Global Information Assurance Certification Paper

Copyright SANS Institute
Author Retains Full Rights

This paper is taken from the GIAC directory of certified professionals. Reposting is not permited without express written permission.

Interested in learning more?

Check out the list of upcoming events offering
"Security Essentials Bootcamp Style (Security 401)"
at http://www.giac.org/registration/gsec

CONTROLLING VENDOR ACCESS FOR SMALL BUSINESS

GIAC GSEC Gold Certification

Author: Chris Cain, cicain08@gmail.com
Advisor: Dr. Hamed Khiabani

Accepted: September 5th, 2013

Abstract

A security policy is an important piece to securing an organization, but without including vendors, it may just be a document on the shelf. Securing any infrastructure can be difficult especially for small businesses that rely on outsourced consultants for services. Many times controlling how much access vendors have and how they provide service can be problematic due to contracts, access needed and lack of IT knowledge from management. Following a systematic approach and developing the proper methods and checks, small businesses can be just as successful implementing a policy that is used specifically by outside consulting staff. The information gathered within this document will include a vendor questionnaire, a policy template and considerations for implementing such a policy for stakeholders who may lack the appropriate technical knowledge. Using the techniques in this document, small organizations will be able to move towards a more secure environment that reduces their risk, maintains relationships while also protecting their data.

© 2013 The SANS Institute Author retains full rights.

1. Introduction

A vendor access policy is a great way to supplement any security policy. Many smaller organizations and large organizations depend on external vendors for supporting their systems. In large organizations, hundreds or even thousands of vendor technicians may require remote access to the network to help maintain business function. Setting up a security policy usually requires having an inventory of devices that need to be secured, entry points into the network and access rights for individuals. External vendors many times have just as many if not more rights on the network then internal staff; this is especially true in smaller organizations. Smaller organizations may not have any policies in place due to lack of resources and staffing to complete such tasks. They may also believe they may not need one since they have so very few employees. As many smaller organizations begin to depend more on their network and data to be accessible though, the case for developing policies is more important due to the risks that are associated with doing business online and with external parties. This can be especially true when using cloud providers as well.

Giving vendors access and making sure they can perform their duties in a timely manner is important. Having vendors comply with an organization's policies though can be tricky due to lack of monitoring, auditing, control of permissions and contracts. Many times vendors request or require non-delegated access to resources to complete tasks, which requires no onsite user interaction. This can be concerning if the vendor is not being audited and the organization would like to protect their data. A company vendor policy could also affect a vendor's Service Level Agreement (SLA) due to stringent requirements for access, which the vendor may not comply with due to these requirements. Balancing the organizations requirements with vendors need for access to the network quickly is ideal.

The templates for policy and the questionnaire provided in this document should assist any small organization that would like to secure its data and network if vendors are used heavily or exclusively.

Chris Cain, cicain08@gmail.com

© 2013 The SANS Institute, Author retains full rights.

© 2013 The SANS Institute Author retains full rights.

2. Managing Vendor Relationships

Maintaining good relationships with vendors is good for a business as vendors help the business maintain smooth operations and may improve their chance to succeed. Much like hiring the right employees for an organization, having the right vendors helps to ensure the organization is providing quality products and services. Communication is important with vendors and just like regular staff updating vendors on changes in the organization and how well they are performing is a great way to maintain a positive relationship. Getting their input on business decisions is also a good way to maintain relationships with vendors and make them feel more closely attached to the organization.

Assessing a vendor quarterly or annually should be part of this and should use various assessment types, including a library of questions based on best practice standards similar to what regular employee receives. Using standard review forms or questionnaires is a great way to simplify the process for management that may not understand the proper questions to ask or look for. When utilizing vendors the process tends to follow a life of selection, annual assessment and termination, similar to an Employee Life Cycle (Levine, Mitchell).

Many support vendors will follow security practices due to its importance and prevalence in network systems. Software developers although do not see security as clear cut as many of their positions require a working product and security could get in the way of that. Getting a software developer to follow a policy for support can be difficult without proper engagement from both sides.

2.1 Vendor Risk Management

The point of doing any vendor policy is to reduce an organizations risk level and many times vendors are forgotten in this process. Using vendors for support can bring associated risk if there is no auditing or review occurring. According to the Trustwave 2012 Global Security Report, “In 76% of incident response investigations conducted, a third party responsible for system support, development, and/or maintenance of business environments introduced the security deficiencies.” (Trustwave, 2012). Many times the associated risk vendors bring could be avoided by having a vendor policy in place that is

Chris Cain, cicain08@gmail.com

© 2013 The SANS Institute Author retains full rights.

communicated, followed and understood by the vendor. Balancing the level of risk the organization is willing to take compared to the level of access the vendor has can be difficult, but there are ways to quantify it and ease the process.

Many large organizations have processes in place already to handle vendor risks and have appropriate procedures to deal with incoming vendors that provide support. Government use of vendors is well known and many times they are used exclusively to provide support or to provide services for many different agencies. Vendor risk is very apparent with Government agencies and can be seen in recent events with privacy and loss of data from vendor staff. Even with appropriate procedures in place, such as Security Technical Information Guides (STIGs), security incidents still occur and can affect the Governments reputation. A good example is with the NSA and the confidential information that was released to the public. These are a few good reasons why managing vendors is so important.

Vendors will typically use their own software or devices to access a network remotely including SSH tunnels, VPN technologies or out of band devices, which may include their own vulnerabilities and risks if not patched appropriately. When vendors access systems remotely it is done in the background and typically unknown to the organization, partly to prevent interrupting the company's business during business hours.

Another risk to consider is vendor staff. If a vendor is lacking appropriate staff to handle an organization's requests or if only one vendor staff is able to understand the organization's network and they were to leave abruptly this could affect the business operations of the company as well and leave the vendor without the ability to support the organization without the proper documentation in place.

If vendors have full access to an organizations data then this could cause a conflict of interest in which they could potentially modify the organization's data to their own benefit without the organization knowing or implementing issues that are contained and used as a reason to use that vendor. Many things need to be considered when using vendors for support. For smaller organizations that would like to fall into better compliance and security can use low cost answers to some of these issues.

Chris Cain, cicain08@gmail.com

© 2013 The SANS Institute Author retains full rights.

Other risks include the financial status of the organization providing support. If the company were to go out of business the support agreement could be affected and the organization may not know about the vendor financial problems until it is too late. This could cause a lapse in support that could affect the organization significantly. Receiving status updates reports on support items covered as well as financial status of the company could be an included item in any policy that is created.

2.1.1 Cloud Based Providers

Many organizations are moving toward cloud-based vendors to provide services. The SaaS or --aS model overall seems to be the trend in many industries and prices are continuing to fall for even small organizations. Moving servers, software, data, and even desktops offsite seems to be a viable solution for many organizations to avoid the management that goes along with having devices inside the organization as well as the cost that goes into supporting them. Securing these resources though can be difficult as the resources are maintained offsite with the vendor who manages those resources. Using a risk benefit analysis is one way to balance the need for a cloud based provider. When using these providers it is even more important to review initial contracts and review reports that are created every month or quarterly. When using cloud based providers it may be difficult or impossible to have them follow an organization's security policy if it is a smaller organization or if the provider has its own policies and procedures it implements. This is typically a good thing as it covers the bases of a small organization that may not want to create policies of its own. Using a standardized document for the vendor to fill out is another way to understand the risks involved with signing up with a cloud provider. The Shared Assessment Program (SAP) offers resources and documents to use when initially vetting cloud providers and the risks they may bring onto an organization. The worksheets they provide are great tools to utilize.

Standardized Information Gathering (SIG) was a tool created by the Shared Assessments Program. This program was created by leading financial institutions to provide standardization, consistency, speed, efficiency, and cost savings into a vendor risk assessment process.

© 2013 The SANS Institute Author retains full rights.

Social Engineering can be a valid concern as well when using vendors. Having policies in place so that vendors are not able to gain access to users passwords is important. Many times vendors may use various staff to help support an organization and without proper procedures and checks in place a person could identify themselves as the vendor and gain access to the systems. A good example of this is Internet Service Providers (ISP's) that may have to gain entry into the organization to setup new services. Verifying the person's identification can be missed if the person identifies themselves as part of the vendor staff or provider.

2.1.2 Data Loss Prevention

This issue is becoming more prevalent in today's environment. Data loss prevention (DLP) should be a concern for organizations wanting to protect their data. Using vendors is just an extra level to consider as many times vendors don't have as much loyalty to the organization as do regular employees. Especially with larger enterprise organizations and government agencies as confidential information can be moved and hidden so readily and whistleblowing is more common. More of these cases are being reported in the news with vendors leaking critical and confidential information, which can affect the organization or government's reputation as well.

Securing organizations data can be accomplished through a layered approach. Separating administrative accounts is part of this solution and would include creating accounts for vendors to use for administrative purposes and would allow tracking of these accounts. Reducing rights of these accounts would be an additional step to control these accounts from needing to access the data the organization deems as important or confidential. Encrypting this data is another step that would make sure that if the data was taken offsite it could not be decrypted and used. Adding this as requirement in the policy would be important. Maintaining maintenance periods and physical access to the information and building could be another layer that would only allow access to vendors during specified times, but this may be difficult to control if there was an emergency.

Chris Cain, cicain08@gmail.com

© 2013 The SANS Institute Author retains full rights.

3. Vendor Policy

Determining which vendors that should be covered in the policy can be difficult. If a vendor has contact with company resources including physical access to data, server rooms and PC's then they should be included in a vendor policy.

Defining vendors in the policy is important to avoid any confusion with vendors that may not necessarily require similar restrictions, such as janitors, food vendors, construction crews or landscapers. Example vendors that would need to follow and review a vendor policy could include ISP support, software vendors, A/V support, network support and help desk support to name a few.

The ISO 27001 series for securing an organization using an Information Security Management System (ISMS) is an ideal way to properly implement a security policy (Calder, Alan). Many times large vendors that support the organization will have their own security policies in place that will follow these standards.

If security systems are in place that may pick up rogue devices it may be ideal that vendors document the devices being used or notify the organization beforehand that they will be using their own personal devices to provide support so that any alerts or false positives found by the security devices are properly handled rather than reported as an intrusion. This could typically occur when an organization has both internal and external support working together.

Controlling vendors' devices can be difficult to manage as many use their own personal devices and laptops to perform work onsite or offsite via a VPN or SSH type connection. Many vendors will bring their own personal access points for internet access when onsite. This can bring potential security issues and issues with data loss prevention or DLP. Having a policy state that vendors devices are not permitted is not an ideal solution either as vendors typically need their devices to support the organization. If a vendor's device were to be compromised then that responsibility may lie on the vendor and should be stated in the policy. Implementing technologies may be a way to mitigate this risk as well, including mobile device management (MDM) and/or segmenting the network, though this may not be suitable in smaller organizations where cost is a concern and vendors will be the ones supporting the segmented network.

Chris Cain, cicain08@gmail.com

© 2013 The SANS Institute Author retains full rights.

This should be a standard for all internal staff as well as vendor support. Many of the devices controlled by vendors are border or internet facing, making it much more important these devices are secured with secure passwords. This includes applications that may have backdoors or administrative accounts that should need to be locked down.

If vendors make changes and no documentation exists on those changes it may be difficult for a different vendor to support those products as it could take more time to troubleshoot. In most organizations developing a change control process is important due to the quantity of individuals supporting those systems. With vendors this is especially true as many do work at off hours when no staff is on site. This can be troublesome for a small organization if the next day they find problems with their systems. Change control is an important way to also track things the vendors have been doing and if they are following policy. Being able to confirm tasks were completed and how long those tasks took is a great way to accompany any monthly or quarterly reports the vendors send on the work they completed and time taken.

Separating duties between services and applications should be a requirement for internal IT staff and this should especially include vendors as root and administrator privileges give too much control over an organization's resources. This can be difficult when proprietary software that is being supported by the vendor was also developed by the vendor and is used exclusively or non-exclusively by the organization (Levine, 2006). Separation of duties requires that user accounts be defined for each separate vendor that is accessing the company's resources. Mark Cooper goes into more detail in his document "Controlling Remote Access for Vendors" on how to properly setup user accounts for vendors that are accessing an organizations resources (Cooper, 2003). Separating accounts is also important to restrict data loss prevention that can commonly occur when administrative accounts of access to confidential data.

When intrusions occur that could potentially harm the business vendors need to report these incidents in a timely manner so that management is aware. Including this in a policy is a way for an organization to make sure they are aware of issues in the current environment and threats that could affect the business productivity and operation. Many times these events are not reported and they could cause problems with any new vendors that are to support the network and find outstanding issues that were not reported

© 2013 The SANS Institute Author retains full rights.

initially. These types of items could be communicated in a report on a monthly or quarterly basis so that management is aware.

Reports are a great way for vendors to put together any issues they ran into during the month or quarter and also anything they see upcoming in need of repair or added that would need to be added to any budget. Many vendors provide continuing reports of the environment and report on issues they have been working on. These are great form of communication so that management and the organization can verify if the vendor is meeting the contractual needs.

Developing maintenance periods is another way to ensure that staff are aware when events occur that are not normal during business periods. This also alerts internal IT staff to when vendors are logged into equipment. If monitoring is installed and finds logins active during non-maintenance periods then this could be a sign of a breach. Having vendor support scheduled and written ensures also that staff are aware when to expect to see vendors on site.

3.1 Handling Vendor Contracts

"The scope and methodology for conducting third-party vendor risk assessments should be proportional to the types and sensitivity of data exchanged and the capacity of the organization to conduct a comprehensive evaluation of the privacy and security infrastructure of the third-party vendor" (Katz, 2012). This long statement says a lot about what an organization needs to consider when selecting a vendor. Part of what this statement says is that if a vendor does not follow proper security practices within its own organization then it will not follow them when supporting your organization. Understanding that security practices are best implemented if practiced is key to knowing whether a vendor will subject your organization to security risks that should be controlled in the beginning. When best security practices are followed in the vendor's organization then this increases the likelihood they will be practiced at the organization in an emergency situation.

Using a specialized system or template when first evaluating vendors is a great way for small organizations to make better decisions that may affect its overall risk. Many times when going through negotiation process it is easy to refrain from asking or to

© 2013 The SANS Institute Author retains full rights.

simply forget key questions that could affect the contract. The template provided in this document can be used to assist in meetings with IT or software vendors for support and includes a questionnaire that can be filled out either by the vendor or organization during the evaluation process.

There are some things to plan and look for when deciding on a vendor to support the organization. For many small businesses these negotiations are difficult as they may be inexperienced with them or lack enough knowledge to make an informed decision. Going into negotiations confident with the appropriate information and questions; small businesses can be effective in creating a contract that reduces their risk in vendor relations.

The first thing any organization should do is to try and avoid any startup vendors that are seeking to provide support. Also, it is important to avoid any long term contracts such as three years that may be a default for many organizations. For starters signing up for a year contract may be the best, or month to month to start is always a good idea if the vendor is not well known. These contract terms can and should be negotiable for most companies. Being unable to verify past experience is difficult for any organization to decide and measure the appropriate risk since there is no history to confirm the vendors' claims, especially if the vendor is handling an important aspect of the organization's systems.

It is worthwhile and mandatory in many fields to meet with at least three different vendors to provide a comparison to find the vendor that best fits the organization. After initial meetings with vendors it is important that the organization verify the vendors' staff knowledge by either verifying certification status and/or checking with references that they provide.

During negotiation stages there are a few things to receive confirmation on from the vendor. One of those items is that the organization receives assurance from the vendor that would indemnify the organization from lawsuits that may be brought by any third party suppliers claiming copyright and/or patent infringements. This should be included as part of the vendor policy as copyright infringements and software privacy are serious issues that can create unnecessary risk for a small organization. During the negotiation of the contract terms it's important that if the contract is an annual contract to

© 2013 The SANS Institute Author retains full rights.

make sure there are no automatic renewals that may be part of the contract. This can catch an organization by surprise if they are planning an exit strategy and find the contract automatically renewing before they have ended the contract. This occurs quite often with Internet Service Providers. Including a dispute resolution clause in the contract is also a good idea so that if there were a dispute then appropriate action would be taken to lessen the impact. If the vendor is a software or development company including assurances in case their business fails is important to build a strong contract. This could include finding out the availability of the source code if the software developer were to be sold or go out of business. This is even more important for small developers that provide software that is crucial to the organization. (Stratis Health)

3.1.1 Vendor Questionnaire

Using a standard questionnaire allows a small organization to evaluate vendors that are going through initial proposals and allows an organization to easily make better decisions in a quantitative manner. Using these types of forms allows vendors an almost a fool proof method to evaluate vendors security posture. Many online sources have forms readily available for download or even creating one for the organization can assist in the evaluation process as well. The following is a typical questionnaire that can be used to evaluate a vendor and to evaluate their position on security as well. This is meant for small organizations that may not have access to such information. This questionnaire will avoid any cost or contractual related questions as those should be negotiated with the vendor. This type of questionnaire may not be suitable for vendors to answer during the negotiation stage due to its length, but could be something they fill out as part of the negotiation process or filled out by the organization if the answers are known. The answers given may be technical in nature, but can be translated if needed by either the vendor, outside technical advisors or internal staff that may carry more technical knowledge. Many times vendors will have the organization complete its own questionnaire to understand the environment they will be supporting.

Chris Cain, cicain08@gmail.com

© 2013 The SANS Institute Author retains full rights.

3.2 Vendor Support List

When it comes to determining what a vendor needs access to, many questions may need to be answered. If a vendor is supporting an application do they really need access to the company's Email system or, for example if they are supporting a database do they need credentials to access the phone system. Access control becomes more important when organizations grow. As organizations grow so does their systems and with this their credentials and the influence these credentials carry grows even more important. Not separating these credentials vendors may begin to gain access to systems they don't need access to. This type of growth can cause authorization creep to occur. The key to this is using a policy to guide vendors and internal staff to create accounts for vendors to use that has the appropriate privileges for them to provide support.

Including in the policy the handling of new vendor support staff or contracted vendors is important for an organization. When vendors change their support staff that work with the organization management should be notified in a timely manner. This ensures that any miscommunication or issues occurs the organization has updated contacts. There should be also some consideration for subcontractors. Many vendors may subcontract support staff without the organization knowing, which could cause a conflict of interest and possibly increase risk for the organization. At times vendors may not have a choice, but to subcontract certain types of specialized tasks. These subcontractors need to follow the same policy as the vendor and should be known to the organization.

Communicating the policy to vendors is one of the most important steps in making sure the policy is complied with. If vendors understand the company's expectations and concerns they will be much more inclined to accept them if they know there are audits and procedures in place. This could involve initial meetings or conference calls to go over why the policy is needed and that security is a concern. Awareness is a great first step to this. Initial meetings with vendors and listening to their view of how they would secure the organization are a great way to get their input on the process and implementing any policy.

How would these policies be audited if all IT support is contracted? Using multiple vendors could be beneficial in regards to auditing and could provide a checks

© 2013 The SANS Institute Author retains full rights.

and balance type system. Though, this may be too costly for most small organizations. Using the vendor to audit themselves may be another way with proper documentation to implement such a system. Outsourcing a separate company to perform audits is a way to make sure the current vendors are following guidelines developed in the policy as well but may come at a cost too. Tools can also be used to monitor systems and email reports to management.

4. Conclusion

A vendor access policy is a great supplement to a security policy and should be developed if vendors are used exclusively. Using a standard procedural approach described in this document, smaller organizations that may lack the appropriate knowledge to develop such a policy can now create proper guidelines for vendors to follow as well as reduce their risk and ensure their data is protected.

Using questionnaires during initial contract negotiations is a way for an organization that may lack the knowledge to hire an appropriate vendor to support the organization and find the best company. These questionnaires can also assist in determine if a vendor may be more likely to follow a security policy that is planned to be put into place as well.

Controlling cloud based providers is especially difficult as many are large vendors that control the resources, so this may be difficult for smaller organization to audit this environment. Many cloud based providers have security policies in place so this risk could be much more mitigated compared to smaller vendors that provide on-site support.

Maintaining vendor relationships is ideal to receive appropriate feedback and input into the organization's future and plans. Using reports and getting feedback on concerns and ideas from vendors is a way to maintain relationships. If the vendor is performing well

Data loss prevention or DLP is becoming more of a concern in today's age and controlling what a vendor has access to and can take offsite are crucial. Vendors may have no loyalty to an organization if there is no relationship and this could cause a loss of data if that data can be used by external sources.

Chris Cain, cicain08@gmail.com

© 2013 SANS Institute, Author retains full rights.

© 2013 The SANS Institute Author retains full rights.

Making sure communication is ongoing either through the use of monthly or quarterly reports and meetings is important to make sure a vendor is on top of any outstanding issues as well as indicate performance and security risks. It can also give the organization clues into how the infrastructure is fundamentally and if any new equipment is needed in the future for budgetary purposes. Getting their input on ways to improve the organizations function is a great way to utilize vendors as well. Using vendor reports are also a great way for management to audit the tasks that are being completed by vendors as well as determine future needs for budgeting purposes and growth planning.

The following appendix includes a generic vendor access policy template as well as sample questionnaires that can be used by small organizations that may not have access to such resources. Some entries may only be suitable for some organizations and can be adjusted accordingly.

Chris Cain, cicain08@gmail.com

© 2013 SANS Institute, Author retains full rights.

© 2013 The SANS Institute Author retains full rights.

5. Appendix

Vendor Access Policy

1.0 Purpose

The purpose of this policy is to define standards for vendors accessing resources on <Company Name>'s network. These standards are designed to minimize the potential exposure to <Company Name> from damages which may result from unauthorized use of <Company Name> resources. Damages include the loss of sensitive or company confidential data, intellectual property, damage to public image, damage to critical <Company Name> internal systems, etc.

2.0 Scope

This policy applies to all <Company Name> vendors, contractors, subcontractors, visitors or agents with a <Company Name>-owned or personally-owned device used to connect to the <Company Name> network. This policy applies to any connections used to perform work on behalf of <Company Name>.

3.0 Policy

3.1 General

1. It is the responsibility of <Company Name> vendors, contractors, and agents with access to <Company Name> resources that due care is ensured to properly secure <Company Name> resources.
2. It is the responsibility of <Company Name> vendors, contractors, and agents with access to <Company Name> resources that due care is ensured when using vendor devices on <Company Name> networks.

3.2 Requirements

1. <Company Name> vendors' devices used to administer <Company Name> resources are properly secured with strong passwords (determined by password policy), antivirus (if applicable), and are secured physically. This includes <Company Name> network devices, which may include firewalls, out of band (OOB) devices, routers, switches and wireless access points.
2. At no time should any <Company Name> vendor provide, release, share, or distribute data or information deemed confidential to <Company Name>.
3. Any vendor software installed on <Company Name> network is documented and communicated to <Company Name> management. This includes remote access software, backdoors and anything used for administering <Company Name> resources. Software installed should be legally obtained and have proper licensing attached when installed on <Company Name> system's.
4. At no time should any <Company Name> vendor provide their login password to anyone, including coworkers, vendor staff or <Company Name> staff. Passwords used by vendors to access or create on <Company Name> devices and systems should follow

© 2013 The SANS Institute Author retains full rights.

standard secure practices defined by <Company Name> Security Policy. This includes passwords and procedural documents for <Company Name> that are kept at vendor facilities for access.

5. Any changes made on <Company Name> network or applications are documented following appropriate guidelines agreed upon by <Company Name> and vendor.

6. If an intrusion or incident occurs on <Company Name> that was illegitimate or was to cause harm, management should be contacted in a manner agreed upon by <Company Name> and Vendor.

7. Any accounts used to administer <Company Name> resources should be created for vendor use and be separate from the default administrator accounts.

8. Maintenance performed on <Company Name> network should be communicated and documented during an agreed upon time between <Company Name> and Vendor.

9. Any subcontractor's used by vendors to complete tasks for <Company Name> will be communicated to <Company Name> before the subcontractor is used.

10. Reports of findings are given to <Company Name> via a document or in person on an ongoing basis with reporting timeframe determined by Management and Vendor on a monthly or quarterly basis.

4.0 Enforcement

Any violation of this policy by a vendor may be subject to action including termination of contract and/or court action.

5.0 Definitions

Term	Definition
Vendor	Any external contact provider that supports <Company Name> resources and requires access to the internal infrastructure to provide support.
Device	Any items used to provide access to resources on <Company Name> network and may include routers, switches, firewalls, out of band devices, and wireless access points.
Out of Band	A network device used for remote access to systems using analog lines and modems rather than traditional Ethernet switch technology.
Subcontractor	Any staff hired by vendors that are not directly employed by vendor, but are used to provide services for the organization.

6.0 Revision History

Chris Cain, cicain08@gmail.com

© 2013 SANS Institute, Author retains full rights.

© 2013 The SANS Institute Author retains full rights.

Support Vendor Questionnaire
for current and initial vendor agreements

This questionnaire is used to align the organizations expectations with those of the vendor.

The following questionnaire may require follow-up discussion.

General Information	
Vendor name	
Vendor location (Address, City, State, Zip)	
Vendor contact (Name, Phone, Email, Fax)	
Date	
Is vendor a Cloud Based Provider?	☐ Yes ☐ No ☐ Maybe
Is vendor able to provide references?	
Does vendor provide monitoring services? If so, explain further.	
Does vendor provide support currently?	☐ Yes ☐ No
How many employees does vendor have employed?	
How long has vendor been in business?	
Does the vendor follow a security policy currently within their own environment?	☐ Yes ☐ No ☐ Maybe

Chris Cain, cicain08@gmail.com

© 2013 The SANS Institute, Author retains full rights.

© 2013 The SANS Institute Author retains full rights.

What password policy does vendor use when setting passwords on devices? (I.e. complexity rules, length, renewal period, etc.)	
What process do you follow when reporting incidents, including security incidents, hardware failures, or network events that could lead to operational events?	
How many staff members will be supporting or currently do support the organization?	
What items will be support and managed?	☐ PC's ☐ Servers ☐ Network Devices ☐ Software ☐ Other
Are there any technical items that are and will not be supported?	
What products do you focus your experience on most? (I.e. Microsoft, Cisco, Citrix, VMware, etc.)	
What are the supported response times? (Please include during normal business hours, emergencies during normal business hours, and after hours emergencies)	
Will vendor software need to be installed to	☐ Yes

Chris Cain, cicain08@gmail.com

© 2013 The SANS Institute Author retains full rights.

support the systems?	☐ No ☐ Maybe
If vendor software will be used does it require licensing?	☐ Yes ☐ No ☐ Maybe
What is your policy on performing updates, do you have maintenance periods or specific days and times that you perform updates?	
Do you provide monthly or annual reports on tickets, issues, or findings that would be useful for the organization? If so, how often are these reports created and what is included in them?	
Are you able to provide hardware replacement? If so, do you carry any inventory onsite?	
What experience does vendor have in supporting environments that follow compliance regulations such as HIPAA or PCI to name a few?	
What is your policy and where do you store passwords and procedural documents for clients? Are these documents encrypted?	
What backup methods do you recommend or support, including strategy? (I.e. differential, incremental, etc.)	

Chris Cain, cicain08@gmail.com

© 2013 The SANS Institute Author retains full rights.

6. References

- Calder, A. (2009). *A Management Guide, Implementing Information Security Based on ISO27001/ISO27002*.
- Levine, M. (2006). *Controlling Vendor Access*. Retrieved from http://www.auditserve.com/ControllingVendorAccess/tabid/203/Default.aspx
- Cooper, M. (2003). *Controlling Remote Access for Vendor Support"* . Retrieved from http://www.giac.org/paper/gsec/2948/controlling-remote-access-vendor-support/104954
- Kuhn, R. D., Hu, V. C., & Ferraiolo, D. F. (2006). *Assessment of Access Control Systems*. Retrieved from http://csrc.nist.gov/publications/nistir/7316/NISTIR-7316.pdf
- Shackelford, D. (2011). *Compliance and Security Challenges with Remote Administration*. Retrieved from http://www.sans.org/reading_room/analysts_program/netop-02-2011.pdf
- Katz, D. (n.d.). *Contracting in a World of Data Breaches and Insecurity: Managing Third World Vendor Engagements*. Retrieved from http://lexisnexis.com/in-house-advisory/fullArticle.aspx?Bid=62741
- Trustwave, "Global Security Report" (2012) Retrieved from https://www.trustwave.com/downloads/Trustwave_WP_Global_Security_Report_2012.pdf
- Standardized information gathering. (2012, 2 2). Retrieved from http://sharedassessments.org/media/SIGv7_overview_2_1_2012.xls
- *Vendor Questionnaire*. (2012, 5 10). Retrieved from http://www.franciscanalliance.org/Documents/Vendor_Questionnaire.pdf
- Aging Services of Minnesota, (2009), "Contract Checklist" Alliance Purchasing produced by Stratis Health

Chris Cain, cicain08@gmail.com

© 2013 The SANS Institute Author retains full rights.

Last Updated: November 22nd, 2014

Upcoming Training

Click Here to {Get CERTIFIED!}

Community SANS Denver	Denver, CO	Dec 01, 2014 - Dec 06, 2014	Community SANS
Community SANS Charlotte	Charlotte, NC	Dec 08, 2014 - Dec 13, 2014	Community SANS
SANS Cyber Defense Initiative 2014	Washington, DC	Dec 10, 2014 - Dec 19, 2014	Live Event
SANS CDI 2014 - SEC401: Security Essentials Bootcamp Style	Washington, DC	Dec 12, 2014 - Dec 17, 2014	vLive
Mentor Session - SEC 401	Montreal, QC	Jan 15, 2015 - Mar 19, 2015	Mentor
SANS Security East 2015	New Orleans, LA	Jan 16, 2015 - Jan 21, 2015	Live Event
Community SANS Los Angeles	Los Angeles, CA	Jan 19, 2015 - Jan 24, 2015	Community SANS
Mentor Session - SEC 401	Minneapolis, MN	Jan 21, 2015 - Mar 04, 2015	Mentor
Community SANS Memphis	Memphis, TN	Jan 26, 2015 - Jan 31, 2015	Community SANS
Community SANS Oklahoma City	Oklahoma City, OK	Jan 26, 2015 - Jan 31, 2015	Community SANS
Mentor Session - SEC 401	Toronto, ON	Jan 29, 2015 - Apr 02, 2015	Mentor
Community SANS Seattle	Seattle, WA	Feb 02, 2015 - Feb 07, 2015	Community SANS
Cyber Threat Intelligence Summit & Training	Washington, DC	Feb 02, 2015 - Feb 09, 2015	Live Event
Mentor Session - SEC401	Medina, OH	Feb 02, 2015 - Apr 06, 2015	Mentor
Community SANS Las Vegas	Las Vegas, NV	Feb 02, 2015 - Feb 07, 2015	Community SANS
SANS vLive - SEC401: Security Essentials Bootcamp Style	SEC401 - 201502,	Feb 02, 2015 - Mar 11, 2015	vLive
Mentor Session - SEC 401	Williamsburg, VA	Feb 04, 2015 - Apr 08, 2015	Mentor
Community SANS Boston	Boston, MA	Feb 16, 2015 - Feb 21, 2015	Community SANS
SANS Scottsdale 2015	Scottsdale, AZ	Feb 16, 2015 - Feb 21, 2015	Live Event
SANS Munich 2015	Munich, Germany	Feb 23, 2015 - Mar 07, 2015	Live Event
SANS Secure India 2015	Bangalore, India	Feb 23, 2015 - Mar 07, 2015	Live Event
Community SANS Des Moines	Des Moines, IA	Feb 23, 2015 - Feb 28, 2015	Community SANS
Community SANS Annapolis	Annapolis, MD	Feb 23, 2015 - Feb 28, 2015	Community SANS
SANS Cyber Guardian 2015	Baltimore, MD	Mar 02, 2015 - Mar 07, 2015	Live Event
SANS Northern Virginia 2015	Reston, VA	Mar 09, 2015 - Mar 14, 2015	Live Event
Community SANS Ottawa	Ottawa, ON	Mar 09, 2015 - Mar 14, 2015	Community SANS
SANS Secure Canberra 2015	Canberra, Australia	Mar 16, 2015 - Mar 28, 2015	Live Event
Mentor Session - SEC 401	Morrisonville, NY	Mar 17, 2015 - May 19, 2015	Mentor
SANS Oslo 2015	Oslo, Norway	Mar 23, 2015 - Mar 28, 2015	Live Event
SANS Houston 2015	Houston, TX	Mar 23, 2015 - Mar 28, 2015	Live Event
SANS 2015	Orlando, FL	Apr 11, 2015 - Apr 18, 2015	Live Event