IT Security and Compliance, what is the difference and how to deal with it

Marcel de Haan

DHDA

Apeldoorn, The Netherlands

22 June 2020

Version: 3.0

Table of contents

1. Summary

IT Compliance and IT Security are not always approached as different challenges within companies. In case of a major issue, being a regulator report or a security incident, the standard response is: “Get this resolved as soon as possible”.

Insiders know security is not a short term challenge but a long term process of embedding in first line management activities, and although from a content perspective Compliance and Security deal with the same subject, they have different motives, usually issues have a different impact and with different stakeholders.

This paper will provide a pragmatic approach to manage Compliance and Security issues, explaining how organisations can be helped within in the short term, however, ensuring a foundation to gain maturity for the long run. It addresses how to embed change management into the security strategy. This approach will satisfy multiple stakeholders at once; including regulators and supervising bodies.

Although this might sound as an open door this paper distils the following approach with some detailing that causes significant output. Plan for an assessment and find out your specific challenges. Depending on the results consider the following:

1. The short term plan should be focussed on the quick fixes and expect these to be temporary, in spite of the attempt to achieve sustainability.
2. The short actions related to compliance and to security should be separately managed.
3. Ensure the foundation for the long term objectives within the short term plan:
    a. Governance:
        i. Ensure strong anchoring of board support. Not only a tap on the shoulder and good luck wishes. SMART commitment for both long-short term plan of actions.

ii. Ensure the security organisation is defined and start the hiring process with people that fully own their profession

iii. Ensure an up to date Information Security Policy is in place. Supported by management and involvement of the supervising bodies or even regulators. Taking them along the innovative journey delivers goodwill during the execution [1].

b. Planning:

i. Ensure key security measures (Identity and Access Management (IAM), Infrastructure security and monitoring, Security Incident Management) are part of the IT planning and budgets should be in place.

ii. Ensure Security by Design is part of the IT planning and real time security, control and administration tooling.

c. Reporting and follow up:

i. Ensure the Information Security Dashboard is put in place, which can be improved and optimized over time with real time feeds. This is a key instrument for managing effectiveness, being in control of Digital Security and continuous improvement.

2. Introduction

Security used to be mainly IT oriented, evolved into Information security, and controls mostly being managed and tested with use of Excel sheets. Frameworks expanded to other disciplines like information security governance to support the world of digital security and auditors [2]. Information Security should become a strategic subject and regarded as a process which requires continuous improvement [3]. The better term to use is Digital Security, which includes all data, applications and infrastructure security.

Although from content perspective IT Compliance and Security (or Digital Security) should be the same, the chance to be non-compliant is higher, however the impact of a security issue is usually many times higher. For this reason the approach to improve compliance is expected to be different.

Digital Security

In 2008 security was mainly IT-oriented and the main focus was on using IT controls to mitigate or detect security vulnerabilities. Research has shown that the number of IT security incidents has increased over the years, as has the financial impact per data breach [4].

In 2009, an average of 25% of EU organisations experienced a data breach [5]. Mastering emerging technologies such as big data, Internet of Things, social media and combating cybercrime [6], while protecting critical business data, requires a team instead of a single IT person. To protect this data, security professionals need to know about the value of information and the impact if it is threatened [1]. IT risk management requires different capabilities, knowledge and expertise from the skills of IT security professionals [7]. Hubbard [7] refers to the failure of ‘expert knowledge’ in

impact estimations and to the importance of experience beyond risk and IT security, such as collaboration and reflection.

In the past [8] IT security controls were implemented based on best practices prescribed by vendors, without a direct link to risks or business objectives [8]. These controls depended on technology and the audits and assessments (in spreadsheets) were used to prove their effectiveness [9]. The problem with this approach lay in the limitations of mainly IT-focused security and security experts working in silos with limited, subjective views of the world [10]. This is important, as information security is subject to many different interpretations, meanings and viewpoints [3].

The state of security in 2010 shifted towards 'information security'. ISO specifies information security as *"protecting information assets from a wide range of threats in order to ensure business continuity, minimise business risk and maximise return on investment and business opportunities"* [11]. Its core principles are Confidentiality, Integrity and Availability (CIA) [11]. Later non-repudiation and auditability were added to comply with audit and compliance regulations. Thus Information Security should ensure a certain level of system quality and assurance [12].

The scope of Information Security was then expanded to other disciplines in the enterprise since digital became more and more common in our way of doing business. In their book 'Information Security Governance', Von Solms and Von Solms describe the growing number of disciplines involved in IS [15]. By 2011 IT managers and IT security managers were increasingly urged to engage with business to determine risk appetite and the desired state of security. In 2005 ITGI proposed to co-develop IS together with the business [1].

Control frameworks should serve two worlds:

- The world Digital security (fka IT security, then Information Security and sometimes Cybersecurity)

- The world of IT Audit and Assurance

These frameworks are used with multiple objectives by multiple people with personal perspectives and agenda's not always serving the collective goals. Sometime implementing the framework becomes the objective rather than keeping the company save or the regulator happy.

Information Security frameworks have involved over time.

- Since 2011, the role of culture [3], awareness [16], compliance [17] and knowledge sharing [10] has also been included in security strategy frameworks [18].
- Due to research on IT governance at the Antwerp Management School (AMS) [19], relational mechanisms such as culture, behaviour and knowledge were incorporated in the COBIT 5 Information Security Framework [20] in 2012. In this framework the distinction between governance (strategic level), management and operations was made.
- Basie and Rossouw von Solms [21] differentiate between three levels: the strategic level (Board of Directors and Executive Management), the tactical level (senior and middle management) and the operational level (lower management and administration). All directive setting and controlling (including monitoring and evaluating) is seen as part of the strategic level of governance [21]. An example is the adoption of Information Security Control Frameworks such as the Information Security Forum (ISF) Standard of Good Practice and COBIT2019. Dialogues at these three organisational levels are most of the time different. [22]

The picture underneath explains the need for a framework as the foundation for the Information Security Assurance process.

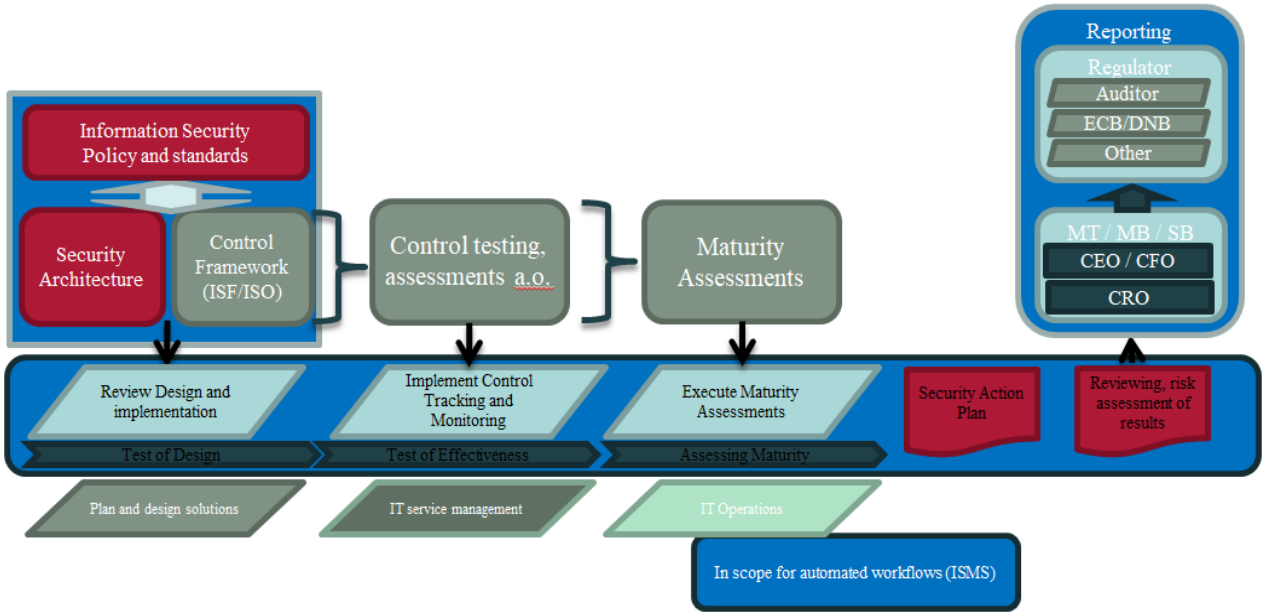


Figure 1 Information Security Assurance process (Marcel de Haan)

The paper "What do we know about information security governance?" by Stef Schinagl and Abbas Shahim, d.d. 20 October 2019, states: "… security has shifted from a narrow-IT-focused isolated issue towards a strategic business issue with "from the basement to the boardroom" implications." and that "… organizations must also develop strategies, mindsets and tone at the top to ensure resilient businesses to take advantage of the opportunities that digitalization can bring." Experience shows that both larger and smaller businesses, often do not view security as a subject that deserves a strategy [23]. While companies that do this can make a leap forward and actually have better results[1].

In 2007 Harvard professors Hunter and Westerman examined companies that treated risk management as a continuous improvement process and revealed the fact that those who did were

[1] In 2015 Ponemon and Accenture suggest in their research publication *The Cyber Security Leap: From Laggard to Leader* [61] that companies that address BIS as a strategic topic perform better and can 'leapfrog' others. [1] A total of 247 companies participated in this study, which was performed by Accenture in collaboration with Ponemon Institute.

perceived to have higher value [24]. Gordon et al. [25] examined companies which are open to voluntary disclosures concerning information security and publicly accept feedback on their security investments and activities. Here, too, there was an increase in company value [26]. A similar effect was shown in Japan [27], on the effects of information security incidents on corporate values in the Japanese Stock Market. In 2011 Shackelford [28] quotes; *"over 90% of respondents to a survey by the Ponemon Institute* [29] *reported experiencing a cyber-attack during the last year, costing on average more than $2 million per organisation. Such attacks have been shown to negatively impact the stock prices of targeted firms* [28].

Digital security is a more comprehensive and overarching term that covers the information security, IT security and cybersecurity domain, in relation to all assets, data, applications and infrastructure.

- Information security concerns security of all information, physical and digital and usually referring to actions within a company.
- Cyber security is a more recently used term referring to security related to cyber-attacks, the dark web, and the deep web, etc., (Business).
- IT security refers to security related to automated process of data, towards both internal as external threats.

IT management has a wider scope, like business (and data) processes and data management have a wider scope.

IT Compliance versus Security

Although from a content perspective Compliance and Security is all about the same subject Digital Security there are differences.

IT Security:

- Is practiced based upon the company's objectives
- Is driven by the need to protect against constant threats and should be continuously maintained and improved to deal with these threats
- Focussed on threats, vulnerabilities (risks) and controls
- Learn from a hacker

IT Compliance:

- To meet external requirements and facilitate business operations.
- Is driven by business needs and ready when any third party is satisfied
- Focussed on laws, regulations and policies
- Learn from an auditor

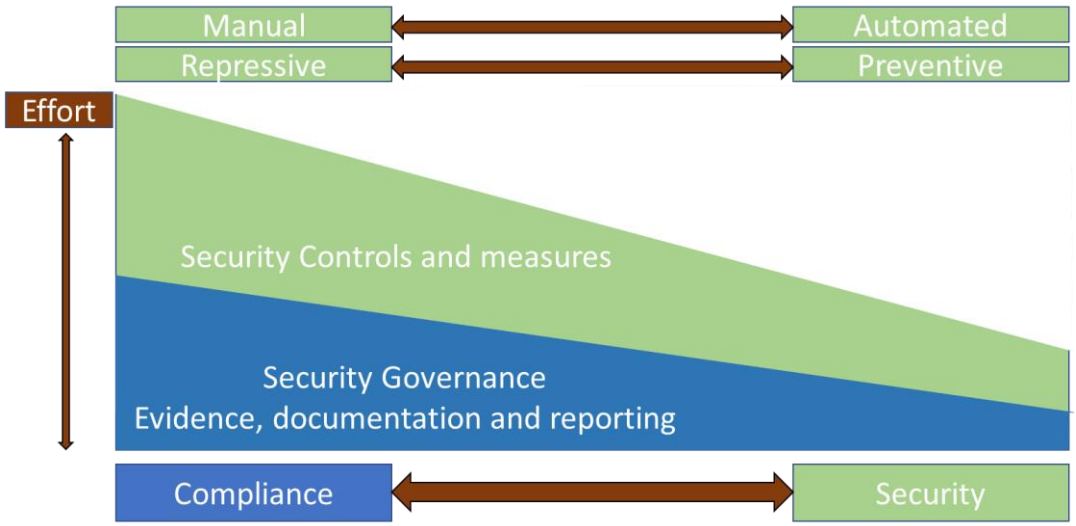


Figure 2 Shift of focus moving from Compliance to Security (Marcel de Haan)

When shifting the focus from Compliance to Security, with a solid foundation, the controls become more efficient, more preventive and automated. As a result the effort required for evidencing, documentation and reporting becomes more automated and efficient. A potential 70% saving is achievable.

Although the chance of not being compliant may be higher than being hacked, the impact of being hacked is much higher and could be devastating for a company. Recent history has already proven that, as explained in this ransomware article.

When the company solely focusses on getting the compliance report passed it might be tricked due to the wrong focus. Target [30] [31], Equifax [32] and Diginotar [33] [34]cases demonstrate us that passing the audit did not prevent from a large hack that led to board layoffs and personal prosecution [35] [32]

With a single focus on both IT Compliance and Security (in the long run) a business will be empowered to not only meet the standards, but also demonstrate that it goes above and beyond in its strategic objectives regarding security. However, a company needs to be mature within Information Security to be able to take this approach; a catch-22.

Background

Security or compliance issues are: “a nuisance, and need to be dealt with as quickly as possible”, to ensure regulators are losing interest in the company and the focus can remain on the sales. In case of an issue, a first regulator report or a (number of) security incident(s), companies tend to fix the issues completely led by the regulator or the incident, with the explanation that the company wants to be secure and as a result often mixing up the compliance and security issue. This usually results in postponing the inevitable, because likely nothing will be “really” fixed. The

regulator will return and come up with even a more disastrous audit and report or a real security incident will take place.

From the company's perspective this is a logical point of view. The history of these companies, the maturity level, the reasons for their success, the healthy financial situation all contribute to this behaviour, stick to the known strategy and the reasons for success. A company can be driven by quarterly or yearly numbers. The sense of urgency is missing, even an aggressive business change strategy, like "we must go digital" is not reason enough, ….. until it goes terribly wrong.

By now most companies have hired a CISO or organised a similar role, however in general the CISO is mostly dealing with daily challenges we refer to as "the shit of yesterday", and not with realising an longer term strategy to make the company really resilient [2].

To be successful the security team should focus on the long term. Of course, the issues and auditor's findings of yesterday are important, but to change and improve, focus on the future. As described by Hinssen,[2] we should focus on the "The Day After Tomorrow" which creates long-term value instead of focusing on the "Shit Of Yesterday" which actually only creates negative value. The following figure shows that we spend most of our time on today and things that went wrong yesterday, while the most value can be gained by focusing our time and energy on tomorrow and even better still the day after tomorrow.

---

[2] Peter Hinssen, The Day after Tomorrow: How to Survive in Times of Radical Innovation, 2017

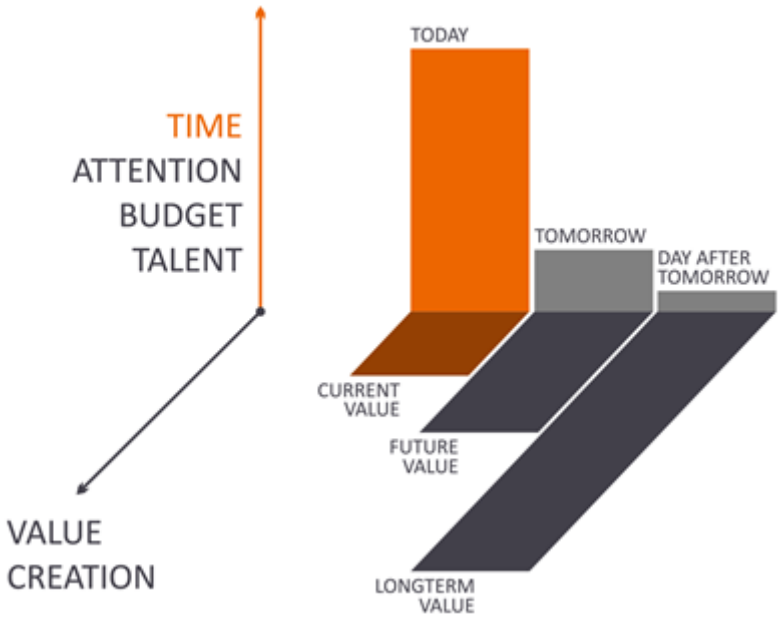


Figure 3 Managing the Shit of Yesterday (taken from Hinssen, The Day after Tomorrow)

Approach

Knowing the above mentioned challenges we have distilled a central question we want to answer with a suitable approach;

How can company's be supported dealing with these different challenges, lacking the experience and maturity regarding IT Security and Compliance, maybe not realising how big of a challenge they have, with one approach?

Whatever the trigger for taking action may be, the general approach is always the same, you may recognise the PDCA [36]cycle and its associated PDSA cycle for continuous learning. Continuous improvement, as part of Total Quality Management [49], is established by executing this PDCA cycle numerous times and studying interventions, in order to understand their effectiveness during the maturing process. Edward Deming [36][1] refers to this learning element as the PDSA cycle, a Plan-Do-Study-Act [48] cycle, which builds deductive and inductive learning into learning and improvement.

a. Understand the company

Objectives and the reasons why a company is moving and behaving as it is.

b. Asses and measure and determine the real IT Security “problems”

   Based upon “a” framework, and conclude the key risks and issues. This might seem difficult but in practice is quite simple with help of technical validation tools. They immediately present flaws in the environment which can be translated into “low hanging fruit for the CISO”

c. Define an improvement plan in stages with different objectives

   Content depends on both the assessment results and the reason for triggering this action, being a security incident or a third party report.

d. Implement the improvement plan and frequently measure and report via a clear dashboard

   Status and results of the improvement plan and status or “maturity” of IT security. Bobbert presents the top ingredients for such a dashboard and underlying administrative tool collected from multiple C-level executives. [37] In later studies he added real time technology monitoring criteria, that reflect the complete “Fitness” state of the environment to this [38].

3. How do companies tend to approach a compliance or security issue?

Familiar statements are:

"With solving the issues as reported by the regulator, we will gain trust and they will not give us more attention."

"Let's get them off our back asap and only do what they ask us, nothing more and nothing less."

"With solving the issues as reported by the regulator, we will solve the key risks and we will be secure enough. And at the same time, because we as an organisation want to be secure, we meet our business objectives and remain within the risk appetite."

"When we will solve the (technical) issues concerning certain security incidents, we will manage the risks and we will be secure enough."

The situation will be very different between companies, even between industries. Media show on a daily basis what is happening worldwide, how ill prepared companies are, how the industries are driven by different objectives, how more and more IT dependent companies are and how cyber criminality is being organised and is an industry on its own. Fact is that many companies, small and large, in all different industries are dealing with this cyber security challenge.

Being in control is more important than the quantity of documentation

Experience shows that when a company can present a well-defined improvement strategy and plan, more trust will be gained with the regulator. But regulators, understanding the lack of maturity, very much like the action plan approach with deadlines and progress reports focussing on short term success. The best way to approach this is, before giving any promises: Think first, ensure you have all facts in place and then present the plan with a short *and* long term in mind. Not meeting all deadlines is not as bad as not showing you are in control. Provide early notice, describe the reasons and impact and reschedule.

Well-defined and executed 3 lines of defence is conditional

Prepare any communication with a regulator, ensure independent (second line) compliance management internally and separate this from (first line business and IT) security, but ensure both take their full responsibility. First line is responsible, defines and reports, compliancy is managing proper communication with regulators. Clear charters to describe the separation of lines of defence and functions substantiate the trust.

The **first line** of defence has line management oversight and is mainly the IT operations function and the “business”. This first line implements the policies and standards and is responsible for monitoring of the networks and infrastructure. The first line is also responsible for the workforce awareness and behaviour. The first line has process controls in place (e.g. encryption, anti- malware, data leakage prevention) and mechanisms in place to test the effectiveness of the controls (e.g. least privileged, segregation of duties etc.).

In the **second line** of defence the CISO Office, according to Forrester [39], is responsible for governing those tasks and ensuring that the appropriate monitoring, reporting, and tracking of

key controls is being performed by IT operations. In this second line also risk management, financial control, quality management, compliance, threat intelligence and brand monitoring is taking place. This second line reports to the board or senior management.

Since the role of the CISO is becoming increasingly important to IT enabled companies the IIA states; *"The board must ensure that the CISO is reporting at the appropriate levels within the organisation. Keep in mind that, although many CISOs continue to report within the IT organisation, sometimes the agenda of the chief information officer (CIO) is in conflict with that of the CISO. As such, the trend has been to migrate reporting lines to other officers, including the general counsel, the chief operating officer (COO), the chief risk officer (CRO), or even the chief executive officer (CEO), depending on the industry and the organisation's dependency on technology* [40].

Finally the **third line** of defence, internal audit, reviews the first and second line to ensure that the controls are effective, have suitable coverage, are deployed consistently and are proofed with evidence. So the external auditor and regulators can perform their external duties. Recently the IIA and COSO collaborated into a examining the main principles to consider for the CISO when navigating between the first, second and third line of defence.

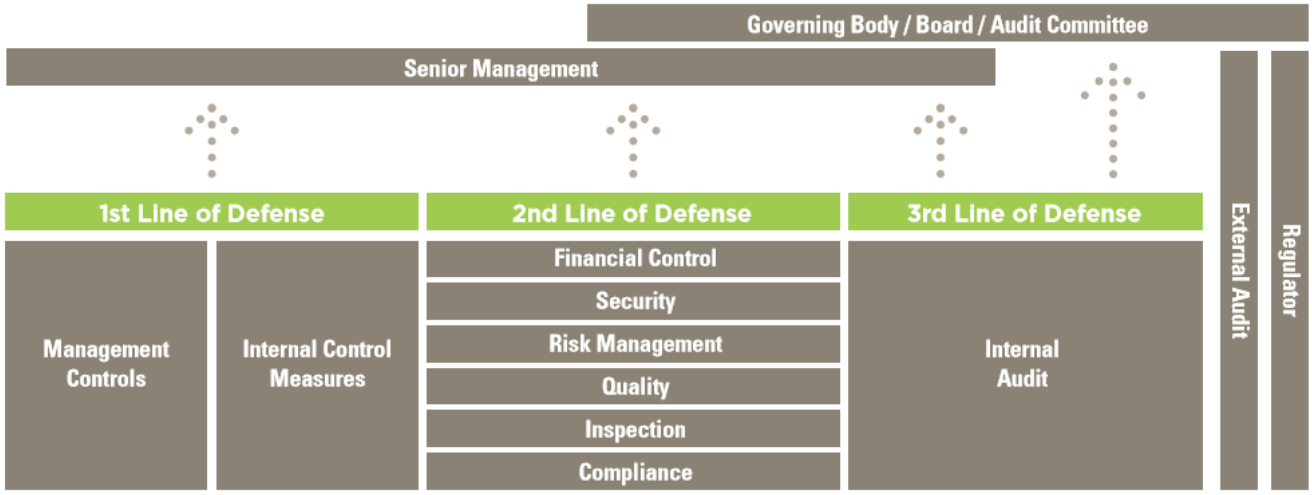


Figure 4: Three lines of defence concept taken from the IIA report from 2013 [40].

Documentation and evidence process can block actual fixing

In case a single improvement project is defined driven by a compliance issue, the documentation process usually absorbs all capacity and budget. Solving the actual issue is in reality not the prime objective (anymore). For this reason make sure the improvement project plans for both activities specifically and separately.

Short term fixes are usually not reusable

Although, companies would like to put quick fixes in place which are reusable, accept the fact that not more than 20% of the fixes is reusable. Quick fixes are usually focussed on technical issues and cleansing activities, with the objective to reduce as much risk as possible. Without a clear policy, standards, security architecture and processes (controls within processes), based on a carefully considered risk appetite (the agreed level of risk and related costs, the business is willing to consider), it will not possible to implement sustainable solutions.

For example revoking high privileged accounts. After cleansing creation of new privileged accounts needs to be checked frequently (usually a manual process), proving “effectiveness” of the control. What control is being tested, a regular cleansing activity? These checks are time consuming and prone to error and building up the workload. Management of privileged accounts for system management teams cannot be cleansed just like that. How to manage an admin account on hundreds or thousands of on premise servers or hosts? This cannot be solved quickly.

The long term approach will be standards (rules around privileged accounts), improved change and access management processes, embedded controls with automated support based, on a security architecture to avoid any security GAPs. The design will be based upon business requirements and considering the business Risk Appetite

4. What approach should companies take?

Although Compliance and Security are different, the "Approach" to deal with these challenges are the same. However,

a. The type of assessment may differ
b. The content of the actions within the "short term" improvement plan will partly differ

Compliance and security are different risks

From a contents perspective, IT Compliance and Security should be pretty much the same problem. However these are very different challenges due to different motives.

Compliance concerns meeting requirements of a third party, such as a government, security framework, or client's contractual terms.

- If an organization wants to do business in a country with strict privacy laws, or in a heavily-regulated market like healthcare or finance, or with a client that has high confidentiality standards, they must play by the rules and bring their security up to the required level.
- Although more mature organisations move towards "internal" compliance towards its internal standards based on internal motivations.
- In case of a nasty regulator report the boardroom starts to get worried about reputation and even career and personal impact [40]. Then compliance becomes a material issue.
- The pressure of ensuring compliance also tends to impact behaviour within a company. Personal impact and stress due to whatever fear triggers primary reactions, personal agendas and pushing short term improvements. This kind of behaviour usually results in windows dressing and not in actually solving security issues.

Security is the practice of exercising due diligence and due care to protect the confidentiality, integrity, and availability of critical business data (and support applications and infrastructure).

- Security is a subject which tends to be avoided. It is not well understood, complicated and being regarded as a real burden holding up real needs like new functionality, or budget for new functionality and marketing.
- The company is no longer agile and the change process is being stretched and an agonizing process of checks and balances. It works against DevOps and CI/CD (Continuous Improvement/Continuous Development). Every excuse is being used to avoid time wasted on this subject: “it is only unnecessary documentation, that is not agile”.

The impact of **Compliance and Security risks** can be quite different. A hack tends to be less likely, especially with the vast increase of laws and rules. But, not always very well understood, one leads to the other, they are not independent of each other.

- Failing an audit, being non-compliant, will endanger the license to operate, will put pressure on the Supervisory Board and board members are personally liable and at risk of being dismissed.
- A hack may result in a high cost, potentially bankruptcy, public exposure, losing customers or customer trust and potentially questions on political level.

Each organisation experiences a different learning process based on stressors (Nassim Taleb[3]). In general first a real issue needs to happen first before action is being taken, and these reactions may differ depending on the incident.

[3] "Antifragile" is when something is actually strengthened by the knocks. - Nassim Taleb

- APM terminals suffered from a security incident and suffered from the results. As a result in a short period of time all funds were available to really solve the issues and improve Cyber Defence. The reaction: solve the Security Issues.
- Delta Lloyd suffered in 2015 from DNB audits which resulted in a huge fine and the dismissal of a number of managers. The reaction: “Heavily improve the Risk Management process”. This very much centralised Risk Management process did result in a lot more evidence and reporting, but did not necessarily resulted in the required improved security and skill levels within the first line of defence.

Short and long term approach for IT Compliance and Security

It’s a misconception that with making sure a regulator is “happy” the company has solved the compliance risk. Regulators also grow in maturity and are actually focused on the contents. The number of rules and regulations will only increase and the required “evidence” becomes more intense. The TIBER.[4] program of the DNB (forcing companies to perform a red-teaming hack-simulation, reporting the results to the DNB) is a good example how a regulator wants to have “real” prove of the level of security and test the responsiveness to cyber-attacks.

Conclusion: Compliance is NOT just a short term challenge, but is a process which needs to be managed. However, with both “short term fixes” and a long term preventive approach it is possible to provide a more sustainable digital assurance.

When solving “a” cybersecurity incident, the solution tends to remain on a technical level, without proper root cause analysis. In case of a real security issue such as the DDOS attacks at ING in 2013 [41] , the boardroom immediately understands the strategic importance of IT security, no resources are spared to solve the problems. When the maturity lacks regarding governance, organisation and IT security processes, a company will not be able to stay on top of the security challenge and one day will become a victim of a dramatic security incident (again).

Conclusion: IT Security is NOT just a short term challenge, but is a process which needs need to be managed in the first line of the managers responsibility, similar like quality. However, with both “short term fixes” and a long term approach for sustainable solutions.

In the visual below Schninagl and Shahim reflect the traditional IT security Governance compared to the future Digital Security. [42]

---

[4] The Governing Council of the European Central Bank (ECB) has decided to set up TIBER-EU to increase the cyber-resilience of market infrastructures and financial institutions throughout Europe. TIBER: Threat Intelligence Based Ethical Red Teaming.

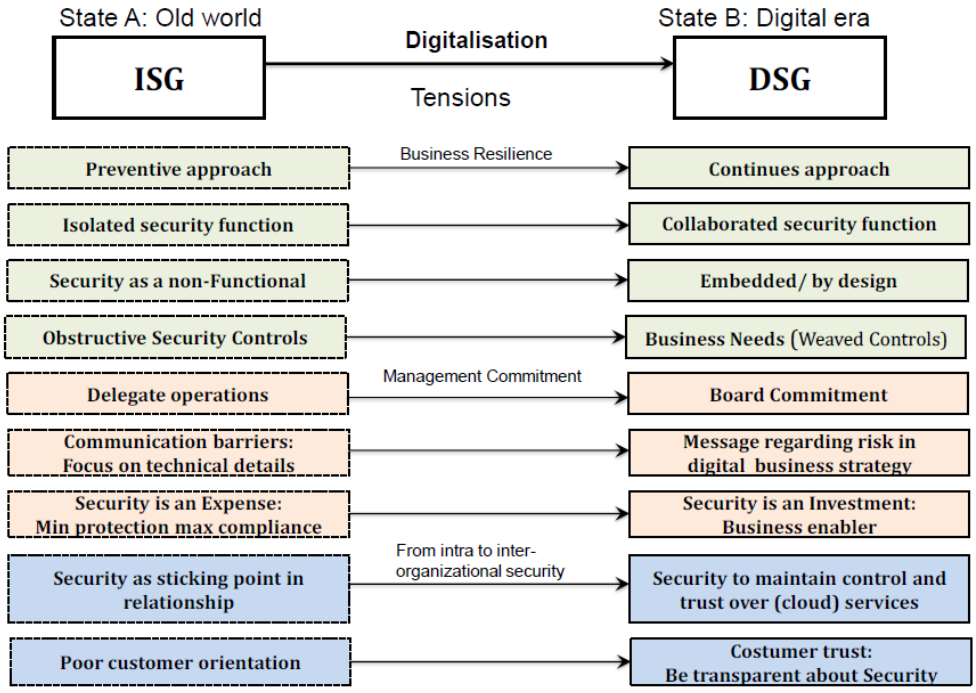


Figure 5 From IT Security Governance to Digital Security as strategic boardroom topic Taken from Schninagl and Shahim (2019)

Supportive tooling

The key to ensure compliance (towards internal and/or external requirements), besides in the basics solving security challenges, is the required evidencing. Companies have to prove they are compliant, prove definition, existence, effectiveness and even in certain areas continuous improvement. In the short run for specific areas of attention it would be possible to perform "control testing" (to prove effectiveness), manually and with use of MS Office tools. However the burden of this process will increase exponentially, and not only for the testers, but also on the first line operations, who need to provide evidence over and over again.

The solution for this is automation, Information Security Management Systems (ISMS). There are many tools on the market which will help with the following.

- Workflow management, automate the testing process, ensuring test requirements are being met.

- Storage of evidence, a single location in which one version of the truth is being collected and readily available.
- Reporting, with the availability of the different frameworks with cross mapping, it is possible to provide any report for any stakeholder, with the same truth, with a push of the button.

The principle being supported here is **"Test once, Comply many".** Organisations tend to be in reactive mode. When a regulator or customer wants prove or a report, testing starts, everybody starts running, a different shared drive is being defined and all evidence is being collected again, which likely was already available. But the required framework is just slightly different.

The ultimate maturity within this process is the automated collection of evidence, when the ISMS tool is being connected to the underlying systems, usually IT systems tooling and security tooling. At that moment it would be possible to real-time report on security and controls.

Short versus long term approach

The table underneath shows the differences between the long term and short term approach. Only when taking the long term approach an organisation can truly get "in control" (efficiently) of both Information Security and Compliance. However, usually the focus is ONLY on the short term approach.

#	Action	Short term approach	Long term approach
1	Define company objectives	Year planning both business and IT, project portfolio.	Mission, vision and business and IT strategy, risk appetite, policies and enterprise architecture
2	Assess and measure	a. Quick assessment (1 month) b. Full assessment (2 months) c. External Pentest (3 months)	a. Audit (3 – 4 months) b. Certification (6 – 12 months)
3	Conclusion	a. Compliance risks b. Security risks, often concerns User Access management, network security and monitoring, change	a. Root causes of identified issues (governance, ownership, architecture, automation) b. Long term maturity level (effectiveness, automation,

#	Action	Short term approach	Long term approach
		management and Resilience	metrics)
4	Define improvement plan	a. 3 to 12 months period, partly **short term quick fixes** to mitigate key risks and issues. b. **Separate** the compliance from the security part of the plan. Requires different (project) management	a. 12 – 24 months full scope definition and design of controls in all control areas b. 12 – 36 months prove effectiveness of all controls
5	Execute improvement plan	Temporary resources, with owners within the business (both IT and business departments)	Within line organisation managing security and compliance as daily business
6	Measure and report (refer to # 2)	a. Improvement plan progress b. Start with Information Security Dashboard for CISO	c. Yearly maturity assessments d. Yearly testing (e.g. pentest, red teaming)

Figure 6 Short term versus long term approach (Marcel de Haan)

The short term “fixes”, also known as “low hanging fruit” or “no regret moves”:

a. should be risk driven (could be a Compliance and or a Security risk);

   Risks should be categorised in critical, high, medium and low. The improvements which reduces the highest risks will get priority.

b. not requiring architecture, however ensure no future blockades;

c. will be only for the short term and usually replaced in the longer run;

   Referring to examples as provided before, manual checks and balances or improvements within processes will be replaced with better, potentially automated solutions in the long run).

d. compliance actions should be fully separated from security improvement actions, but completely lined up in the improvement plan.

5. Conclusion

Final statement

Compliance and Security are different risks with different motives and a different impact, based on the same content. Resolving Compliance and Security issues require some different actions in the short term and a similar long term approach. The pragmatic challenge remains, in reality C-level executives (a Boardroom) tend to be focussed on the short term. How to deal with this?

Seek support for the following steps:

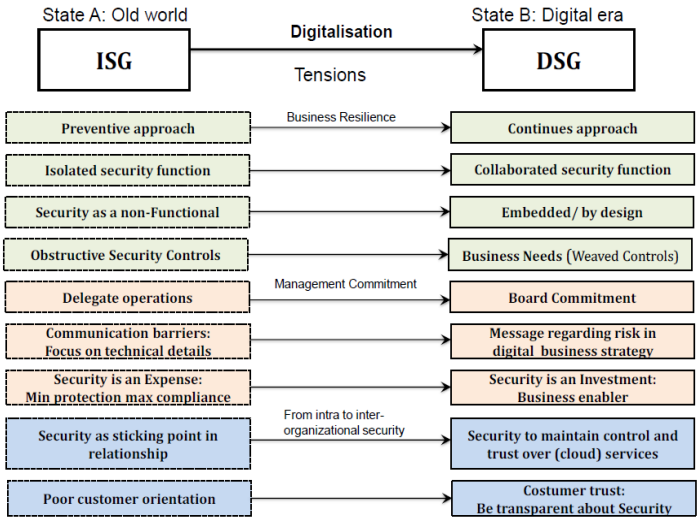
1. Performing different types of **assessments**, based on different frameworks, defining the conclusions and presenting the results.
2. Development of an **improvement plan** with short term fixes to reduce risks as fast as possible, but including preparation (building the foundation) for the long term improvements.
3. **Implementation** solutions in short term and with building the foundation for the long term. This may concern finding the most adequate solutions for improvements, developing policies and standards, defining processes, building up and filling in the organisation, implementing technical solutions and selecting the partners, but also defining control registers and implementing an ISMS tool.
4. **Defining progress reporting**; this concerns the Information Risk and Security reporting, which concerns not only the progress on the improvement plan, but also the results of assessments, tests, audits, identified risks and security incidents.

Prepare for the long term within the short term approach

The next table provides guidance what can be done within the first year to ensure the organisation is prepared for achieving long term objectives. As part of the short term approach incorporate **preparation** for the long term approach. Make the organisation a self-sustaining entity for both Security and Compliance. The Dashboard will show Security, Risk and Compliance challenges.

#	Action	Long term preparation within the short term action plan
1	Define company objectives	a. Identify the mission, vision, strategy, key objectives, values and success factors of the company. b. Define or update the **Information Security Policy** c. Ensure **Security Architecture** (specifically considering hybrid cloud solutions) is on the agenda of the Architecture team. d. Start with an initial set up of **standards** (reuse what is available)
2	Assess and measure	a. Adapt and agree **the audit plan** with the audit staff, aligned with the long term improvement objectives b. Define **certification objectives** if required
3	Conclusion	a. Identify the **missing building blocks** for the long term objectives. Usually the governance challenges (people, process, organisation, architecture and budget)
4	Define improvement plan	a. Ensure the **Security Organisation**, Determine the in house and outsourced services and start the hiring process of resources (Security Architect, CISO, Security Operations and Internal Control) and providers. b. Ensure **key IT Security projects** within the IT strategy (e.g. User Access Management solution, Network security and monitoring solutions, Security Incident Management, Threat Intelligence) c. Specifically ensure within the IT planning **automation for controls** and controls testing (ISMS and/or GRC tooling, real-time) d. Ensure the **Sourcing contracts** with the Sourcing department are in control or agree improvements with the Sourcing department
5	Execute improvement plan	a. Ensure the line organisation (CISO and IT / Systems Management and Security operations) have planned for improvement activities (**change budget**), for next year
6	Measure and report	a. Ensure CISO owns **the Information Security Dashboard** for Security, Risk and Compliance b. **Assessment Plan** for yearly maturity assessments c. **Test Plan** for yearly testing (e.g. pentest, red teaming)

Figure 7 Long term preparation within short term approach (Marcel de Haan)



Samples of measurements

- Annual improvement plans, security calendar
- Governance; Risk CISO, Security Operations
- Business Impact Analysis, Agile, training plan
- Risk Governance, Security Board
- Security Board, approvals, risk priorities
- Frequent information security reporting
- Business Case
- (Cloud) Security Framework, control register
- In control statements

Figure 8 From IT Security Governance to Digital Security as strategic boardroom topic Taken from Schninagl and Shahim (2019) – with practical examples of measurements

A final message. When a company does fully focus on IT security, compliance is not being forgotten. Risk and Compliance are fully integrated, however components, of organising and implementing Security. Although sometimes for good reasons short term fixes are necessary which can be fully focussed on compliance, with a decent foundation designing and implementing sustainable controls and solutions, risk and compliance will become much more embedded, part of te design (security as a design) and as a result much more efficient.

Citations

[1] ITGI, Information Risks; Who's Business are they?, United States: IT Governance Institute, 2005.

[2] Y. B. M. Bobbert, Leading in Digital Security_Twelve ways to combat the silent enemy, Utrecht, 2020.

[3] J. Van Niekerk and R. Von Solms, “Information security culture; A management perspective,” *Elsevier,* pp. 476-486, 2010.

[4] Ponemon, “Cost of Data Breach Study: Global Analysis,” Ponemon Institute LLC, United States, 2016.

[5] Ponemon Institute, "Business Case for Data Protection," Ponemon Institute LLC, 2009.

[6] B. Cashell, W. Jackson, M. Jickling and B. Webel, "The Economic Impact of Cyber-Attacks," Congressional Research Service, The Library of Congress, United States, 2004.

[7] D. Hubbard, The Failure of Risk Management, Hoboken New Jersey: John Wiley & Sons, 2009.

[8] W. Yaokumah and S. Brown, “An Empirical Examination of the relationship between Information Security / Business strategic alignment and Information Security Governance,” *Journal of Business Systems, Governance and Ethics ,* vol. 2, no. 9, pp. 50-65, 2014.

[9] D. Zitting, “Are You Still Auditing in Excel?,” Sarbanes Oxley Compliance Journal, 2015. [Online]. Available: http://www.s-ox.com/dsp_getFeaturesDetails.cfm?CID=4156.

[10 W. Flores, E. Antonsen and M. Ekstedt, "Information security knowledge sharing in organizations: Investigating the effect of behavioral information security governance and national culture," *Computers & security,* Vols. 2014-43, pp. 90-110, 2014.

[11 ISO/IEC27001:2013, “ISO/IEC 27001:2013 Information technology -- Security techniques -- Information security management systems -- Requirements,” ISO/IEC, Geneva, 2013.

[12 Y. Cherdantseva and J. Hilton, “A Reference Model of Information Assurance & Security,” *IEEE proceedings of ARES,* vol. SecOnt workshop, no. Regensburg, Germany, 2013.

[13 GOV.UK, “The Security Policy Framework (SPF),” Statement of Assurance questionnaire in Excel - Gov.uk. [Online].

[14 Halkyn, “ISO27001 Self Assessment Checklist hits record downloads,” 19 February 2015. [Online].

[15 S. von Solms and R. von Solms, Information Security Governance, New York: Springer Science (ISBN 978 0 387 79983 4), 2009.

[16 A. Al-Omari, E.-G. O. and A. Deokar, “Information security policy compliance: the role of information security awareness,” in *Proceedings of the American Conference on Information Systems*, US, 2012b.

[17 A. Al-Omari, O. El-Gayar and A. Deokar, “Security policy compliance: user acceptance perspective,” in *Proceedings of the 45th Hawaii International Conference on System Sciences*, Maui, 2012.

[18 B. Stackpole and E. Oksendahl, Security Strategy, Boca Raton Florida: Auerbach Publications, 2011.

[19 W. Van Grembergen, S. De Haes and E. Guldentops, “Structures, Processes and Relational Mechnisms for IT Governance,” in *Strategies for Information Technology Governance*, US, Idea Group Publishing., 2004, pp. 1-36.

[20 ISACA, COBIT5 for Information Security, United States: Information Systems Audit and Control Association, ISACA , 2012.

[21 R. von Solms and S. v. B., “Information Security Governance_ A model based on the Direct–Control Cycle.,” *Computers and Security, Science Direct,* no. 25, pp. 408-412, 2006.

[22 Y. Bobbert, “ Biggest bang for the security buck,” Zero Trust magazine 112019, 2019.

[23 Y. Bobbert and J. Mulder, "A Research Journey into Maturing the Business Information Security of Mid Market Organizations," International Journal on IT/Business Alignment and Governance, 1(4), 18-39, October-December 2010, United States, 2010.

[24 G. Westerman and R. Hunter, IT Risk, Turning Business Threats into Competitive Advantage, Boston MA: Hardvard Business School Press, 2007.

[25 L. A. Gordon, M. P. Loeb and L. Zhou, “The impact of information security breaches: Has there been a downward shift in costs?,” *Journal of Computer Security,* vol. 19, no. 1, pp. 33-56, 2011.

[26 L. Gordon, M. Loeb and T. Sohail, “Market Value of Voluntary Disclosures Concerning Information Security,” *MIS Quarterly,* vol. 34, no. 3, 2010.

[27 M. Ishiguro, H. Tanaka, K. Matsuura and I. Murase, "The Effect of Information Security Incidents on Corporate Values in the Japanese Stock Market," Institute of Industrial Science, The University of Tokyo, Tokyo, Japan, 2011.

[28 S. Shackelford, “Should your firm invest in cyber risk insurance?,” *Business Horizons,* no. Center for Applied Cybersecurity Research & Kelley School of Business, pp. 349-356, 2012.

[29 Ponemon, “Perceptions about network security,” Ponemon Institute, United states, 2011.

[30 S. Srinivasan, “Cyber breach at Target,” *Harvard Business School,* 2016.

[31 Forbes, “Target's CEO Steps Down, Company Shares Drop,” http://www.forbes.com, United States, 2014.

[32 A. Glenn, “Equifax: Anatomy of a Security Breach,” Georgia Southern University, 2018.

[33 Rechtbank van Amsterdam, “Gerechtelijke uitspraak Diginotar,” ECLI:NL:RBAMS:2014:4888, 2014. [Online]. Available: https://uitspraken.rechtspraak.nl/inziendocument?id=ECLI:NL:RBAMS:2014:4888&keyword=internet%20ontbreken..

[34 R. Prins, “Interim Report; DigiNotar Certificate Authority breach “Operation Black Tulip”,” Fox IT, The Hague, 2011.

[35 Fox-IT, “DigiNotar Certificate Authority breach, “Operation Black Tulip”,” FOX IT in assignment of the Ministry of the Interior and Kingdom Relations, Den Haag, 2011.

[36 W. Deming, "Elementary Principles of the Statistical Control of Quality," *JUSE,* 1950.

[37 Y. Bobbert, Improving the Maturity of Business Information Security: On the Design and Engineering of a Business Information Security Administrative tool, Nijmegen: Radboud University, 2018.

[38 Y. S. J. Bobbert, “Zero Trust Validation: From Practical Approaches to Theory,” Iris Publishers, Scientific Journal of Research and Reviews, 2020.

[39 A. Rose, “The CISO’s Handbook — Presenting To The Board,” Forrester, Cambridge, MA, USA, 2013.

[40 IIA, “Cybersecurity, What the board of directors needs to ask,” The Institute of Internal Auditors Research Foundation (IIARF), Altamonte Springs, Florida, 2014.

[41 NOS, “Disruptions in Online Banking—377%,” 2014. [Online]. Available: http://nos.nl/artikel/618846-storingen-online-bankieren-377.html.

[42 S. Schninagl and A. Shahim, ““From the basement to the boardroom”: towards digital security governance,” VU press, 2019.

[43 v. t. Achternaam, “Titel van artikel,” *Titel van logboek,* pp. Pagina’s Van - Tot, Jaar.

[44 v. t. Achternaam, Boektitel, Naam van de stad: Naam van de uitgever, Jaar.

[45 Y. Bobbert, “Porters' Elements for a Business Information Security Strategy,” *ISACA Journal,* vol. 1, no. United States, pp. 1-4, 2015.

[46 S. Postuma, “Structures, Processes and Relational mechanisms needed for the implementation of Business Information Security Strategy,” Antwerp Management School, Antwerp Belgium, 2013.

[47 Y. Bobbert and J. Mulder, “Boardroom dynamics: Group Support for the Board’s Involvement in a Smart Security,” *ISACA Journal ,* no. 5, 2016.

[48 R. Moen, Foundation and History of the PDSA Cycle, Detroit: Associates in Process Improvement-Detroit, 2009.

[49 P. Charantimatch, Total Quality Management, India: Pearson, 2006-2011.

[50 W. Shewhart, Statistical Method from the Viewpoint of Quality Control;, Dover: Department of Agriculture, 1939.

[51 Y. Bobbert and J. Mulder, “Enterprise Engineering in Business Information Security. A case study & expert validation in Security, Risk and Compliance artefact engineering. A comparative analysis of a security measurement tool,” in *Springer*, EEWC 2018,, Springer Nature Switzerland AG 2019, 2019, pp. LNBIP 334, pp. 1–25,.

[52 AIVD, “Jaarverslag AIVD,” Algemene Inlichtingen en Veiligheidsdienst, Den Haag, 2014.

[53 Y. Jewkes and M. Yar, Handbook of Internet Crime, UK: Willan Publishing, 2010.

[54 CIGI, “Global Cyberspace Is Safer than You Think: Real Trends in Cybercrime,” Centre for International Governance Innovation, 2015.

[55 J. Cummings, “Building a cyber savvy board,” in *Navigating the digital age*, Korn Ferry, 2018, pp. 313-318.

[56 NU.nl, “The Netherlands: Number One in Online Banking Disruptions,” January 13 2014. [Online]. Available: www.nu.nl/tech/3674517/internetbankieren-relatief-vaak-getroffen-storingen.html.

[57 C. Seale, Researching Society and Culture, Sage Publications - Second edition: ISBN 978-0-7619-4197-2, 2004.

[58 Y. Bobbert, “Use of DEMO as a methodology for business and security alignment,” *Platform*

for Information Security, pp. 22-26, 2009.

[59 J. Dietz, Enterprise Ontology, Delft University: Springer, 2006.

[60 J. Mulder, Rapid Enterprise Design, Dissertatie TU Delft: VIAGroep NV Rijswijk, 2006.

[61 Accenture, "The Cyber Security Leap: From Laggard to Leader," Accenture, 2015.