nccgroup
freedom from doubt

Third Party Supplier Security

Managing risk and compliance through external due diligence audits.

Presented by: Stephen Higgins

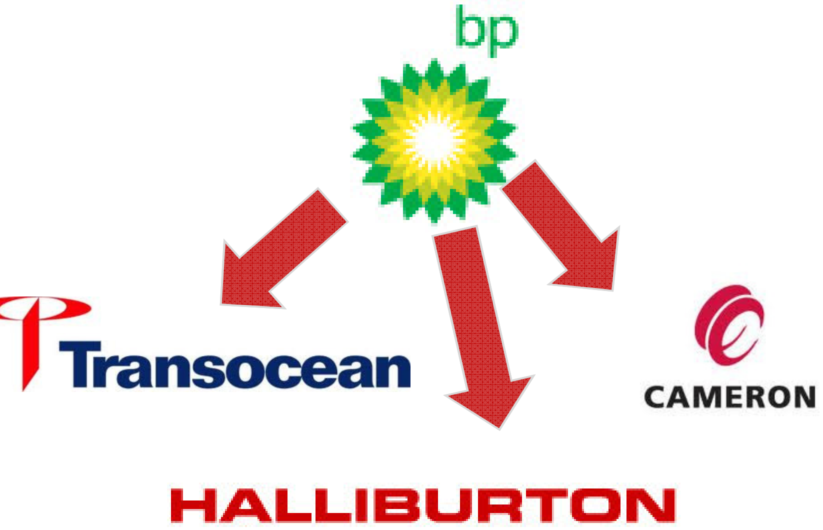
6th December 2012

To cover

- When third party supplier security goes wrong . . .
- Compliance and Legislative security obligations
- Best practice controls for securing third party suppliers
- Different models for due diligence reviews
- Business case for using an independent external auditor.

When the supply chain goes wrong

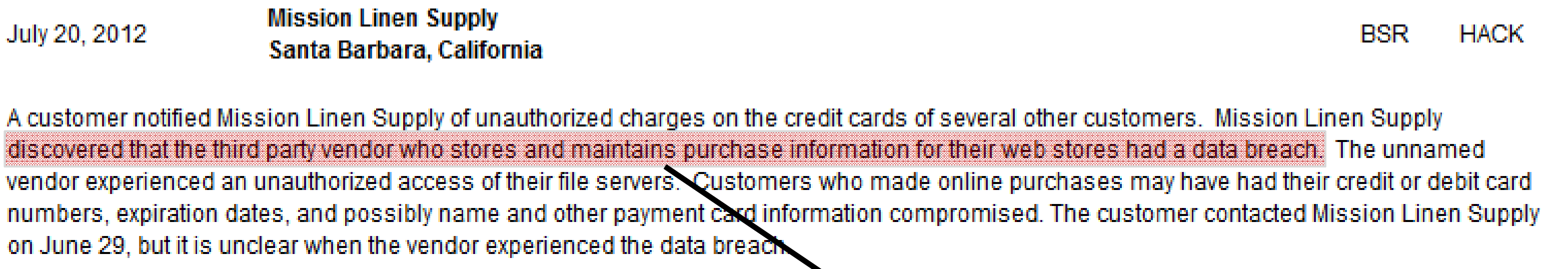
nccgroup
freedom from doubt



- **BP's Deepwater Horizon** is the largest accidental marine oil spill in the history.
- BP issued **$40bn** worth of lawsuits against rig owner Transocean, cementer Halliburton and blowout preventer manufacturer Cameron.
- Impact to BP:
  - Clean-up and litigation costs
  - Worldwide Brand impact.
  - Senior Management team resignations
  - Future contracts

And when it goes wrong with sensitive data. . .

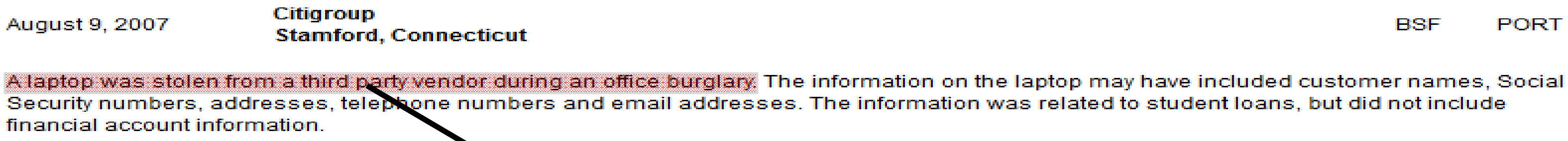
- US state disclosure laws allow us to look at real incidents where the root cause of a data breach was because of a lapse in security by a third party supplier.



July 20, 2012 | **Mission Linen Supply**
Santa Barbara, California | BSR | HACK

A customer notified Mission Linen Supply of unauthorized charges on the credit cards of several other customers. Mission Linen Supply discovered that the third party vendor who stores and maintains purchase information for their web stores had a data breach. The unnamed vendor experienced an unauthorized access of their file servers. Customers who made online purchases may have had their credit or debit card numbers, expiration dates, and possibly name and other payment card information compromised. The customer contacted Mission Linen Supply on June 29, but it is unclear when the vendor experienced the data breach.

… discovered that the third party vendor who stores and maintained purchase information for their web site had a breach.



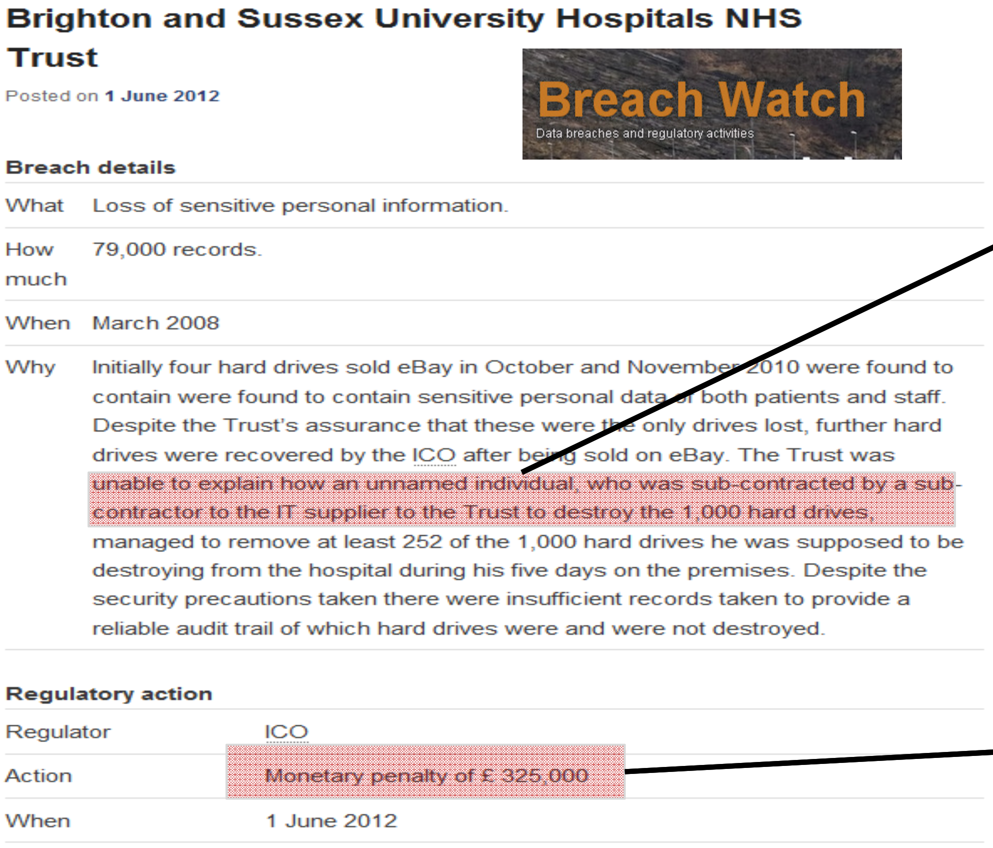
August 9, 2007 | **Citigroup**
Stamford, Connecticut | BSF | PORT

A laptop was stolen from a third party vendor during an office burglary. The information on the laptop may have included customer names, Social Security numbers, addresses, telephone numbers and email addresses. The information was related to student loans, but did not include financial account information.

A laptop was stolen from a third party vendor during an office burglary.

And in the UK . . .

- A web-site called Breach Watch collects UK data breaches which includes breaches caused by third parties and the monetary penalties . .



Brighton and Sussex University Hospitals NHS Trust

Posted on **1 June 2012**

Breach details

What	Loss of sensitive personal information.
How much	79,000 records.
When	March 2008
Why	Initially four hard drives sold eBay in October and November 2010 were found to contain were found to contain sensitive personal data of both patients and staff. Despite the Trust's assurance that these were the only drives lost, further hard drives were recovered by the ICO after being sold on eBay. The Trust was unable to explain how an unnamed individual, who was sub-contracted by a sub-contractor to the IT supplier to the Trust to destroy the 1,000 hard drives, managed to remove at least 252 of the 1,000 hard drives he was supposed to be destroying from the hospital during his five days on the premises. Despite the security precautions taken there were insufficient records taken to provide a reliable audit trail of which hard drives were and were not destroyed.

Regulatory action

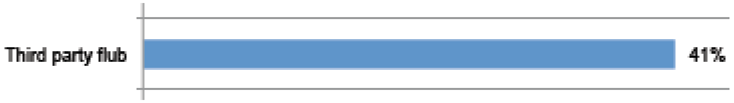
Regulator	ICO
Action	Monetary penalty of £ 325,000
When	1 June 2012

The Trust was unable to explain how an unnamed individual, who was sub-contracted by a sub-contractor managed to remove 252 of 1000 hard drives he was supposed to be destroying.

Monetary penalty of £325,000

Some data breach statistics. . .

- The following are extracts from the 2011 Ponemon Institute Cost of a data breach study and the Trustwave 2012 Global Security Report.



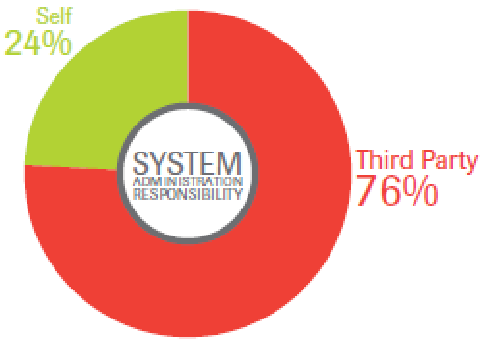
Data was lost or stolen due to a third party.

Forty-one percent of organizations had a data breach caused by a third party. This can include when protected data is in the hands of outsourcers, cloud providers and business partners.

2011 Cost of Data Breach Study: United States
Ponemon Institute, March 2012

System Administration Responsibility

The majority of our analysis of data breach investigations – 76% – revealed that the third party responsible for system support, development and/or maintenance introduced the security deficiencies exploited by attackers. Small businesses within the food and beverage and retail industries were most often impacted by these attacks, as they typically outsource all development and support of their systems. Anecdotally, merchants were unaware of the security best practices or compliance mandates by which their partners were required to abide. In other instances, victims were unaware that this third party was only responsible for a subset of security controls – thus still leaving these systems open to attack.

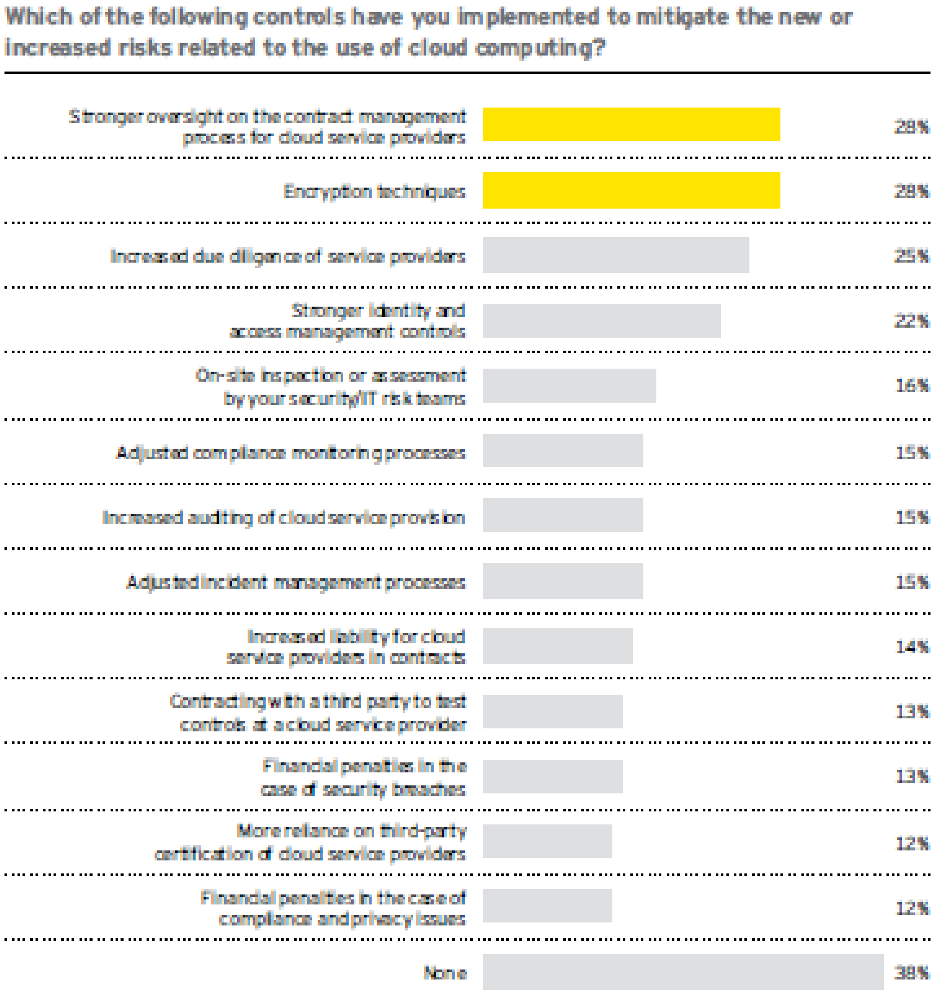


Business context for outsourcing . . .

- Outsourcing security controls and sharing sensitive data has many business benefits:
  - ✓ Cost savings.
  - ✓ Improve quality.
  - ✓ Allows the business to focus on core activities.
  - ✓ Rapid implementation of a major change in strategy or approach which could not be done in-house for cultural, resource or capability reasons.
  - ✓ The need for new or increased capability which had never been implemented and operated in-house.
  - ✓ Speed of exploitation of new technologies or capabilities to deliver competitive edge.
  - ✓ Transfer of risk.
  - ✓ To meet compliance or contractual obligations.

Caution for using outsourced cloud services

- In the Ernst &Young 2012 Global Information Security Survey, there is focus on third party contract management and auditing of cloud service providers to address risks of using new technologies.
- We are finding that organisations want a systematic and repeatable approach to auditing their third party suppliers.

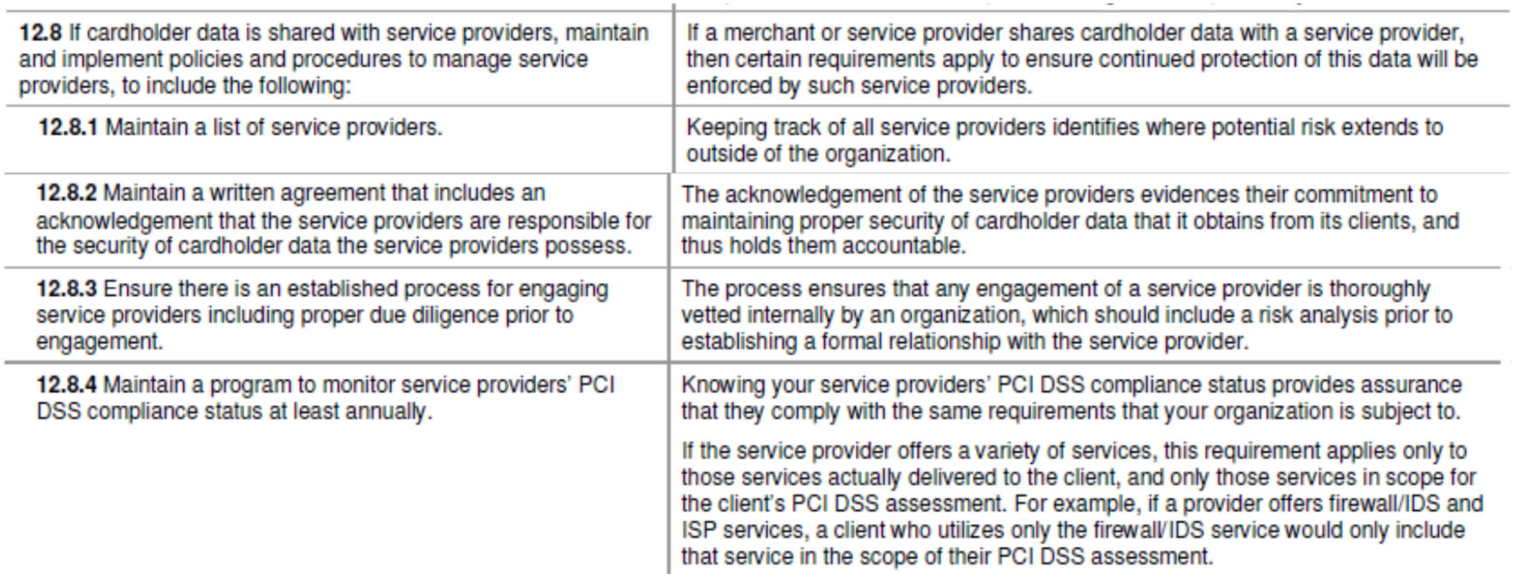


Compliance and legislative third party compliance obligations. . .

- Organisations have a responsibility for the security of their data assets and their customer’s data. Typically these can be categorised into:
  - Legalisation - Data Protection Act (DPA).
  - Compliance – ISO 27001, HMG Information Assurance Standards, Sarbanes-Oxley Act (SOX), Payment Card Industry Data Security Standard (PCI DSS) etc.
  - Contractual – Meeting security requirements defined in contract with business partners, customers etc.
- A data breach where contractual or legislative obligations in relation to managing the organisations data when shared with a 3rd party will still impact the organisation:
  - **Brand impact and reputation** – it’s your name and it’s you who your customer’s will blame – and it’s your share price.
  - **Fines** – You will pay the fine and be liable and you may not be able to pass on the liability.
  - **Remediation costs** – it is prohibitively expensive to fix a problem in a hurry.
  - **Customer confidence & lost revenue** – a breach may impact other customer’s confidence in your services.

Example - PCI DSS Best Practice. . .

- Third party providers may manage part or all of the organisation's Cardholder Data environment
- PCI related Service providers are responsible for validating their own compliance with PCI DSS.
- An entity (PCI Merchant or Service Providers) must contractually require all associated third parties with access to Cardholder Data to adhere to PCI DSS (Requirement 12.8 and sub-requirements).
- Due Diligence of third party suppliers may consist of:
  - Include service provider in scope of entity's assessment – right to audit.
  - Request evidence relating to independent assessment of service provider.
  - Service provider performs a self assessment



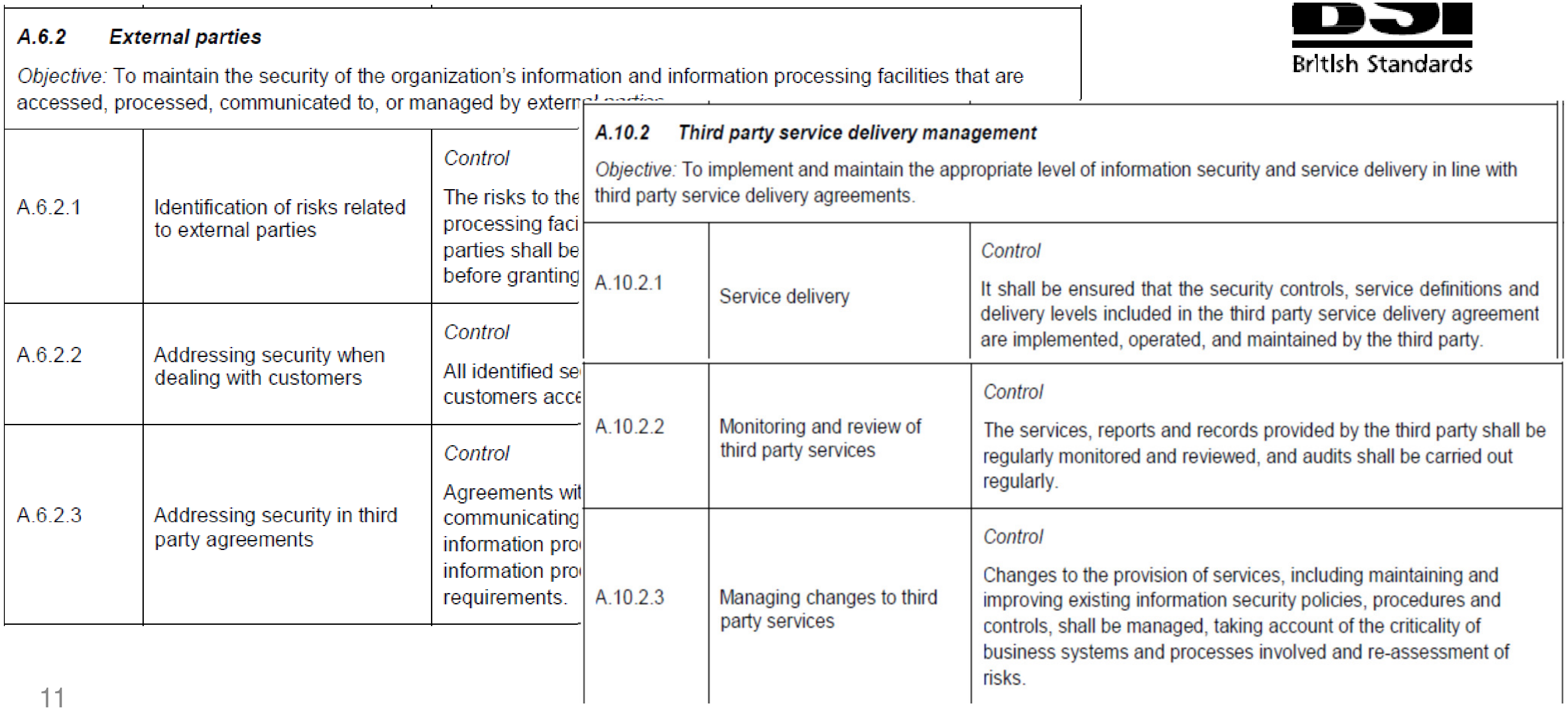
12.8 If cardholder data is shared with service providers, maintain and implement policies and procedures to manage service providers, to include the following:	If a merchant or service provider shares cardholder data with a service provider, then certain requirements apply to ensure continued protection of this data will be enforced by such service providers.
12.8.1 Maintain a list of service providers.	Keeping track of all service providers identifies where potential risk extends to outside of the organization.
12.8.2 Maintain a written agreement that includes an acknowledgement that the service providers are responsible for the security of cardholder data the service providers possess.	The acknowledgement of the service providers evidences their commitment to maintaining proper security of cardholder data that it obtains from its clients, and thus holds them accountable.
12.8.3 Ensure there is an established process for engaging service providers including proper due diligence prior to engagement.	The process ensures that any engagement of a service provider is thoroughly vetted internally by an organization, which should include a risk analysis prior to establishing a formal relationship with the service provider.
12.8.4 Maintain a program to monitor service providers' PCI DSS compliance status at least annually.	Knowing your service providers' PCI DSS compliance status provides assurance that they comply with the same requirements that your organization is subject to. If the service provider offers a variety of services, this requirement applies only to those services actually delivered to the client, and only those services in scope for the client's PCI DSS assessment. For example, if a provider offers firewall/IDS and ISP services, a client who utilizes only the firewall/IDS service would only include that service in the scope of their PCI DSS assessment.

Example(2) – ISO 27001/2 Best Practice. . .

nccgroup
freedom from doubt

- Third party providers should be included in the ISO 27001 Risk Assessment and reviewed against the organisations risk appetite.
- ISO 27002 controls for managing the risk associated with third party provides should be applied to treat the risk where applicable.

BSi
British Standards



A.6.2 *External parties*

Objective: To maintain the security of the organization's information and information processing facilities that are accessed, processed, communicated to, or managed by extern

A.6.2.1	Identification of risks related to external parties	*Control* The risks to the processing faci parties shall be before granting
A.6.2.2	Addressing security when dealing with customers	*Control* All identified se customers acce
A.6.2.3	Addressing security in third party agreements	*Control* Agreements wit communicating information pro information pro requirements.

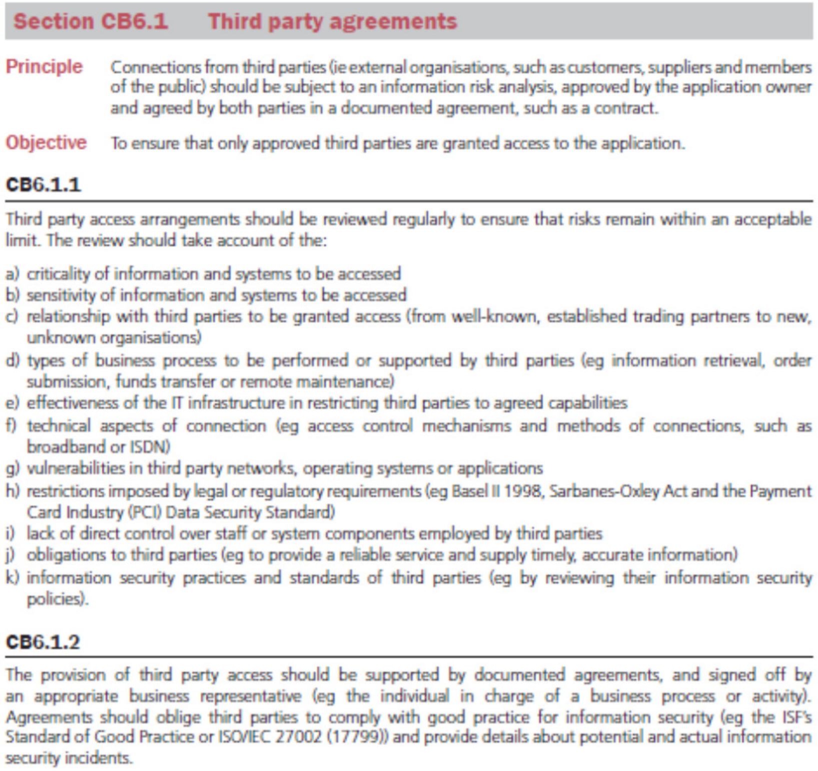
A.10.2 *Third party service delivery management*

Objective: To implement and maintain the appropriate level of information security and service delivery in line with third party service delivery agreements.

A.10.2.1	Service delivery	*Control* It shall be ensured that the security controls, service definitions and delivery levels included in the third party service delivery agreement are implemented, operated, and maintained by the third party.
A.10.2.2	Monitoring and review of third party services	*Control* The services, reports and records provided by the third party shall be regularly monitored and reviewed, and audits shall be carried out regularly.
A.10.2.3	Managing changes to third party services	*Control* Changes to the provision of services, including maintaining and improving existing information security policies, procedures and controls, shall be managed, taking account of the criticality of business systems and processes involved and re-assessment of risks.

Example(3) – ISF Standard of Good Practice

- The Information Security Forum Standard of Good Practice provides guidance on Third Party Agreements and Third Party Access. .



Section CB6.1 Third party agreements

Principle Connections from third parties (ie external organisations, such as customers, suppliers and members of the public) should be subject to an information risk analysis, approved by the application owner and agreed by both parties in a documented agreement, such as a contract.

Objective To ensure that only approved third parties are granted access to the application.

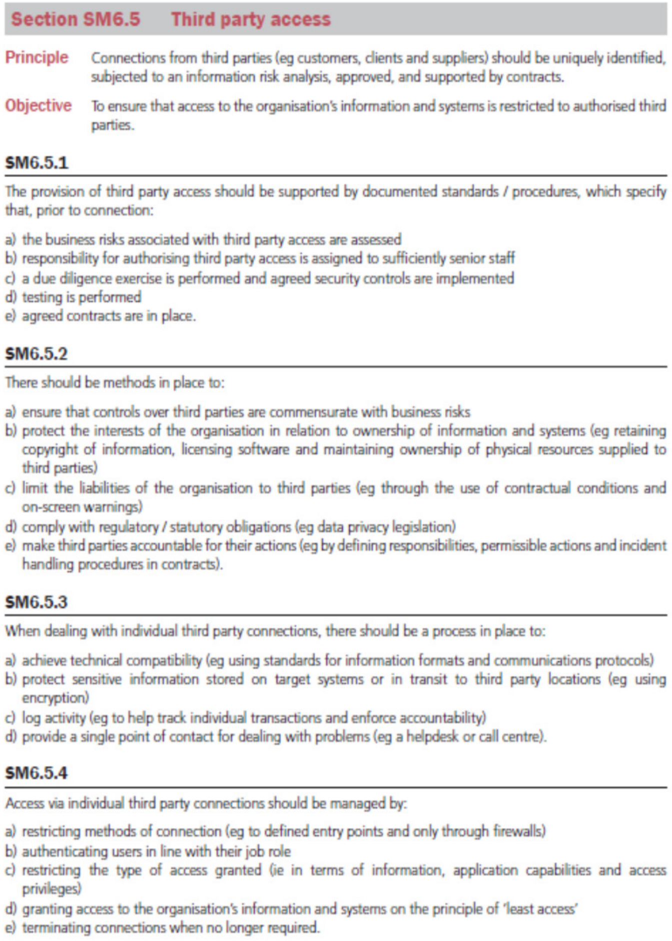
CB6.1.1

Third party access arrangements should be reviewed regularly to ensure that risks remain within an acceptable limit. The review should take account of the:

a) criticality of information and systems to be accessed
b) sensitivity of information and systems to be accessed
c) relationship with third parties to be granted access (from well-known, established trading partners to new, unknown organisations)
d) types of business process to be performed or supported by third parties (eg information retrieval, order submission, funds transfer or remote maintenance)
e) effectiveness of the IT infrastructure in restricting third parties to agreed capabilities
f) technical aspects of connection (eg access control mechanisms and methods of connections, such as broadband or ISDN)
g) vulnerabilities in third party networks, operating systems or applications
h) restrictions imposed by legal or regulatory requirements (eg Basel II 1998, Sarbanes-Oxley Act and the Payment Card Industry (PCI) Data Security Standard)
i) lack of direct control over staff or system components employed by third parties
j) obligations to third parties (eg to provide a reliable service and supply timely, accurate information)
k) information security practices and standards of third parties (eg by reviewing their information security policies).

CB6.1.2

The provision of third party access should be supported by documented agreements, and signed off by an appropriate business representative (eg the individual in charge of a business process or activity). Agreements should oblige third parties to comply with good practice for information security (eg the ISF's Standard of Good Practice or ISO/IEC 27002 (17799)) and provide details about potential and actual information security incidents.



Section SM6.5 Third party access

Principle Connections from third parties (eg customers, clients and suppliers) should be uniquely identified, subjected to an information risk analysis, approved, and supported by contracts.

Objective To ensure that access to the organisation's information and systems is restricted to authorised third parties.

SM6.5.1

The provision of third party access should be supported by documented standards / procedures, which specify that, prior to connection:

a) the business risks associated with third party access are assessed
b) responsibility for authorising third party access is assigned to sufficiently senior staff
c) a due diligence exercise is performed and agreed security controls are implemented
d) testing is performed
e) agreed contracts are in place.

SM6.5.2

There should be methods in place to:

a) ensure that controls over third parties are commensurate with business risks
b) protect the interests of the organisation in relation to ownership of information and systems (eg retaining copyright of information, licensing software and maintaining ownership of physical resources supplied to third parties)
c) limit the liabilities of the organisation to third parties (eg through the use of contractual conditions and on-screen warnings)
d) comply with regulatory / statutory obligations (eg data privacy legislation)
e) make third parties accountable for their actions (eg by defining responsibilities, permissible actions and incident handling procedures in contracts).

SM6.5.3

When dealing with individual third party connections, there should be a process in place to:

a) achieve technical compatibility (eg using standards for information formats and communications protocols)
b) protect sensitive information stored on target systems or in transit to third party locations (eg using encryption)
c) log activity (eg to help track individual transactions and enforce accountability)
d) provide a single point of contact for dealing with problems (eg a helpdesk or call centre).

SM6.5.4

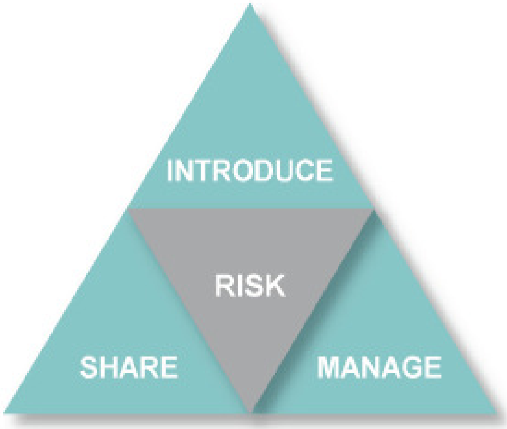
Access via individual third party connections should be managed by:

a) restricting methods of connection (eg to defined entry points and only through firewalls)
b) authenticating users in line with their job role
c) restricting the type of access granted (ie in terms of information, application capabilities and access privileges)
d) granting access to the organisation's information and systems on the principle of 'least access'
e) terminating connections when no longer required.

Risks presented by Third party suppliers

- Organizations may outsource business processes, obtain services, or have business relationships with third party suppliers that could influence the security of information assets.
- Performing a risk assessment is essential to understanding the level of risk that could be introduced to the organization by conducting business with third party suppliers.
- Third parties represent three major areas to consider for risk management: they may introduce risk, they may share risk, or they may manage risk:

	Third Parties may:	Such as:
1	**Introduce risk**	The development of an application that processes, stores, or transmits CHD
2	**Manage risks**	An outsourced business process
3	**Share risk**	A shared business process



Security requirements for different third party suppliers

- Any organisation may have different categories of 3rd party vendors which can broadly fit into:
  - ✓ **Fully Outsourced service** – all aspects of the service are outsourced to a 3rd party.
  - ✓ **Managed services** - the third party service provide provides service either on-site or off-site.
  - ✓ **Contractor services** – the third party service provider provides specialist to augment the organisations resource.
  - ✓ **Technology or product supplier** – the third party provides a technology or product and support services to the organisation.
- **Identifying and communicating which security requirements and controls apply to and should be fulfilled by each third party may be complex**.
- **Further, validating that each third party are adhering to their security obligations adds another layer of complexity.**

Key best practices for security within third party contracts

- **Explicit security obligations** – All security obligations and roles and responsibilities to be met by the supplier should be explicitly entered into the contract (typically in a security schedule)

- **Liabilities relating to a data breach** – The compensations and penalties that could be imposed in the event of a data breach should be clearly specified. This must be agreed and clearly understood by the supplier.

- **Right to Audit** - This allows for the security health of the supplier to be monitored. It should consider sub-contractors to the supplier and indicate the mode of audit (e.g. the organisation's internal audits, an external independent auditor or self-assessment).

- **Post-contractual Obligations** – Outline obligations by the supplier in relation to protecting confidential information, revocation of access rights, disposing or returning information, disposal or destruction of assets upon terminal of the contract.

- **Incident reporting obligations** – include within the agreement obligations of the service provider to notify the company of any issues affecting the delivery or security of the outsourced service.

Options for reviewing third party supplier security obligations

Method	Approach	Pros	Cons
Organisations Internal Audit	The Organisation's Internal Audit Function or Security Team performs a security audit of their third party suppliers.	• Retain control over the audit • Can focus on perceived risks of each supplier to the organisation. • Direct control over costs and may be cheaper than external auditors.	• There may be a lack of Internal resources. • Internal resource may not have the right skills and experience. • Not independent which may lead to contractual disputes. • Becomes challenging for a large number of third party suppliers
External Auditors	An Independent third party performs a security audit of third party suppliers.	• Provides access to specialist skilled auditor resources. • Independence / neutrality may benefit in terms of confidentiality issues. • If external auditor misses something, they may be liable.	• Typically more expensive than internal audit. • May not focus on areas deemed important.
Self-Assessment	Customer completes a security questionnaire	• Customer attests to meeting security obligations to hold liabilities. • Customer provides supporting evidence of controls in place	• There is no due diligence unless third party provide internal / external audit reports to back up attestation.
ISO27001 certification	Supplier holds ISO 27001 certification	• Supplier holds the cost of achieving and maintaining compliance and the cost of the ISO 27001 audit.	• ISMS scope may not cover all security requirements associated with the service.

Business case for using an external security auditor of third party suppliers

- NCC Group are increasingly being asked to perform an independent security review of an organisations third party suppliers based on the following:
  - ✓ Where there isn’t the internal resource to perform audits.
  - ✓ Where there are a large number of suppliers to be audited.
  - ✓ Where the Internal resources don’t have experience of specific compliance standards (e.g. ISO 27001/2, PCI DSS, SOX, HMG Information Assurance Standards etc.)
  - ✓ Where using an external suitably qualified neutral organisation to conduct the audits avoids any political or contractual disputes between the two contracted organisations relating to the audit findings.
- In addition, we provide the following value:
  - ✓ Because our auditors have a breadth of experience across a number of security requirements, we are helping find issues with the supplier’s compliance status not directly related to the areas being audited.
  - ✓ We provide an auditing tool to cover different types of audits that can be manipulated to meet specific client requirements.
  - ✓ We have resource willing to travel to different geographical locations.

Example – The challenge

nccgroup
freedom from doubt

- We were approach by a large multi-national financial organisation to deliver an extended external security audit programme to review 113 Critical Suppliers, 443 High Risk Suppliers and additional third party on-boarding suppliers.
- In order to conduct a level of due diligence proportionate to the risk posed by the third party supplier, the organisation wanted a tiered approach to performing the external security audits consisting of two types of audit:
  - **Comprehensive or Onsite Audit** - 2 days onsite audit by a qualified Information Security audit with 2 days reporting total 4 days.
  - **Off Site or Desk Based** – Each Supplier submits a competed Self-Assessment Questionnaire (SAQ) tool and which is reviewed offsite – 2 days total (will involve some email/telephone interviews exchange of evidence with the supplier)
- The organisation wanted the audit management process to be dully managed by the auditing company so they could focus on the findings and remediation.

The Solution

- We created an audit management programme for the organisation and worked with the organisation to create a standard set of security controls based on different best practices and specific organisations security requirements to be reviewed.
- Key aspects of the external service are:
  - ✓ **Dedicated Audit Management Team** – Small team managing and administrating the audit programme covering scheduling, resourcing, quality assurance of reports, management and progress reporting to the customer and dispute management.
  - ✓ **Tailored Third Party Audit Tool** – Creation, tailoring and maintenance of an audit tool to facilitate the audit process.
    - ❑ Based on based practice (e.g. ISO 27001/2) focussing on controls identified during risk assessment and commonality across the supplier base.
    - ❑ Drop down menu to facilitate auditing and to provide statistic generation to provide reporting across the supplier base..
    - ❑ Report generation functionality to increase audit efficiencies.
  - ✓ **Pool of qualified Information Security Auditors** – Senior Information Security auditors with a breadth of experience of conducting and performing security and compliance reviews.

How we approached this . .

freedom from doubt

- **Initial engagement & set up**
  - Assign overall responsibility for the programme
  - Set up Secure Portal for client.
  - Project Initiation Meeting and PID outlining key tasks, timelines, contacts, MI required by client.
  - Receive key customer data from client, e.g. breakdown of different supplier types
- **Audit Approach**
  - Fine-tune and agree the audit standard
  - Review and tailor the planned documentation
  - Agree format, expected content, additional governance and compliance concerns
- **Programme and Audit plan**
  - Allocate key milestones
  - Schedule audits
- **Review of the audit programme – the feedback loop**
  - Monthly meeting to review programme process
  - MI submitted to client in the required format
- **New third parties**
  - Incorporate new third party suppliers into the programme based on the agreed priority and assigned category

Last Thought . . .

- Third party supplier may be under financial constraints in the current challenging business climate.
- The financial stability of a service provider can indirectly impact on information assurance:

➢ **Morale** - The morale of their staff is likely to be lower and attrition rates may increase, leading to the loss of key information assurance expertise.

➢ **Priority** - Third party supplier may give priority of service to more profitable customers.

➢ **Efficiencies** - Cost-saving exercises may result in a breach of some agreed minimum security standards, such a segregation of duties, tools for centralised auditing or frequency of security updates.

➢ **Post-contract obligations** – Third party suppliers may be reluctant to engage fully in knowledge or service transfers to alternative service providers and to secure dispose of customer’s data

Questions . . .

nccgroup
freedom from doubt

- Supplier Assured by NCC Group can give you the independent assurance and peace of mind you need that your third party suppliers are taking serious, proactive measures to ensure the on-going security of your information.
- Our expert team will review your supplier data security controls from an environmental, procedural, physical and technical stance. Underpinned by industry best practices such as ISO 27001, we will deliver a holistic view of your supplier's current security posture.
- We deliver this as a fully managed service, engaging with your third parties on your behalf to conduct the audit.
- On completion of the project, you will receive a full management report containing any identified security issues, enabling you to take appropriate steps in order to mitigate any possible risk.
- It's essential to treat the information security of your suppliers with the same seriousness as your own, and verify the systems and processes they have in place.

Supplier Assured

How secure are your third party suppliers and partners?

nccgroup

freedom from doubt

UK Offices

Manchester - Head Office

Cheltenham

Edinburgh

Leatherhead

London

Thame

European Offices

Amsterdam - Netherlands

Munich – Germany

Zurich - Switzerland

North American Offices

San Francisco

Atlanta

New York

Seattle

Australian Offices

Sydney