they are the only ones who can effect substantial change, it shows top-level commitment. • If such a committee is a decision-making body that sets the overall direction of cyber security strategy and approach, it proves the Board is actively engaged. • If board members are briefed and they carry out reviews when things go wrong, and they are involved in crisis management, it shows they are close to the operational reality. • If senior management clearly expresses their expectations in terms of strategic objectives and priorities, available resources, and overall risk tolerance, and assigns responsibilities in achieving results, that will ensure that everyone understands the importance of cyber security.
4. How does the vendor ensure that cyber security gets addressed in its business, how are Board Members connected into what is happening in the business, and how are they held accountable?	• There should be a clear link showing how any top-level Board Committee oversees the execution of the strategy. • Vendors should be able to demonstrate integrated links from the strategy through to the furthest point in the business (next to the customer) and back. • Can the vendor provide evidence that board members and senior executives have clear personal responsibility for taking action on cyber security, or do they just sit on a committee?
5. What approach does the vendor take to ensure that every part of their business considers the impact of security? How is this done in a consistent and repeatable way?	• Cyber security is everyone's challenge and everyone must be part of the solution. The ability to demonstrate this "all-of-company" approach to deciding what happens and what doesn't, ensures that security becomes part of the DNA of the business. • The more that cyber security is centralised to a handful of individuals in "HQ", the more it only becomes "their" problem. End-to-end means end-to-end resources must be involved. • How do other parts of the business take this corporate strategic direction and use the information as inputs into their risk management and operational process?
6. What is the vendor's approach to resourcing cyber security activities? Is it all done via a central dedicated team or is each part of the business involved including regional security resources?	• Whose problem is it? If it isn't my problem and my performance does not include the best approaches to security, then I will not address the challenges. The organisational design and the way a vendor embeds security determines if it really is an all-of-company strategy or just a bolt-on being addressed by a few people. • Companies should be able to demonstrate for all major functions how risk management and cyber security is embedded into their activities including processes and resources. • Companies should also be able to demonstrate how local security requirements are monitored and dealt with within corporate processes.

The requirement	Additional considerations…
7. Every company has security incidents, how does the vendor learn from their security incidents? How are they reviewed by their senior executives so that learning is incorporated back into what they do?	• A "blind" board is a poor board. It is often said that only those at the very top of an organisation can stimulate the biggest change of behaviour and approach. If they do not see the security failings or incidents, they do not understand what their customer sees or recognise what they have to personally change in their business. • The company should be able to demonstrate regular reporting to a Board-level committee on what incidents have occurred, what lessons have been learnt from those incidents and how have things been improved following the incidents.
8. Have the vendor's internal IT systems ever been a victim of a cyber-attack, and how have they learned from this to improve their products and services?	• A company's ability to learn from its own security challenges better equips it to understand the challenges its suppliers might face and how to mitigate challenges from a risk perspective. • A company should be able to demonstrate "how it takes its own medicine" when it comes to cyber security.

4.2 Standards and Processes

To get a repeatable quality product demands repeatable quality processes and standards and a similar approach by your vendors employees and suppliers. Cyber security is the same: if their processes are random or their approach to cyber security standards is random, the quality, safety and security of the end-product will also be random.

The requirement	Additional considerations
9. Does the vendor adopt and support any global standards within the broad definition of cyber security? What standards do they conform to and in which standards bodies do they hold senior roles or actively participate in?	• If the culture of the business is to adopt international standards whenever possible and to be open to integrating best practices into business processes it is likely to be in harmony with the latest thinking on cyber security. • A company that is part of the standards community supporting the development and adoption of cyber security standards demonstrates that the company is open to adopting best practices and standards. • Can your vendor demonstrate support and acceptance for the technical standards that are applicable to your company • in order to enhance the trustworthiness of independent software testing you may want to explore how the vendor adopts testing best practices in industry (such as Common Criteria), and strive for standardization so as to enhance the internal cyber security testing capability and quality
10. How does the vendor determine what best practices and standards (or laws) should be followed? What processes did they go through to determine and resolve conflict between laws and standards and how do they keep this up-to-date?	• The problem with standards and best practices is that "good" is in the eye of the beholder. A mechanism to keep up-to-date shows customers that they are getting the latest requirements. To really apply the broadest set of views, standards and ideas means that a company must continually assess how others are addressing the challenge and build new improved thoughts and requirements into their operations. • The company should be able to demonstrate a comprehensive approach to scanning the world for best practices, standards, codes etc., and distilling this into a set of company policies, procedures, and baselines.
11. In an effort to conform to a range of technical standards, what teams or capabilities does the vendor have to support a wide range of management and technical standards including cryptography?	• You will need to extend this list of requirements to specify a range of both management/ process standards, such as ISO 27000 series, and a range of technical standards for your industry, such as X.805, PCI, and OWASP. • You will need to satisfy yourself that the vendor can accommodate existing standards and is prepared to modify their technology as standards are revised and new standards are developed. • Cryptography/ encryption is a specialised area, sometimes governed by local laws. You will want to satisfy yourself that your vendor has encryption/cryptography dedicated resources and understands legal as well as technical requirements

4.3 Laws and Regulations

The law is complex, variable and ever-changing. As you will know, just because a country has a law does not mean that it is implemented; if it is implemented, it might be implemented in different ways or there might be different interpretations of the same law or code. Laws, codes, standards and international controls add complexity and risk to a supplier and a business.

The requirement	Additional considerations
12. How does the vendor assess and attempt to understand the cyber security and privacy laws and requirements in the countries in which they operate? How is this information used in the design, development and operation and maintenance of their products and services?	• In addition to the fact that inconsistent laws in different countries where a global company does business pose obvious challenges, the problem with laws and codes is that the interpretation might be different. It is important that a company has a mechanism to keep up-to-date on and assess laws and codes so that customers know they are getting products that meet the latest requirements. To really consider the broadest set of views, standards and ideas means a company must continually assess how others are addressing the challenge and build new thoughts and requirements into their operations. • The company should be able to demonstrate a comprehensive approach to scanning the world for best practices, standards, codes, etc. and to distilling this to inform continuous improvement of company policies, procedures, baselines, etc. • Given the variable, yet critical nature of laws, a company should be able to demonstrate how it deals with unclear or conflicting laws in product development and service in a consistent and repeatable way. • The law is as important as a technical standard or requirement. The vendor should have the ability to show how they meet the legal requirements of a country or region – especially in the areas of personal privacy and data protection. • Daily business activities follow processes. Therefore, the ability to demonstrate that compliance requirements are considered in designing products and services shows a holistic approach to all requirements.
13. How does the vendor ensure that their processes are aligned with local laws and requirements? What do they do when a local law conflicts their policies, standards or processes? Has your vendor made public statements in relation to its relationships with governments?	• The law is the law and it is important that your vendor can show that their equipment and services are legally-compliant. • Every company that operates in other countries has the challenge of ensuring that the voice of the local teams is heard in HQ. Vendors should be able to demonstrate how this voice is integrated into HQ thinking and product development. • The company should be able to demonstrate how it deals with conflicting laws and requirements with the local law taking precedence. • The vendor should be able to explicitly state whether it is under any obligation to provide information/ data to another Government • The vendor should disclose its relationships with any governments relating to national security, the introduction of "backdoors," or the weakening of encryption or security protection. • The vendor should be able to explicitly state where data will be stored and what legal jurisdiction governs that data.
14. How does the vendor ensure that their processes and products conform to export control and operating laws (including cryptography) of the country in which they are deployed?	• A company should be able to demonstrate integrated governance, policies and procedures that span the sales, service, contracting and product design processes that cater to specific legal requirements – whether they are trade compliance, licence management, export control, etc. • A company should also be able to demonstrate appropriate control points that confirm that key requirements are being executed. • If they cannot do that, the buyer runs the risk of having to replace equipment or services that breach laws.
15. What is the vendor's corporate policy on intellectual property rights?	• A company should be able to set out a range of policies, procedures and approaches that detail its response to such things as licensing, IPR and cross-cultural differences. Ethical and legal challenges occur in many countries but responses should be consistent and embedded in the way a company does business. You should ensure that the vendor has an internal code of conduct or business conduct policy.

The requirement	Additional considerations
16. How does the vendor ensure that their sales team only sells products and services that comply with local laws and regulations, including any export controls or trade sanctions?	• Sales teams are there to sell, this is what motivates them and it is crucial for the success of the business. They might also believe that rules and regulations get in the way of sales. In addition, buyers might not have the strongest procurement resources and therefore a vendor must be able to demonstrate how their processes protect the buyer. • It is important for a vendor to be able to show a set of integrated processes that combine sales, legal and delivery or support, and that are aligned with a buyer's internal and external requirements.
17. How does the vendor review contracts to ensure that they contain accurate information on their capabilities in terms of cyber security?	• Projects and contracts can frequently be very complex, long-term by nature and include input from many parts of numerous companies. A vendor should be able to demonstrate that what is agreed and contracted for fulfils the buyer's objectives, including laws and regulations.
18. Given that all large high technology-based companies use other vendors' technology, the vendor should be able to clearly describe licensing and control mechanisms in place.	• You want to satisfy yourself that the third-party components that your vendor uses have been appropriately licensed. This avoids any potential conflicts downstream that might require swapping hardware or software, resulting in expensive disruptions.

4.4 Human Resources

Many companies say that their people are their most important asset, which is true. However, from a security perspective, they can also be a challenge. The way people are employed, trained, and motivated and the way their performance is managed often determines the difference between success and failure – not just in the area of cyber security, but also in the delivery of the overall company strategy.

The requirement	Additional considerations
19. Does the vendor include the management team in the cyber security awareness education of all employees? If so, how is this done? Do their senior executives and Board of Directors receive continuous training on legal compliance?	• It is important that awareness education is seen to matter to the management team – including middle management – otherwise employees will ignore it. For that reason, management should attach importance to and "walk the talk" by participating in awareness training for all employees. • The ability of a vendor to demonstrate that "we are all committed" and "it is the responsibility of each one of us" ensures a greater chance of success. • The understanding of legal compliance by decision makers and supervisors of daily operations of the business will impact the stable and continuous operation of the company. They should have knowledge of cyber security laws.
20. Not all positions carry the same risk in terms of the insider threat. Does the vendor identify "sensitive" or "critical" positions when it comes to cyber security?	• It is a "must" to ensure that the critical positions that offer services to customers are trusted and provided with essential protective measures. • Established mechanisms to identify critical positions, and focus on the potential risks of these positions to conduct effective management of the positions, show the maturity of a vendor. • For example, the positions that have direct access to your core ICT and can directly change product software can bring more serious threats to products and services.

The requirement	Additional considerations
21. What approach does the vendor take to recruiting and vetting employees in "sensitive" or "critical" positions? Does the vendor undertake background check, exit vetting and sign appropriate contractual clauses?	• This shows a consistent approach to people quality and integrity. It recognises the risk of insider threats and demonstrates an approach to mitigate those risks. • A vendor's ability to demonstrate this shows it takes a holistic approach to cyber security.
22. What processes and mechanisms does the vendor have in place to provide regular awareness and specific training on cyber security which is consistent with employees and contractors' duties, and policies, procedures, and other requirements? How do they know people have taken the training?	• How does the vendor make cyber security a basic culture that embedded into the essence of its culture and accepted by all employees? What basic systems and procedures does the vendor establish to assure this. • Cyber security is a long-term requirement that means that everyone's knowledge must be frequently updated. If your vendor's knowledge is not kept up-to-date, it might indicate a loss of focus and lack of preparedness. • When considering your vendor, it is worth determining if they have regular training and awareness, use a variety of global and local training and awareness tools, and if they do additional work in the functional areas i.e. more detailed training on the specifics. In essence, you will want to satisfy yourself that the organisation's personnel and partners are adequately trained to perform their information and cyber security-related duties and responsibilities, consistent with related policies, procedures, and agreements.
23. Does the vendor have any policies that focus on increasing the competence and understanding of those undertaking "sensitive" or "critical" positions?	• The implication is that because you know a position is sensitive or critical, it has different, stricter requirements. A company should be able to demonstrate that the risk to a customer is more than just knowledge; it is also about experience and it is about values such as integrity.
24. Many countries have laws on anti-bribery and anti-corruption, how does the vendor deal with this with their employees?	• A vendor must be able to demonstrate how it makes its employees aware of varying national laws and internationally-accepted best practices in terms of actions to prevent bribery or corruption. • How does the vendor publicise and embed the values of the company and what is "right or wrong" in a consistent way among its employees?
25. Does the vendor have a mechanism where staff can notify management (in an appropriate way) when they feel that things may not comply with policies, laws or regulations?	• Often a company's employees will see things that Managers do not. The establishment of corresponding notification mechanisms can enable the company to find a problem at an early stage and make improvements. A self-learning closed-loop improvement system needs to show how the company deals with things that just do not fit their processes, and employees often need to use such mechanism(s) to flag things that they do not think are right.
26. What is the vendor's employee exit strategy and how do they use the knowledge gained from that process in the improvement of their policies, procedures, and culture?	• Employees leave for many reasons; some of them because they feel uncomfortable with what they see. Some of this feedback might indicate security concerns. Vendors should be able to demonstrate that they take all forms of input - including from employees leaving the company - on the way a company is run and its policies and procedures as a way of solving issues and improving the business.
27. Does the vendor have a formal disciplinary guide on cyber security?	• The vendor needs to be able to demonstrate how they balance incentives and disincentives that create the right culture of security for the customer, the company and the employee. • If an employee knowingly goes against a company's policy on cyber security, there should be clarity on what policy and process will be adopted and what potential disciplinary actions may be taken against them.
28. When disciplinary action is taken with an employee, how does the vendor account for the potential failure of their manager or supervisor, i.e. do they address any management or supervisory issues as well?	• It is important for a company to demonstrate that managers have a role in the performance and conduct of their team – they cannot just blame someone else for their team's performance and actions. A company should be able to demonstrate how they ensure accountability and proportionality in incentives and disciplinary approaches for the individual, manager(s) and team(s).

4.5 Research and Development

Companies do not want to use their scarce capital to buy high technology products from companies that do not have rigorous R&D processes that deliver consistent high quality and safe products. Nor, do they want to see vendors making investment decisions between investing in a new product or investing in making all products safe and secure. Cyber security, like quality, cannot be bolted onto a product. Companies need to demonstrate their long-term commitment to enhancing their R&D approach to cater for cyber security design, development and deployment in addition to investing in the next generation of products.

The requirement	Additional considerations
29. Does the vendor have a formal set of R&D processes that cyber security requirements are embedded in and are they based on any industry standard or best practice?	• If a company cannot demonstrate a mature set of processes and approaches to R&D, they have no firm foundation on which to embed quality and cyber security. Random processes equal random quality, random security outcomes and increased risk. • There is no perfect model or one global standard for security so a company needs to demonstrate how it utilises knowledge and best practices from many sources.
30. How does the vendor's R&D processes cater to, and assess the effectiveness of, cyber security requirements including a dynamic threat environment. What mechanisms do they use to determine what is mandatory and what is just good practice?	• Whilst many will see cyber security as a part of quality, which it is, it does have different elements – particularly around how dynamic the threat can be and entrance points for attack can vary. Vendors should be able to demonstrate a closed-loop approach of embedding security requirements into R&D, finding new issues or knowledge, and testing the effectiveness of security outcomes. If they are not effective, they must change them and then loop back to embed new or modified knowledge and learning to enhance cyber security.
31. Customers around the world have differing and sometimes conflicting security and functional requirements; does the vendor have a set of integrated processes that takes a customer requirement all the way through to the end of the relationship and assesses what can and should happen?	• Different laws and regulations, social cultures and user preferences in different countries shape various customer requirements. A set of fixed and inflexible processes cannot satisfy the need for customer or jurisdiction-specific requirements. Lack of proper management may create the result that what the customers get is not what they expect and may be even contradictory to the function they want. Vendors should be able to show effective management of different or conflicting requirements.
32. Does the vendor have a product life-cycle strategy that ensures the product is maintained from a security perspective over its life? What does this tell you and how do they use it?	• As a potential customer you will want to assure yourself that the product(s) you are buying will have an appropriate life-time use (say 3-5 years) so you can recoup your purchase cost. The vendor should be able to detail how they go about managing the life-cycle of a product or a set of associated products. In essence, they should satisfy you that the product(s) you buy will not be obsolete or not upgradeable, in a short time-frame. • if security requirements conflict with other requirements, such as function, reliability, performance and so on, how does the vendor decide which requirement has primacy?
33. The vendor should detail how their main product development process works and how progress is reviewed and continuously improved from a technical and quality perspective. They should detail what reviews, checkpoints and go/no-go decision points are built into that process.	• Most technology is complex, so understanding how your vendor builds in multiple technical reviews, business reviews, security reviews, quality reviews, and checkpoints into their processes should give a customer comfort about a vendor never losing sight of the objectives and success outcomes.

The requirement	Additional considerations
34. Modern software is very complex. It usually contains millions of lines of computer code and thousands of components from different suppliers. What procedure and technology does the vendor use to ensure the right components are used at the right time?	• The development process may be defined very well. However, the lack of an effective IT management platform to support the processes may make it difficult to implement the company regulations and customer requirements. If the various elements that make a complete computer system are not included in "configuration management", or not controlled properly, then systems may not work consistently, and you cannot track and trace what is being used and where it is being used.
35. Configuration management is a systems engineering process, and supporting technology for establishing and maintaining consistency of a product's performance, functional and physical attributes is required throughout its life. In complex technology environments this mechanism is a cornerstone for consistent, high quality and secure code. What is your vendor's approach?	• The company should be able to demonstrate systematic "configuration management" or control systems that prevent technology elements from being maliciously tampered with or the wrong elements being embedded in product development and compilation. • This should include version control, change management, third-party tools and components.
36. Segregation of duties is important to limit threats and potential damage, how is this implemented by the vendor in R&D, especially for software engineers?	• It is important to understand how insider threats are mitigated. Segregation of duties is an important part of this. Vendors should be able to map out their R&D roles and what parts of the R&D process each role can be involved with. From a security perspective, the ability to limit the phases, actions, products, and source code an individual has access to can limit risk.
37. Many technology companies embed third-party software and open-source software into their own computer code, how does the vendor track and manage what is in each of their products?	• Whilst your vendor's code and computer technology may be built to high standards, there might be weaknesses in other vendor's technology that they use. Knowing where a problem is and whose software or hardware is involved forms a key part of assessing the risk and carrying out remediation activities.
38. Open-source and third-party software can often be found on many websites. How does the vendor know that the software they are downloading is legitimate and does not contain malware or back doors?	• If a vendor does not strictly control what software components are used and where they have sourced them, it demonstrates a lack of quality control. If they have very rigorous processes to ensure they only take source code from reputable sites, this can be a risk-mitigating factor. • Some rogue sites may have tampered with open-source code and introduced malware which is why vendors must be vigilant.
39. Before your vendor uses software from a third-party, what process do they go through to ensure any known vulnerabilities are resolved before it is accepted for use and after it has been deployed?	• A good adage for buyers and sellers is the ABC model: Assume nothing, Believe no one, and Check everything. You should check that your vendor validates that the third-party software he is embedding in your product has all known vulnerabilities fixed before he ships your product. This should be a continuous process as new vulnerabilities may be found after a product has been launched • If a vendor is imbedding third-party components in to their product you should verify with your vendor that the third-party software is covered by a lifecycle management process?
40. How does the vendor ensure that the defect in a third-party piece of software, or an open-source component, or even a common software routine is fixed wherever that code is used?	• Often a third-party component may be used in multiple vendor products or even in the same product in multiple locations. Therefore, fixing third-party vulnerability requires that your vendor knows every product in which he has used this component; otherwise there is a risk that vulnerabilities do not get fixed in all products.

The requirement	Additional considerations
41. Does the vendor use multiple development languages and tools in their products? If so how do they catalogue those tools and whether they are up-to-date and are supported?	• Your vendor might use a range of tools, software and code from many third-parties and is vulnerable to the fact that companies merge, fail and change their strategies. Because of this, you should satisfy yourself that your vendor has a formal process of reviewing, approving and blocking third-party products and components based on their quality, architecture and product development road-maps. • Your vendor should be able to demonstrate a strategy and a set of mechanisms to ensure that only supported and safe third-party tools and components are embedded in their products.
42. The vendor should describe their approach to being able to track and trace their end-to-end R&D process and the software tools they use – by each open-source or third-party software they use	• Things will go wrong, people may do bad things. If something happens in your company and your systems are down, or compromised in any way, how long will you give your vendors to find the problem? A day, a week, a month? Complex technology might contain thousands of components and many millions of lines of computer code. You should ensure that your vendor can trace all components used in all products sold to all companies, and you can trace all products you have purchased. Vendors should also be able to trace all people involved, what they did and when, as well as all authorisations for that work.
43. Complex products tend to generate millions of lines of computer code; does the vendor have automated code scanning environments to automatically test for coding practice as part of their R&D process?	• Good engineering looks to automate as many tasks as possible because you can "guarantee" quality and drive consistency. Your vendor should have a number of automated tools and techniques to dynamically scan your products for a wide range of issues – this should, ideally, be automatically fed back into the vendor's quality management system. • Automation cannot solve everything and spot everything so a blended set of approaches should be utilised to ensure a company does not become over-reliant on pure technology-based verification.
44. The vendor should describe their mechanisms for determining if a product can be released to the market, and the authorisation process.	• Satisfy yourself regarding the rigour of the approval process. You will have heard from many ICT teams, maybe your own company's, where they say that something is 95% complete. Your vendor should be able to prove that the product is 100% complete in all ways and this should be reviewed by non-project team members. • There should be evidence of multiple technical and quality assurance or security reviews, and the final authorisation should not be left to the software engineer to decide – you should not mark your own homework.
45. Throughout the product development cycle and the life of the product, defects will be found. How does the vendor trace all defects and ensure that the defect has been fixed in every product that might use that component?	• As a customer, you do not want to be finding the same problem time and time again. Nor do you want the same problem occurring in different products. For that reason, you need to know how your vendor tracks defects and issues and how this integrates into R&D and training and other areas.
46. The vendor should describe how they maximise the growth in their competence on cyber security. Do they have centres of excellence or a security skills centre? How does this work?	• Not every person in your company can be an expert in everything. In large-scale complex technology engineering this is also the case. Therefore a vendor needs to be able to assess the breadth and depth of its security capability and make sure the right teams have access to this important skill and expertise, and you need to know how this is done.
47. Threats are constantly evolving, how does the vendor monitor these and take them into account in their design, development and deployment phases?	• If your vendor is always looking in the rear view mirror to drive a car they might drive into a brick wall. You will want to satisfy yourself that your vendor is looking forward, anticipating the next issues and catering for them in product design and development. • Vendors should be able to demonstrate that they take every source of threat or attack into account and they should be able to show how this feeds into designs and other requirements.

The requirement	Additional considerations
48. The vendor should detail how their processes are supported by the relevant technology. For instance, how do they use any threat databases in their testing? Or, have they built a library of test cases?	• Whilst your vendor might tell a good story on processes and standards, they need underlying supported and integrated company technology to be efficient and effective. Is this the case with your supplier? • For each of the processes or departments of your vendor, a set of integrated technology platforms should be in place to support their operation and the vendor's business objectives.
49. The vendor should describe their approach to release management. Some vendors have a single code base for all customers for all countries; some vendors have a code base and then branches for specific regions or countries and customers. Both core methods have strengths and weaknesses. Which approach do they take?	• There is no right model for one product around the world or one product per country or customer. If there is only one product for the world you might lose flexibility and your vendor may not want to adopt your requirements. If there are hundreds of different products doing broadly the same thing, a supplier's cost will go up and efficiency will go down. The key is to understand how your vendor strikes the right balance and how they manage the challenges of the option they adopt.

4.6 Verification: Assume Nothing, Believe No One, Check Everything

Whilst a robust R&D process is fundamental to delivering quality, safe and secure products, R&D can be under pressure to launch new products quickly without the right testing and verification. Having in place a multi-layered "many hands" and "many eyes" approach to independent verification reduces the risk of unsafe products being distributed. An end-to-end checks and balances process ensures a "no shortcuts" approach and protects customer's investments and services.

The requirement	Additional considerations
50. Does the vendor have a cyber security laboratory that independently verifies (i.e. tested / verified by people who did not develop the product) their products, in addition to the R&D process, before they are released to the market?	• R&D teams have their own business objectives. They should strike a balance between progress, costs and security. A laboratory independent from R&D teams can focus on the achievement of security objectives outside the influence of R&D teams. This approach is also consistent with the protection afforded by segregation of duties. • It is important that a vendor demonstrates that they value getting products right before they are launched.
51. Can the vendor R&D or Marketing ignore the findings of this laboratory?	• It is important from a quality and integrity perspective that there are people, not involved in the project, ensuring that products conform to all quality and security requirements. These people should not be influenced by any other part of the organisation; they should have a right of veto. • Relating back to governance, is there any reporting to senior management on any problems found by the internal laboratory?
52. Does any internal laboratory that the vendor might have, undertake penetration tests, static and dynamic code scanning to ensure that the code conforms to the cyber security design and coding requirements? Do they use the evaluation report to push product teams to make improvements?	• The objective of any such laboratory is to focus on security, all things security, so asking your vendor to show the breadth and depth of any such team should give you comfort in the robustness of the security approach. • However, to drive quality, a company should be able to demonstrate how the issues found in this verification or testing are used not only to improve the product that has been tested but also the fabric of the company's R&D.

The requirement	Additional considerations
53. Does the vendor subject their products to any other independent security verification outside of their HQ's control? If so, what verification and how does this work?	• A little bit of competition between testing teams and a variety of tools, techniques and approaches can improve the completeness and robustness of any security testing process. The more stringent and the greater the investment your vendor pays to these processes shows their strategic intent to long-term security and quality.
54. Does the vendor allow customers or governments to test their products in their internal or an external laboratory with their own staff or with security advisers?	• The level of openness your vendor extends to external parties validating the quality of their products shows both confidence in their approach and trust. A door that is always closed might make you question how serious they are about quality and security.
55. If a customer or government wanted to use an independent security laboratory run by a third-party or adopt Common Criteria (or similar approach), is this something your vendor would do or would consider?	• The willingness of your vendor to embrace various methods for independent evaluation, even with external parties, will give you an indication of their security commitment. • You may find as a company that you want the flexibility to choose the evaluation methods based on the risk of your project and the size of your contract.
56. Does the vendor's HQ (or business groups), if at all, control or interfere with the independence of the internal or external laboratories? Does the vendor HQ or their company have the right to see and modify any report or assessment before the customer or government sees it?	• Sometimes a vendor might be under pressure to launch a product or because of contractual issues may want to present a certain image. If your supplier claims independent testing of their products they should be able to show you how the findings of that process have not been influenced in any way or tampered with because of launch or any other pressures. • Any report from an evaluation process should not be modified by the company before it is sent to the customer or any other appropriate stakeholder other than to protect any inadvertent potential vulnerability disclosure.
57. Does the vendor's HQ R&D get access to any of the tools, processes or scripts that are used by the external laboratories? Could the vendor HQ "second guess" the tests so that the vendor could influence the test results?	• If the vendor's HQ knows how the laboratory will assess "good", is it possible for HQ to mask their products so the laboratory tools think it is good? Having a rigorous approach to confidentiality will indicate that the purpose of any testing laboratory is to improve quality and security, and nothing else.
58. When one of the vendor laboratories or verification centres discovers a defect or potential vulnerability, what is the process for ensuring that R&D fixes the issue so that it does not recur in future products?	• We have all seen instances when we have reported that something is wrong but that nothing improves after that report. Vendors should be able to show you how they deal with every problem or defect in a systematic way. They should be able to demonstrate any issues that have been identified and what action was taken to resolve these issues. With this, it is also important for them to show that they understand the real reason why the problem occurred and what actions they have taken to change any processes, training or templates, etc. so it does not recur.
59. Does the vendor laboratory or verification centre have the ability to re-test the software after it has been fixed / patched to ensure that the problem has truly been resolved and nothing else has been added?	• Quality and security are not about a single test. Technology, threats and the use of products change. Laboratories and third-parties must have the ability to re-test products and to re-test changes to products after those changes or other fixes have been made.

The requirement	Additional considerations
60. How does the vendor systematically integrate the learning from their verification centres into their business processes?	• A vendor's internal, external, and customer testing may find systemic issues in addition to specific product issues. If your vendor uses holistic, integrated approaches, they should be able to demonstrate how they take onboard this knowledge and address the underlying issues.

4.7 Third-Party Supplier Management

Many large high technology companies use third-party companies for hardware components, software components, delivery support and installation. If the third-parties' technology or processes have security weaknesses, this can significantly increase the weaknesses of the vendor's products and services as they are integrated into the product the customer will receive. End-to-end cyber security means a vendor must work with their own vendors to adopt best-practice cyber security approaches.

The requirement	Additional considerations
61. How does the vendor conduct security management with their suppliers? Has the vendor established relevant security criteria and passed them to their suppliers? How frequently does the vendor update their criteria to ensure they keep up-to-date with the latest thinking?	• Security management with vendor's suppliers is indispensible. The vendor must pass on their cyber security requirements and that of their customers to their suppliers otherwise they might be accepting components that have inherent security weaknesses. • The vendor should be able to demonstrate how it complies with industry security standards or establish security criteria and pass on relevant standards to their suppliers. The criteria established should be kept up-to-date to ensure it covers the latest thinking and security knowledge. • How does the vendor assess that that their suppliers provide sufficient resources with sufficient skill for cyber security activities? Does the vendor require their suppliers to organize special cyber security teams? • Does the vendor have special roles, organizations, or process to be responsible for passing cyber security requirements, standards, knowledge to their suppliers, and ensure there's no omission?
62. What procurement process requirements do the vendor's suppliers take with their suppliers?	• It is unlikely that every vendor's supplier can satisfy all security requirements. Security "certification" and reviews on a vendor's suppliers is necessary to make sure that they limit the risk of using security weak suppliers. • Requiring security "certification" of suppliers by vendors can also help suppliers improve their security capability to meet a vendor-imposed standard that qualifies them as a qualified supplier as part of a vendor program requiring suppliers to work with the vendor to address cyber security challenges together. • The company should be able to demonstrate a robust, security-focused process for selecting suppliers and that includes how their performance is measured, monitored and improved.
63. Does the vendor have contractual clauses or security agreements in place with their core technology suppliers that provide a comprehensive, risk-informed set of requirements that they must meet?	• A supplier to a vendor must know what is expected of them in terms of security. A security agreement is a good method to pass on security requirements and legal obligations to suppliers. Security agreements can require suppliers to enhance security management and make them contractually responsible for the security of all of the products they provide. • The company should be able to demonstrate how it is using contracts or agreements to ensure that all components used in its products, from whatever sources, are associated and compliant with security procedure and requirements.

The requirement	Additional considerations
64. What processes does the vendor have in place to assess the conformity of their suppliers to any security clauses or agreements? Does the vendor maintain scorecards or other metrics to facilitate accountability and drive performance?	• Suppliers to vendors may change and security problems may occur at any time. A vendor should be able to demonstrate how it works with its suppliers in a collaborative way to measure performance and how they work together to resolve issues. This might include scorecards, audits and inspections.
65. Does the vendor require their suppliers to notify them in the event that they find vulnerabilities in their products? What does the vendor do with this information? Do they have a vulnerability management process?	• Vulnerabilities can be found in any product or component. A responsible company should disclose vulnerabilities in its products in a consistent and timely manner. • The vendor has to be able to deal with any vulnerability information and therefore should be able to demonstrate an end-to-end process for vulnerability management regardless of who notified the vendor of the issue.
66. What approach does the vendor take if one of their suppliers does not, will not or cannot conform to their cyber security requirements?	• There are clear costs associated with compliance with cyber security requirements, but the benefits may not be as visible and direct. • If a vendor's supplier does not conform to their cyber security requirements, what measures does your vendor take to encourage the supplier to cooperate with them and address cyber security challenges together? What action is taken if they do not?
67. Does the vendor conform to international best-practice standards such as those from the Trade Partnership Against Terrorism (C-TPAT) and the Transported Asset Protection Association (TAPA)? Are they certified?	• There may be differing views around the world about what standard is best, but a vendor should be able to demonstrate compliance and certification based on widely-accepted standards. • It may be recognised that a standard may not be perfect, but vendors should be able to demonstrate where they are able to go beyond the standard to provide additional protections and measures.
68. Does the vendor conduct onsite audits on the security of their suppliers? What is the scope of those audits? The vendor should describe how they work with their suppliers to resolve problems found in an audit.	• Every vendor and every supplier needs to be focused on the needs of their customers. Audits and inspections help the supplier keep focused and they also ensure delivery of the requirements. A collaborative approach to learning the needs of each other helps drive performance in the correct direction.

4.8 Manufacturing

Product manufacturers must source components from a range of suppliers and they must ensure that no security risk has been introduced throughout every stage of the production process.

The requirement	Additional considerations
69. What international standards and best practices does the vendor comply with in terms of manufacturing?	• Manufacturing centres have many complex processes and tasks. They are widely covered by many standards from quality to environmental. A vendor should be able to demonstrate how it takes a holistic approach to a manufacturing process that adopts the best international standards and approaches.
70. The vendor should describe their manufacturing process flow and provide details on how they assess the process, both upstream and downstream, to discover the existence of any tainted and counterfeit products.	• There are many opportunities within a manufacturing process for components to be tainted or corrupted either before a part reaches a vendor's manufacturing centre or after a product has been built and is dispatched to the customer. A vendor needs to be able to detail how it handles spare parts and returns in any location in the world. A key thing to consider is storage media which might contain personal data from a customer.
71. How does the vendor ensure that the components that they buy from a supplier are the ones that they receive in their manufacturing centres and are what they expect?	• A vendor will need to consider that any high technology component that can be corrupted or tainted may have been compromised – they should work on the "no trust" model rather than "trust everything" model. How does the vendor do this?
72. How does the vendor ensure that no components are tampered with by their own staff when in their manufacturing centre?	• The insider threat issue is real. Just as a vendor needs to validate and ensure the integrity of incoming materials, they must also be able to demonstrate processes and controls that ensure that goods leaving the manufacturing centre have not been tampered with by their own staff.
73. How does the vendor tamper-proof their products when they have been built but not yet dispatched?	• Finished but not yet shipped products provide ideal opportunities for tampering. How does the vendor protect against this in its factories and warehouses?
74. How does the vendor ensure that the products customers receive are the same as those that left the vendor's manufacturing centre?	• The next thing that a vendor needs to consider is the possibility that a product that left its factory in a safe and secure condition might be tampered with before it gets to the customer. Comprehensive processes surrounding logistics should be evaluated and considered in the selection of logistics companies.
75. How does the vendor plan their demand of components so that they have the latest component as frequently as possible?	• Given that vulnerabilities can be found at any time, over-supplying can mean that you have components that contain vulnerabilities in stores – just-in-time manufacturing reduces this risk. For this to be effective, comprehensive planning of sales forecasts should be automatically linked to manufacturing.
76. If a customer's specific software is loaded onto their final equipment how does the vendor ensure that this is the same software that was authorised by R&D and has not been tampered with?	• You want your vendor to be able to demonstrate end-to-end integration and be able to show that as hardware and software completes one process in one location and joins another process in another location, there are no gaps and or opportunities for tampering.

The requirement	Additional considerations
77. How does the vendor ensure that someone in the manufacturing centre cannot load malware onto a product?	• The protection of software is very important in manufacturing. A vendor should be able to demonstrate how this process is restricted and detail whether this kind of role is classified as critical and subject to additional monitoring to avoid the insider threat risk.
78. In the vendor's manufacturing centre, how do they ensure that all the test ports are closed by default when the products leave and cannot be accessed after it leaves the manufacturing centre?	• Manufacturing facilities frequently need access to product test ports. If these are not tightly controlled and if they are left open at the conclusion of manufacturing, it might provide an opportunity for a hacker to exploit them at the time of installation. Your vendor should be able to demonstrate how all test ports are automatically closed as part of the systematic manufacturing process.
79. During the manufacturing process, how does the vendor ensure that unauthorised people do not know what customer the equipment is destined for so that they cannot tamper with specific customer equipment?	• Whilst the threat in a manufacturing centre is more likely to be to a specific product or products, all steps must be taken to avoid a situation of bribery or malicious intent, where a specific customer's equipment is targeted. A vendor should limit who knows what specific piece of equipment is destined for which customer. Techniques such as using a coding convention should be used rather than the customer name.
80. When products are returned "unused" from customers because they ordered too many or because they cancelled the contract, how does the vendor ensure that the product has not been tampered with before it is returned?	• Once again the vendor should demonstrate that they apply the "no trust" model even when a product is returned. Their procedures and processes should assume the product is tainted or corrupted and they should re-validate the product's integrity.
81. When a faulty product is to be returned, what processes does the vendor have in place to ensure that no customer data exists on disks or storage before it is sent to one of their return centres?	• Technology equipment usually contains storage components. Therefore, products returned due to any error or fault may contain customer data. Vendors have to be aware of local data protection laws. • Vendors need to be able to demonstrate how their returns and scrap processes work and what actions they take if the storage media cannot be accessed to forensically erase data.
82. When a faulty product is fixed in one of the vendor's centres, how do they ensure that all of the replaceable units are original (i.e. not been swapped with a fake item) and that the product contains no malware? Do vendors re-test their products?	• A vendor must apply the "no trust" model to its thinking and processes. Weaknesses can be introduced at many stages of a process. When things are repaired or redistributed, vendors should show how they mitigate the risk of tampered component infiltration, use of counterfeit units, malware and misconfiguration. • The re-validation of faulty products can prevent tampered, embedded or counterfeited products from entering the supply chain through the return process of faulty parts.
83. Does the vendor have a traceability capability and processes for components? Problems can arise anywhere: in a vendor's hardware or software, from a vendor's personnel, or from a third-party. In the event of an issue, how can they trace the 'who', 'what', 'why', 'when' and 'where' associated with that issue?	• An accurate and quick traceability system can help locate the source of problems quickly and determine the scope of the problem so that the vendor can notify relevant parties to take measures to prevent the spreading of the problem. • The ability to trace forwards and backwards also helps a vendor identify the root cause of the problem, identify improvements that can be made, and avoid the same issue occurring in the future.

4.9 Delivering Services Securely

There is not much point in focusing on designing your products with security in mind if, when you come to deploy them, or support them, the process is not secure. Customers rightly want to ensure when equipment is supporting their business that its operation and maintenance are safe and secure.

The requirement	Additional considerations
84. What access do the vendor's service engineers need to their customer's installed and operational equipment and services? Can they gain access to what they want, when they want?	• A vendor should be able to demonstrate that the customer is always in control of any third-party access to their technology and services. Therefore the vendor should be able to demonstrate a range of processes and policies that guide their personnel, and hold them accountable, regarding what they can and cannot do. • Customers often implement "express written permission" rules and demand auditing facilities to ensure conformance with policy.
85. In what way does the vendor protect the system default accounts or the accounts that the customer gives them to undertake support and maintenance?	• As part of a vendor's policies and procedures they should be able to demonstrate what happens to these access credentials, how they are protected and when they are handed back, and that they are subject to independent verification and audit.
86. What controls does the vendor put around the use of laptops or engineering technology their engineers carry? For example, can the vendor's engineers load their own software tools onto their laptop?	• If employees' laptops are hacked, or otherwise are infected with malware, malicious actors can steal customer information or attack customers' networks through the employees' laptops. Therefore a vendor should detail the measures they take to protect and monitor the laptops of employees.
87. What processes and controls does the vendor have in place to ensure that their engineers only use the right software for each customer?	• Often a customer's technology is complex, contains technology from many vendors and, on occasion, the integration of these components requires a specific set of software to work together effectively. A vendor should be able to demonstrate that any changes or upgrades they do to your technology are in line with the approved software for you as a customer, including the correct version and release level.
88. How does the vendor ensure that their service or support engineers cannot tamper with installed software or install vulnerable or malicious software?	• As a buyer you will want to know that your support engineer does not leave you with something you did not ask for in a malicious or accidental way because it is possible for malicious attackers to replace hardware components or load unapproved software to damage the product integrity and embed malicious or vulnerable software. • Applying the "no trust" model, vendors should be able to demonstrate how malicious attackers are prevented from tampering with products or components during the process of software deployment or upgrade.
89. The vendor should detail the approach they take to hardware hardening, software and hardware checks and security products (such as firewalls) for specific customers.	• There is significant documented best practice that guides your vendor and your own ICT team to "harden" (i.e. strengthen it from attack) the equipment you are buying. The equipment you are buying may also contain a range of security capabilities and features. • You will want to satisfy yourself that any installation, support or maintenance activities adopt and follow this best practice while also ensuring that relevant facilities are correctly turned on or off.
90. When vendors have to capture data for troubleshooting, do they get customers' official authorization and only capture the data within the authorization scope? how do they control what is captured and protect personal data?	• Troubleshooting on technology equipment may require access to data on the equipment. A set of agreed policies and procedures should be available that ensures the protection of personal user data and business data when that is required.

The requirement	Additional considerations
91. If the vendor's support engineer cannot fix the issue on-site, and captured data needs to be sent to another country for review, how is this controlled to ensure compliance with the customer's requirements and local laws?	• Sometimes, complicated faults cannot be fixed by frontline engineers on-site. It requires R&D engineers at another place to do the troubleshooting. • The vendor and you, the customer, need to agree on practices for dealing with data such as if the support required is not located in your own country. What flexibility does your vendor provide?
92. What are the vendor's processes for handling data that they captured for troubleshooting when they no longer need it?	• Data is a customer's asset and can only be used within the validity and scope of the authorisation. When the service is finished, the data must be deleted to prevent the data from being used for purposes other than the service. How does your vendor do this and ensure that it is done?
93. Audit logs form an important part of proving what has occurred on a system? How can the vendor confirm that their audit logs contain all the relevant information?	• A vendor should be able to demonstrate the approach it takes to recording and protecting accurate audit logs. • The use of audit software that is widely recognised and used in industry can make the result more objective and reliable.
94. Customers rely on their vendors especially in times of crisis: service disruption, natural disaster for business continuity. How well-equipped and willing is your vendor to support you in difficult times? Ask for real examples.	• Does the vendor have regular communication channels with their customers, to discuss together with their customers on cyber security requirements, roadmap and plans, so as to meet customers' cyber security strategies to the most extent, including in difficult times? • Risks to computer users come at all times, even in times of disaster, as threat actors will seize every opportunity. Often your vendor will have a wealth of international knowledge, tools and resources that may help their customers. For example, frequent denial of service attacks might require rapid equipment expansion, new or different technology, and you will want your vendor to show willingness to help, and demonstrate flexibility. • Natural disasters do occur and your vendors may play an important part in your business continuity. Exploring their commitment to help you in these difficult times may enable you to assess their long-term commitment to the success of your business.

4.10 Issue, Defect and Vulnerability Resolution

It goes without saying that there is no such thing as a 100% guarantee when it comes to security. Therefore, a company's ability to respond effectively to issues and learn lessons from what has gone wrong is critical to both the customer and the vendor.

The requirement	Additional considerations
95. Does the vendor have a PSIRT/ Vendor CSIRT (Product Security Incident Response Team/Vendor Computer Security Incident Response Team), or equivalent? The vendor should detail their operations and how they can be contacted. What are the processes and requirements that the PSIRT/Vendor CSIRT team is required to follow?	• Problems will occur and you will want to know that when this occurs the vendor can be notified quickly of any actual or perceived security issues. You will also want to satisfy yourself that you have mechanisms in place to track the security incident until it has been resolved. • It will be important to have an approved set of processes that the PSIRT/Vendor CSIRT team follows in performing its responsibilities.

The requirement	Additional considerations
96. What mechanisms does the vendor put in place to deal with a customer CSIRT or coordinators so that they can notify your company of issues and work together to expeditiously address them?	• Your company might want a range of contact mechanisms from one internal central point (a PSIRT/Vendor CSIRT) to multiple locations. Your vendor should demonstrate capability and flexibility in adopting a range of models.
97. Does the vendor have an approach to working with the security researcher community?	• An organisation that does not listen does not learn. Vendors need to work with a wide variety of companies and individuals who may be finding issues with their products. How does your vendor do this in a productive and professional way?
98. In the event of a major incident, how is the vendor equipped to ensure that their customers can and will be informed in a timely manner and that the right resources are made available within their company to respond to the incident? The vendor should be able to clearly describe escalation processes.	• If a significant security incident occurs within your organisation you will want to satisfy yourself that your vendor has the mechanism to quickly notify you, but also that they have internal processes for handling incidents including escalation within their organisation. • Given the reality that most businesses do not have skilled resources sitting around doing nothing, how can the vendor demonstrate that their senior executives are made aware of the situation as a matter of course, and can and will allocate the necessary support to resolve the issue?

4.11 Audit

Talk is cheap, words are easy, pictures are nice – but do you do what you said you would do, in the way that you agreed it should be done, to the timescale, cost, quality and security requirements you have agreed to? How would you know? Rigorous audits play a key role in assuring your customers and stakeholders that the appropriate policies, procedures and standards are being executed to deliver the required business outcomes.

The requirement	Additional considerations
99. What processes and mechanisms does the vendor have for internal security auditing and reporting to ensure that the relevant Board of Directors committee has visibility into the organisation's actual risk posture and incident status and consequences, rather than what may be reported to them?	• If there is formal internal, external, customer and third-party auditing of cyber security activities, it shows that the Board is open to real feedback. • Being able to demonstrate this shows that the strategies, polices and standards are "living" and adapting to new threats and situations. • When formal reporting is given to the Board / Committee on cyber security activities, progress, and performance, it shows that this is part of normal business activities rather than a "project" or some "special" event.
100. Does the vendor have the mechanism to allow external stakeholders or their delegated organisations to conduct the audit?	• Demonstrating openness and transparency to key stakeholders and accepting external audits and reviews shows a commitment and a continuous learning culture. • The more you are open to external party review, the more improvement suggestions you will get.

5 About Huawei

Huawei's products and solutions cover over 170 countries and regions, serve more than one-third of the world's population. We employ 150,000 people and the average age of our employees is 32. On average, 79% of our people are locally-employed in countries in which we operate. By the end of 2013, we have acquired 281 LTE commercial contracts and 162 EPC commercial contacts, in which 110 LTE network and 88 EPC network have been released commercially.

Huawei has a leading role in the industry through continuous innovation and has one of the most significant IPR portfolios in the telecommunications industry. Huawei respects and protects the IPR of others. Huawei invests more than 10% of its sales income into R&D and 45% of our employees are engaged in R&D. In 2013, Huawei invested RMB 30.734 billion in R&D, accounting for 12.9% of the total annual income. The total investment in R&D in the last decade is over RMB151.9 billion.

By 31st December, 2013, Huawei had filed 44,168 patent applications in China, and 18,791 patent applications overseas, 14,555 under the Patent Cooperation Treaty (PCT). We have been awarded 36,511 patent licenses by accumulation. Compared to the quantity, Huawei attaches more importance to the commercial value and quality of IPR. From 2010 until now, our 466 core proposals on 3GPP LTE were granted, ranking No. 1 in industry. Huawei holds a leading position in terms of patents in FTTP (Fibre To The Premises), OTN (Optical Transport Network), G.711.1 (fixed broadband audio) etc. The protection of IPR is therefore critical to the ongoing success of Huawei, and because of this, Huawei is a champion of IPR protection.

We have 16 research institutions around the world, 28 joint innovation centres, and 45 training centres. Overall, 65% of our revenue is generated outside of Mainland China, and we source 70% of our materials from non-Chinese companies. The United States is the largest provider of components at 32% -- some USD7.237 billion of Huawei's purchases were from American companies in 2013.

We provide managed services for more than 120 operators in over 75 countries to help customers achieve operational excellence and we have acquired an accumulated total of over 340 managed services contracts. Huawei has built cloud-based IT solutions and collaborated with over 400 partners to accelerate the commercial application of cloud computing technologies across various industries. By the end of 2013, we had set up 330 data centres for customers around the world, including 70 cloud data centres.

In 2013, Huawei's consumer business shipped 128 million device products all over the world, including nearly 60 million mobile phones,44.5 million mobile broadband devices, 24.4 home devices. The shipment of smart phones reached 52 million for consumer business, an increase of more than 60% of that in 2012.

Huawei is passionate about supporting mainstream international standards and actively contributes to the formulation of such standards. By the end of 2013, Huawei had joined over 170 industry standards organizations and open source organizations, such as the 3GPP, IETF, ITU (International Telecommunication Union), OMA, ETSI (European Telecommunications Standards Institute), TMF (Tele Management Forum), ATIS, and the Open Group, among others. In 2013, Huawei submitted more than 5,000 proposals to these standards bodies and we hold 185 positions in organisations supporting the drive for consensus and agreement on international standards.

By December 31, 2013, 84,187 employees had purchased an equity stake in the company. The Employee Stock Ownership Plan closely links Huawei's long-term corporate development with our employees' personal contribution and forms a long-standing mechanism for dedication and reward-sharing. This gives us the ability to take a long-term view; it also ensures we balance risk with reward and strategy. Employees know if we do not excel at serving our customers, or if we undertake inappropriate activities, their equity and pensions may be destroyed.