NormShield

THIRD-PARTY RISK IN REGULATIONS

HIPAA Compliant

EU GDPR COMPLIANT

NIST

COBIT 5 AN ISACA® FRAMEWORK

Information Security Management System ISO 27001 Certified

PCI DSS COMPLIANT

August 2018

CONTENTS

HIDDEN RISK: 3RD PARTY VENDORS

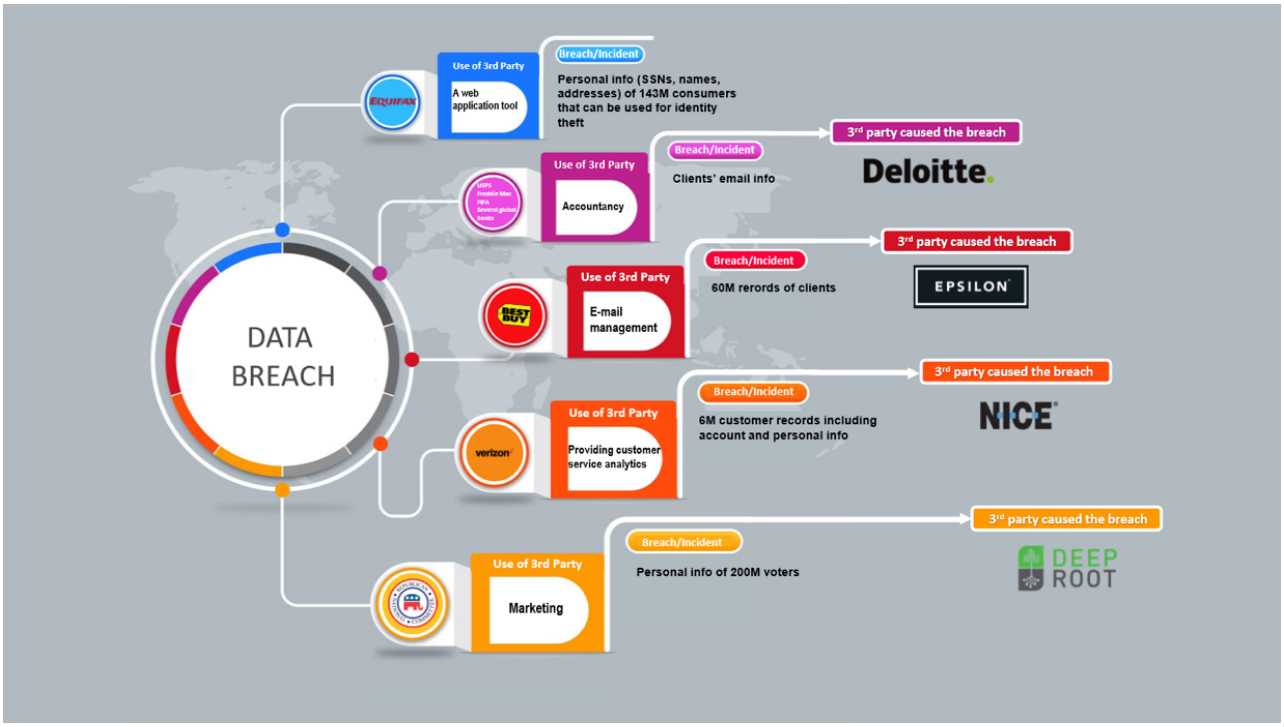
Executive Summary

Many companies rely on regulations created by trustworthy organizations to check their cyber security measurements. Compliance to these regulations helps companies and organizations to improve their security posture and they present themselves as “secure”. Lack of compliance may impose very high penalties and reputation loss.

Even though compliance-aware organizations meet well-known and regulated-by-law standards, they may still suffer penalties due to 3rd party vendors’ lack of compliance.

Since 3rd party attacks (aka supply chain attacks) are on the rise recently, we examine the perspective of regulations (such as GDPR, NIST, ISO 27001, PCI DSS, HIPAA, and COBIT) on 3rd party cyber risk management.

THIRD-PARTY RISK



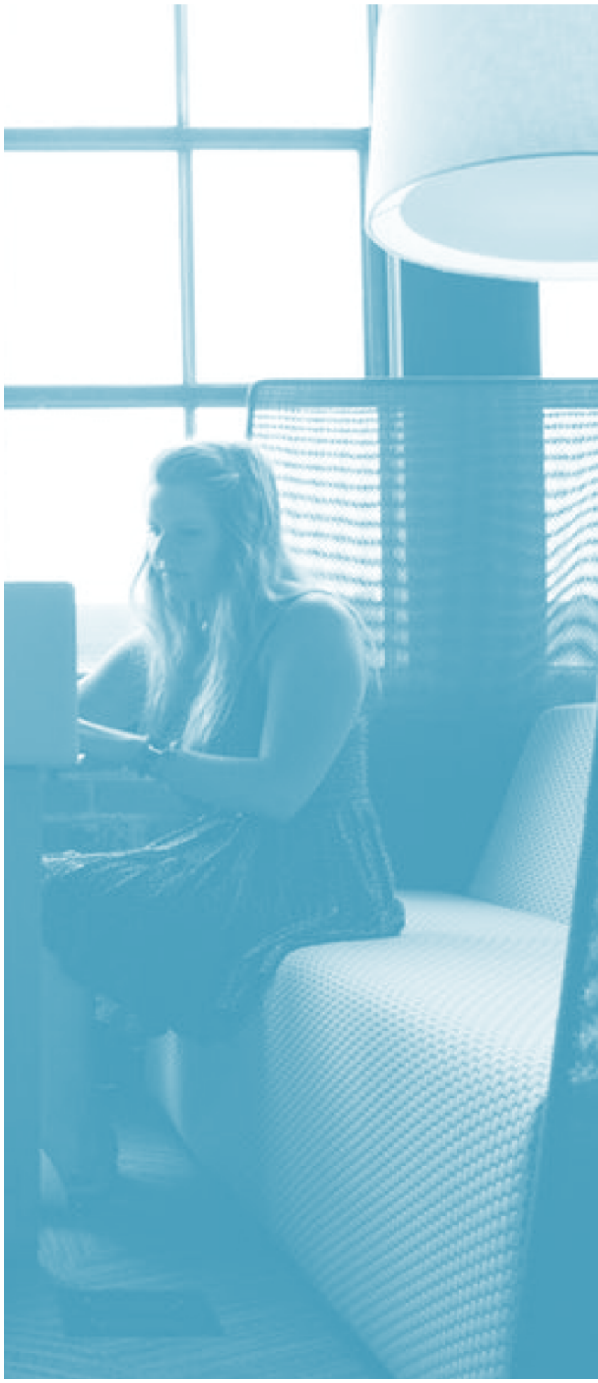
Recent breach of TicketMaster(*) originated from a 3rd party supplier for their website have increased attention to 3rd party risk. Recently, we have heard similar stories about breaches because of 3rd parties such as vendors, subsidiaries, web hosting companies, law firm partners, firms in supply chain, etc.

Large companies such as financial institutions, e-commerce companies have been improving their cyber security system for external or even internal attacks. They can internally identify vulnerabilities of their own system by monitoring and/or scanning tools and take necessary precautions. However, all these efforts might be for nothing if 3rd party cyber risk is unknown. 3rd party risk management and data governance are growing concerns.

(*) https://www.normshield.com/lesson-from-ticketmaster-breach-cdn-security-of-third-party-suppliers/

THIRD-PARTY RISK

"56% of the companies have experienced a 3rd-party breach in 2017"



3rd-party risk is on the rise

A recent survey conducted by Ponemon Institute(+) reveals that 56% of companies have experienced a 3rd-party breach in 2017, which is an increase of 7% compared to previous year. Data breaches caused by third parties cost millions of dollars to large companies.

What is 3rd party?

Third-parties include broad range of companies a company directly worked with such as data management companies, law firms, e-mail providers, web hosting companies, subsidiaries, vendors, sub-contractors, basically any company whose employees or systems have access to your systems or your data. However, third-party cyber risk is not limited to these companies. Any external software or hardware that you use for your business also poses a cyber risk.

(+) https://www.opus.com/ponemon/

GDPR

The Europe Union (EU) General Data Protection Regulation (GDPR) proposed by Europe Commission became active after May 25, 2018. GDPR has very strict rules about collecting, storing, and processing data.

Gathering even very small piece of information about an EU citizen requires consent from customer/visitor and very high responsibility for the companies. The fines are quite high in case of breach; they are up to as high as 20 million Euros or 4% of annual global turnover whichever is the highest.

Therefore, asking to fill a form even for a newsletter requires some adjustment to comply GDPR rules and to avoid penalties.

Is your website GDPR-compliant? Check here.

GDPR

GDPR rules apply to 3rd party data providers

Businesses, as 'data controllers' have been preparing themselves for GDPR long before it is forced by EU. However, self-preparation does not suffice unless third party compliance is taken into consideration. Third parties use and store personal information are called 'data processors' in GDPR and 'data controllers' are obligated to manage their third-party 'data processors' for them to meet GDPR rules.

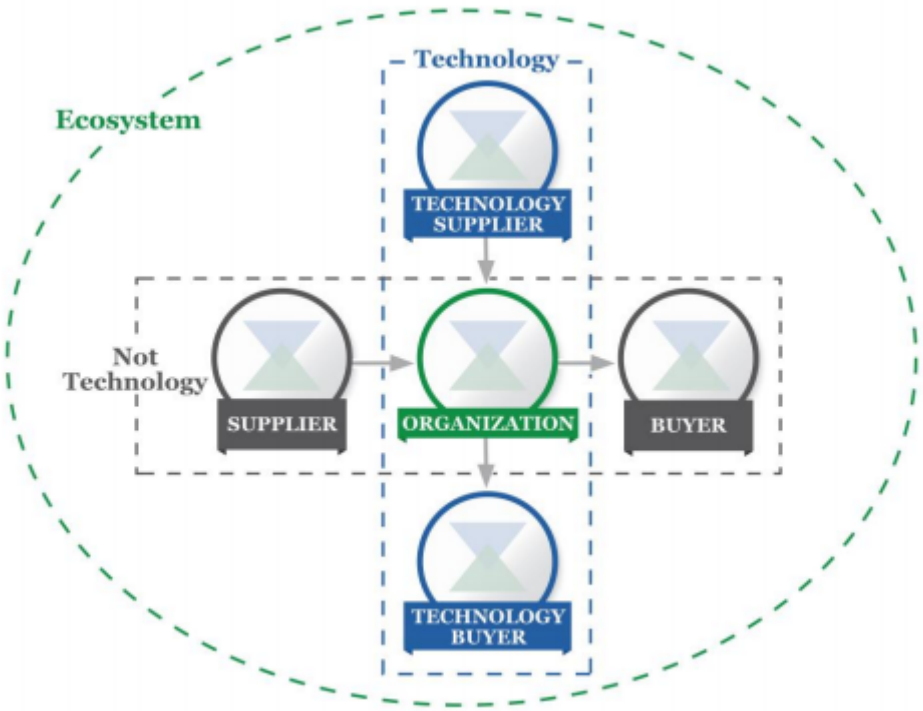
Simple steps to meet 3rd party GDPR compliance

- *Determine all third parties (even website applications) that operate (gather, store, and/or use) personal information*
- *Restrict access to sensitive data (does third party really need to access that data)*
- *Assess 3rd party for GDPR risk*
- *Keep logs of all data-processing activities*
- *Make sure any data-gathering activity ask for consent from use*

NIST

Recently, National Institute of Standards and Technology (NIST) released new version of its Cybersecurity Framework (v. 1.1), which includes several additions such as cyber risk originated from supply chains (aka 3rd party attacks).

The version 1.1 is a risk-based framework to improve cybersecurity of critical infrastructure in the US. However, it is used by many companies as a guideline to assess their cyber risk and some public or private institutions are looking for compliance to this framework.



Source: NIST Cybersecurity Framework v1.1

Further in the Section, cyber SCRM is described in a full-duplex manner with cybersecurity effect an organization [that] has on external parties and the cybersecurity effect [that] external parties have on an organization

NIST

What NIST says about supply chain cyber risk?

The Section 3.3 of NIST updated cybersecurity framework defines the supply chain as follows;

Supply chains are complex, globally distributed, and interconnected sets of resources and processes between multiple levels of organizations. Supply chains begin with the sourcing of products and services and extend from the design, development, manufacturing, processing, handling, and delivery of products and services to the end user. Given these complex and interconnected relationships, supply chain risk management (SCRM) is a critical organizational function.

Further in the Section, cyber SCRM is described in a full-duplex manner with cybersecurity effect an organization [that] has on external parties and the cybersecurity effect [that] external parties have on an organization.

SCRM activities listed by NIST

- Determining cybersecurity requirements for suppliers,
- Enacting cybersecurity requirements through formal agreement (e.g., contracts),
- Communicating to suppliers how those cybersecurity requirements will be verified and validated,
- Verifying that cybersecurity requirements are met through a variety of assessment methodologies, and
- Governing and managing the above activities

PCI-DSS

Payment Card Industry (PCI) Security Standard Council releases Data Security Standard to explain requirements and security assessment procedures. The latest version (v 3.2) was released on April 2016 and starting February 2018 it became effective as requirements.

PCI is an internationally-recognized institution that determines the standards for payment card industry (including merchants of all sizes, financial institutions, point-of-sale vendors, and hardware and software developers) to make cardholders safer.

Any breach on payment systems affect the entire payment ecosystem and consequences usually results in huge financial losses. Financial institutions that experience data breach lose credibility and reliability.

The main document for PCI is PCI Data Security Standards (PCI DSS) which provides an actionable framework to secure and make robust payment card data processes (prevention, detection and response to cyber incidents).

PCI-DSS

PCI DSS's Perspective on 3rd Parties

PCI DSS states that a service provider or a merchant may use a third-party for data storage, processing, or transmitting cardholder data or management of hardware/software components (routers, firewalls, databases, etc.).

However, PCI DSS immediately acknowledges that if a third-party is used, then there may be an impact on cardholder data ecosystem security. Therefore, they offer two options to third-party services to validate compliance. Third parties can either

- *Undergo an annual PCI DSS assessments on their own and provide evidence of compliance or*
- *Undergo assessments upon request of their customers and participate their customer's PCI DSS reviews.*

PCI-DSS

What requirements may be related to third parties?

- SS Requirements on firewall and router configurations (1.1, 1.2, 1.3, and 1.4) are directly related to third party hardware/software service providers that handle these tasks.
- PCI DSS also recommends to always change vendor-supplied defaults and remove or disable unnecessary default accounts before installing a system on the network (2.1) including (but not limited to) operating systems, software that provides security services, application and system accounts, point-of-sale (POS) terminals, payment applications, etc.
- PCI DSS mentions shared hosting providers (2.6) by forcing them to meet specific requirements detailed in an Appendix (A1), a section whose sole purpose is to explain Shared Hosting Provider Requirements.
- Section 3 is all about how to store cardholder data and if a third-party is used for data storage, these requirements have to be met. The motto of PCI is “if you don’t need it, don’t store it).
- Requirements of using anti-virus programs is given in Section 5 and these requirements also apply to third parties.
- PCI DSS defines requirements (6.3) for external software applications (including web-based applications).
- In Section 7 and 8, access control is defined to give requirements on who should access what. This section is directly related to third party data access. Third-party access is explicitly mentioned (as in 8.3.2).
- The risk from third-party personnel (such as personnel for repair services) is elaborated (9.9.3)

PCI-DSS

Steps to prevent liabilities from third-party service providers

- *Establish agreements with third parties. Agreements should be written clearly and should have references to PCI-DSS.*
- *Check PCI DSS requirements and determine which one of those should be met by the third party.*
- *Monitor compliance of the third-party*
- Prior to work with a third party, complete a risk assessment.

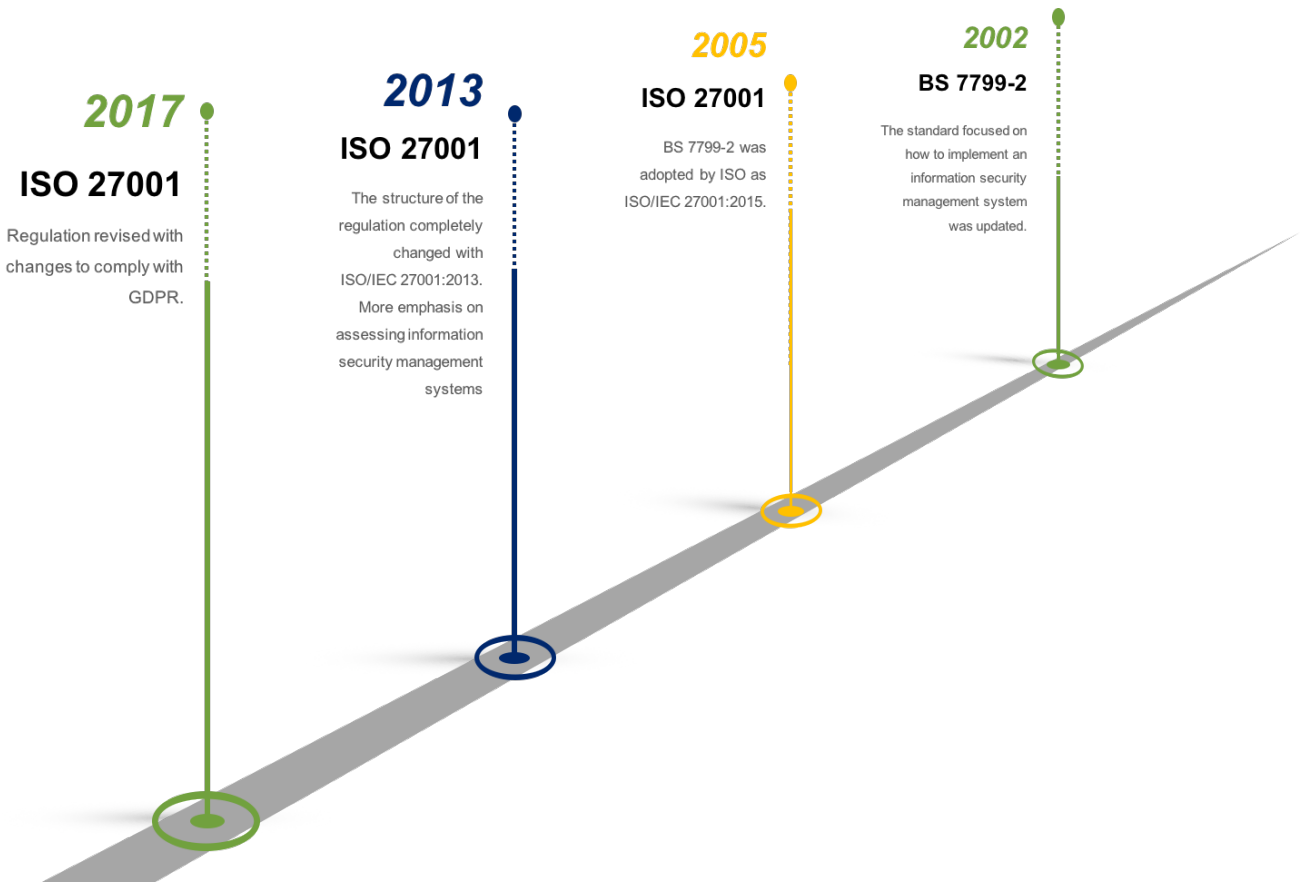
High-Level Overview of PCI-DSS

Build and maintain a secure network and systems	1. Install and maintain a firewall configuration to protect cardholder data 2. Do not used vendor-supplied defaults for system passwords and other security parameters
Protect cardholder data	3. Protect stored cardholder data 4. Encrypt transmission of cardholder data across open, public networks
Maintain a vulnerability management program	5. Protect all systems against malware and regularly update anti-virus software and applications 6. Develop and maintain secure systems and applications
Implement strong access control measures	7. Restrict access to cardholder data by business need to know 8. Identify and authenticate access to system components 9. Restrict physical access to cardholder data
Regularly monitor and test networks	10. Track and monitor all access to network resources and cardholder data 11. Regularly test security systems and processes
Maintain an information security policy	12. Maintain a policy that addresses information security for all personnel

ISO/IEC 27001

ISO/IEC 27001 (some only write ISO 27001) is an information security standard created by ISO and IEC jointly to standardize cyber security practices. It provides certain control items in 18 categories to improve cyber security of an organization.

Compliance to ISO 27001 standard provides benefit to an organization to better manage their IT systems with those control items. Besides, organizations that meet ISO 27001 requirements can be certified after an audit. The regulation is updated in 2017.



ISO/IEC 27001

Do third parties/ suppliers have to comply ISO 27001 standards?

Yes. ISO/IEC 27001, Section A15, defines five controls for Supplier Relationships. Based on these control, third party compliance can be checked in 5 steps.

5 steps to check supplier ISO/IEC 27001 compliance

- Create an information security policy for supplier relationships that address the processes and procedures to be implemented by the organization to mitigate the risks associated with the vendor.
- Make the supplier sign a contractual agreement to ensure that there will not be any misconceptions in future. For example, the organization may include legal and regulatory requirements, 'right to audit' clause, Terms & Conditions etc., in the contractual agreement
- Be clear about the agreements that include requirements to address information security risks associated with Information and communication technology services such as monitoring process, defining rules for sharing information etc.
- Monitor and review supplier services. The organization should monitor, review and conduct audits on supplier services at regular intervals to ensure that supplier is adhere to the terms and conditions as per the agreement.
- Manage change to supplier services such as update of information security policy, use of new technologies/tools, changes to physical location, improvised services, etc.

HIPAA

The Health Insurance Portability and Accountability Act (HIPAA) aims to protect health-related and personal information of individuals, including medical records, health insurance data, SSNs of patients, etc. These information is very valuable and profitable in the black market of dark web.

Every year the data theft or extortion through ransomwares become a very big problem for healthcare providers. Only last year, there were more than 40 major breach incident happened in healthcare industry

HIPAA

3rd Party Risk in Healthcare Industry

When we examine 40+ breach incidents of 2017, we see that third party vendors are second most frequent reason behind a breach followed by phishing attacks.
Health Insurance companies, medical-equipment suppliers, imaging centers, marketing companies, data-management companies, website and e-mail providers are all potential third parties that attackers can find a way through healthcare providers' systems. Here are some breaches caused by third parties in 2017.

- *A medical-equipment supplier, Airway Oxygen, was hacked and the attackers installed a ransomware by holding 500,000 clients' information hostage.*
- *iHealth Innovations, a third-party managing the record backups for healthcare providers, caused a breach of tens of thousands (possibly up to millions) of patient records at Bronx-Lebanon Hospital Center in New York City.*
- *New Jersey Diamond Institute for Fertility and Menopause took the advantage of using a third-party server to store electronic health records. But this advantage turned into a nightmare when more than 14,000 patients' sensitive information were exposed after a cyber-attack to this server.*
- *An attack from a third-party vendor system used by Brand New Day (a Medicare-approved health plan) caused potential breach of 14,000 patients' information including names, addresses, phone numbers, dates of birth and Medicare ID numbers of members.*

HIPAA

What is HIPAA take on 3rd Party Vendors

Many healthcare providers and health plans (covered entities) know the consequences of not following guidelines set by HIPAA rules and they try to comply it as much as possible. However, some overlook that their third parties (business associates, partners, subcontractors) should also meet HIPAA regulations.

As an example, patients' data is given to a research company (business associate) and the research company uses data-management firm for data storage (subcontractor). Both research company as business associate and data-management firm as subcontractor have to abide HIPAA rules.

Ground rules for 3rd party management with HIPAA

- *Business associates of covered entities must comply with the applicable requirements*
- *Require modifications to, and redistribution of, a covered entity's notice of privacy practices*
- *Strengthen the limitations on the use and disclosure of protected health information for marketing and fundraising purposes, and prohibit the sale of protected health information without individual authorization*
- *Expand individuals' rights to receive electronic copies of their health information and to restrict disclosures to a health plan concerning treatment for which the individual has paid in full.*
- *A covered entity can disclose protected health information (PHI) to a business associate under a written contract with certain assurances to comply certain parts of the rule. Similar goes for subcontractor that business associate work with and have access to PHI data.*

COBIT

COBIT (Control Objectives for Information and Related Technologies) created by ISACA is an integrator framework many IT standards such as ISO 27001, COSO, ITIL, etc. It summarizes the key objectives of these guidance materials. Since the first version released in 1996, COBIT is well-accepted by an international material for enterprise IT management and governance with framework, process descriptions, control objectives, management guidelines, and maturity models provided.

Since its release in 2012, COBIT 5 has become a good-practice framework for IT management and governance for enterprises. By following certain checkpoints in the framework, a company can create a good IT risk management.

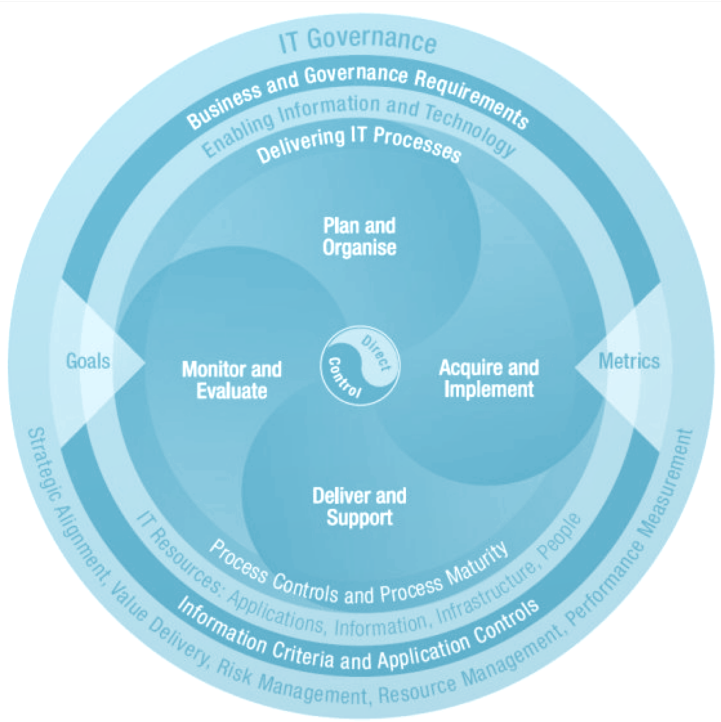


**Image adopted from isaca.org*

COBIT

What is COBIT's View on Third-Party Risk?

One of the main section in COBIT checkpoints is Delivery and Support (DS) where the second subsection (DS2) is all about how to manage third-party services. Here, third parties are defined as suppliers, vendors and partners. COBIT claims that control over the IT process of managing third parties can be achieved by:

- *Identifying and categorizing supplier services*
- *Identifying and mitigating supplier risk*
- *Monitoring and measuring supplier performance and measured by;*
  - *Number of user complaints due to contracted services*
  - *Percent of major suppliers meeting clearly defined requirements and service levels*
  - *Percent of major suppliers subject to monitoring*

COBIT explains details how to manage third party relationships in DS section under four categories:

1. *Identification of all supplier relationships*
2. *Supplier relationship management*
3. *Supplier risk management*
4. *Supplier performance monitoring*

Steps for COBIT compliance of third parties

- *Establish agreements with third parties. Agreements should be written clearly and should have references to COBIT.*
- *Check COBIT control points and determine which one of those should be met by the third party.*
- *Monitor compliance of the third-party*
- *Prior to work with a third party, complete a risk assessment*

NORMSHIELD'S COMPLIANCE CHECK

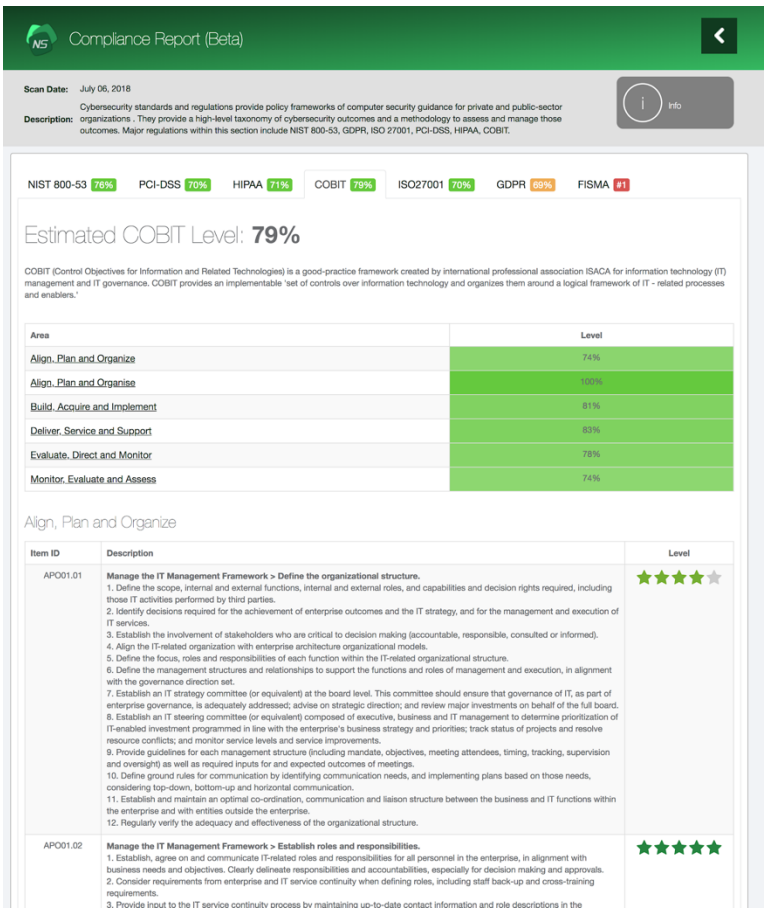
All the regulations recommend to monitor third party vendors and conduct a risk assessment for them. The risk assessment can be done in an old-school fashion questionnaire method. Unfortunately, some third-parties are not so eager to respond, questions might not cover all the risks, and the answers will be only depending on what the third-party knows about it IT structure.

Thus, NormShield Cyber Risk Scorecard, with its benchmarking reports, provides risk scoring and ranking for companies and their third parties. It also checks compliance to well-known cyber security frameworks including NIST 800-53, PCI-DSS, HIPAA, COBIT, ISO 27001, GDPR, and FISMA. Even prior to work with a third party, its compliance to these regulations can easily be checked with NormShield Cyber Risk Scorecard.

NORMSHIELD'S COMPLIANCE CHECK

How It Works

NormShield classifies the findings into FISMA Cyber Security Framework Area and Maturity Level, NIST 800-53 Control Family, FIPS-200 Area, NIST 800-37 Process Step. The classification allows to approximately predict the compliance level of the target company in terms of different regulations including NIST 800-53, FISMA, ISO27001, PCI-DSS, HIPAA and GDPR. The prediction is not a replacement of regular compliance assessment but it is a very good baseline to start working on it. NormShield's shared responsibility platform also allows user to update the compliance level of their organization after the estimated level.



NormShield has a unique feature of **cross correlation** between different regulations. If a company is compliant to one regulation, our proprietary algorithm can estimate the compliance level of other regulations.

ABOUT NORMSHIELD

We provide Cyber Risk Scorecard for companies just like FICO score. Cyber security is on every Board's agenda, and the average total cost of a data breach has risen to $4 million (Ponemon/IBM).

NormShield Cyber Risk Scorecards provide the information necessary to protect business from cyber-attacks.

The scorecards provide a letter grade and a drill down into the data for each risk category so that remediation of vulnerabilities can be prioritized. Unified Threat & Vulnerability Orchestration Platform and Cyber Risk Scorecard.

www.normshield.com
1 (571) 335 02 22
info@normshield.com

NormShield HQ
8200 Greensboro Drive
Suite 900

To learn your company's risk score, visit
https://www.normshield.com/