#white papers

Risk and Compliance

AIRBUS

#white papers

Risk and Compliance

Risk and compliance are two big words used in the Security community. Even if each concept is quite simple, using them to protect companies can prove to be a complex task. This document aims at describing the two approaches and giving guidelines to deploy them wisely.

summary

Authors

Yann BERGER, Security Audits and Governance, APSYS
Jérôme BOUÉ, Security Technical Officer, APSYS
Florent PETIT, Security Technical Coordination, APSYS
Manon PISTRE, Security Compliance, APSYS
Yves RÜTSCHLÉ, Security Architect, APSYS

AIRBUS

Introduction

Companies face multiple risks. Knowing how to manage and take risks is part of the daily life of a CEO or an entrepreneur. Cybersecurity risks are among the most complex to manage. They prove to be systemic due to the latest digitization trends and they evolve as fast as the attackers. To address these risks, an extreme approach would be to remove all connections. The side effect would be a major loss of competitiveness and a probable bankruptcy. It is therefore necessary to manage these risks wisely. Putting in place adequate protections while leaving room for the company's operations and value creation.

Two approaches to managing cyber risks are often mentioned: the compliance approach and the risk approach. Opposing them would be wrong; they are complementary. And regardless of the approach and method used, the objective remains the same: to obtain information, to make informed choices and take action. Risks or non-compliances without choice and action are useless.

The risk-based approach

Let's start by talking about risk analysis. They are used to take a step back and identify security incidents that could occur on the studied object (e.g. system, product, service, project). The consequences and potentiality of these possible incidents are evaluated in order to define the most appropriate actions to wdeal with these risks. In order to do this, it is necessary to ask multiple questions in a structured way:

- What do we want to protect? What is its value?
- What are the impacts in case of loss of confidentiality, integrity or availability?
- What are the threats we face?
- How can these threats reach us? What is the path of attack?
- How difficult will it be for the attacker to achieve these scenarios?

At the end, the analysis generates a list of threat scenarios with their consequences and potentialities, which constitutes a security risk. As a reminder, ISO 31000 defines a risk as «the effect of uncertainty on objectives». We find all these notions in our cyber risk scenarios. We identify the objectives, what we want to protect, the effect or impact that a security incident could have on them, and the level of potentiality for these incidents to occur.

How do you perform a Risk analysis?

There are many methodologies and techniques used to perform risk analyses. It is important to select the most relevant ones according to the objectives and context.
It is possible to perform very preliminary analyses for scoping purposes. This is useful, for example, when launching large strategic projects or to establish the most balanced compliance base possible.
In more complex industrial environments, risk analyses are used at the design stage of a system to accurately adjust this design to security needs.
Some analyses are also imposed by the customer or by an authority during an approval process for example.
Each need has its own level of detail and abstraction as well as its own associated workload.

EBIOS RM

Some methodologies present recurrent pitfalls. Recurrent worries are a lack of understanding between business and security teams and a quest for exhaustiveness that leads to non-efficient analysis.
Based on these observations, the ANSSI has recently published the EBIOS RM methodology which aims to reconcile business and security by proposing a modular, efficient and iterative approach.
Within this methodology, the different stakeholders are pushed to a closer collaboration and several ways of doing are described in order to modulate the analysis to the established needs. And in each step of the analysis, there is flexibility in the techniques that can be used. The framework is established but the analyst retains degrees of freedom on how to proceed.

What to do with the Risks assessed in an Analysis?

As previously mentioned, risk analyses are used to estimate risks precisely with the aim of helping decision-makers in their treatment decisions (according to their technical, organizational and budgetary constraints, etc.).
In an ideal world a risk is identified and treated to reduce it to an acceptable level. In the real world, it is possible that a decision will result in compromises and acceptance of risks that cannot be fully reduced for now. And in the worst case, a feature may have to be abandoned because there is no solution to implement it securely or the associated cost would be too great.
The target is a well balanced level of security. Accordingly, risk analysis can recommend additional security measures but they can also avoid over-specification and the addition of measures that in the end would not bring much.

From one approach to the other

As previously mentioned, risk analyses are used to estimate risks precisely with the aim of helping decision-makers in their treatment decisions (according to their technical, organizational and budgetary constraints, etc.).
In an ideal world a risk is identified and treated to reduce it to an acceptable level. In the real world, it is possible that a decision will result in compromises and acceptance of risks that cannot be fully reduced for now. And in the worst case, a feature may have to be abandoned because there is no solution to implement it securely or the associated cost would be too great.
The target is a well balanced level of security. Accordingly, risk analysis can recommend additional security measures but they can also avoid over-specification and the addition of measures that in the end would not bring much.

The compliance approach

Compliance is a broad approach that aims to protect the company from the cyber threats that are most appropriate to the given security context. It targets a minimum level of security within the company. It proposes effective measures to face the attacks usually experienced by the company. It is based on the risk analyses previously carried out and the collective experience of the security community. In concrete terms, the company defines the requirements that will be applicable to its projects, products, services and applications and then tries to comply with them. These requirements are based on national and international regulations, on the imperatives expressed by its customers and on additional requirements that the company imposes on itself.
These requirements are grouped together in good practices guidelines or standards defined per environment. All the applicable requirements then constitute a security baseline with which projects must comply.

How to assess Compliance?

Compliance can be verified in a brutal way: it is either compliant or it is not. Sometimes there are several conditions to a requirement and if one of them is not met, it is called non-compliance or partial compliance.

It is also possible to show nuance, the non-compliance can be critical, major, minor, ... The graduation may refer to the extent of the deviation from the requirement or to an associated level of risk. The main purpose is to help prioritize and make decisions according to the principle of continuous improvement and gradual increase in maturity. For example, we start with a situation where the requirement is unknown, then progressively things will be done in an ad-hoc manner, then documented, managed and finally they will enter a continuous improvement mode. For example, it is possible to perform a gap analysis that goes beyond the simple search for non-compliance by identifying what is missing to achieve full compliance. These gap analyses require more time but are more interesting, especially when a risk analysis is done afterward.

Finally, compliance analyses can be done in a more or less rigorous way, ranging from a simple declaration by the manager on a questionnaire in a few minutes to an audit with an evaluation based on evidence involving a third party. The latter is a more formal approach, allowing for more accurate results, especially when the audit is conducted by a «Qualified» provider. The audit produces an official report, which gives it more legitimacy, but involves a higher cost.

What to do with a noncompliance?

A non-compliance leads to three options: stop, correct or tolerate.

Very directly, a non-compliance can involve stopping the project. Sometimes it is better to lose the operational opportunity than to take the related security risk.

It is important to understand that requirements generally describe security measures that in turn reduce risk. A non-compliance results in organizational and/or technical vulnerabilities. A technical vulnerability is an entry point for an attacker, and is therefore linked to a security risk. An organizational vulnerability is a weakness in the way the company operates, which can subsequently open doors to attackers, for example by creating new technical vulnerabilities. Organizational vulnerabilities are less direct but more systemic.

So to avoid these vulnerabilities, the second option is to correct the non-compliance by selecting and implementing the most appropriate security controls. These controls consist of the application of technical cyber measures (e.g. firewall), physical measures (e.g. armored door) or organizational measures (access validation process) that will raise the security level.

But in the real world, managers have to take risks in order to seize business opportunities. It is therefore sometimes possible to tolerate non-compliance, usually during a predetermined period of time.

How to identify and assess the risk related to a non-compliance?

The big question. A non-compliance usually has little or no meaning. To make decisions, decision-makers want to know the risk associated with a non-compliance.

To identify and assess these risks, like any other risk, it is always possible to use engineering judgment; it's always better than rolling the dice or playing darts. It is best to make sure that the person who is going to make the judgment has all the information and skills necessary to give a relevant opinion. It is then a matter of telling the little story that will describe the cause and effect links from one step to another, from a non-compliance to the risk for the company («Once upon a time, a company's IT assets that were not updated frequently in accordance with the IT department's requirements and were exposed to the Wanna-Cry ransomware attack, which caused a total shutdown of the production for several days»).

It is also possible to link a non-compliance to risks already established and managed at the company level. The contribution 2 THE COMPLIANCE APPROACH of this non-compliance to existing risks is identified even if the accurate assessment is not. This process has the merit of making communication simpler and often brings more meaning to non-compliances (it accelerates the story telling).

It is also possible to define structured models that will identify levels of risk in front of non-conformities according to their number and type. Anglo-Saxon risk management is very much based on these mechanisms.

Doing a partial risk assessment is also feasible. Assessing only the impact of a non-compliance can often be sufficient to make decisions. The likelihood is still unknown but the workload linked to an impact assessment is often very reduced.

Finally, the last option is to launch a complete risk analysis, with detailed and exhaustive scenarios that will assess impacts and potentialities. This is more the European way of doing things. This is additional work that should be reserved for projects that need it.

Which approach for which need?

How to assess Compliance?

In an ideal world, risk analyses should be comprehensive and systematic. But in the real world, they require time and expertise, and companies generally lack both. The compliance approach is often a sufficient prerequisite.

Risk analyses are therefore reserved for those subjects that really need them, such as in the following situations:

- When the threats are very significant and the compliance base is not sufficient to deal with them
- When systems, sometimes installed before any security considerations, need to be more properly managed. This is particularly the case when a new compliance basis is required for an existing system that is far from being compliant. Risk analysis can then be used to prioritise efforts.
- When clients or authorities require one
- When a more precise knowledge of security needs is required to make design choices
- When the compliance approach is not possible, for example on very specialised systems or when these systems are too new to benefit from mature standards. Typically, the security of industrial systems is a headache: PCs may be running obsolete Windows XP on which the machine operator is not allowed to intervene, no anti-virus is present, and so on. The risk analysis then supports the definition of specific security needs for the system, in order to adapt protection level.

- Finally, it is also interesting to carry out a risk analysis at the company level, in order to take more strategic and organisational decisions. This risk analysis, which is necessarily imprecise in its first iterations, can then be used to zoom in on the areas that need more attention, which in turns means triggering more detailed analyses later on.

In the end, the cost of the risk analysis must be set against the expected benefit. Some protections must be deployed by compliance because they are necessary in the vast majority of cases. It is generally absurd to systematise risk analyses to find that a firewall must be installed in 99% of cases. Implementing a common set of security measures is most often an effective approach to achieving a first level of security with little effort.

On the other hand, when the cost of the risk analysis is very low compared to the cost of a security function (e.g. when developing a very complex product), it is relevant to use risk analyses to define exactly what needs to be protected and against what. By simplifying a lot, we can consider that:

- IT environments should use the compliance approach first and then perform risk assessments for specific situations
- Product development environments should use risk assessments during design to accurately target a good security level
- Industrial environments are in a grey area where each approach could be more valuable than the other depending on the level of specificity and maturity of the considered perimeter.

Two complementary approaches

The two approaches, compliance and risk, support the management of the company's real risks.

We never know exactly what these risks are; by definition, they contain an element of uncertainty. Compliance baselines and risk analyses are necessary to make the most informed choices possible and in the end protect the company's value creation.

The complexity of cybersecurity means that we cannot rely on common sense alone to manage security risks; systems and organizations have become far too complex for that. Implementing an effective risk management requires deep thinking on how to structure a multi-phased response and how to lead the resulting changes.

To do this, a compliance defined at the right level and applied widely throughout the company makes it possible to impose a certain security level. The risk analysis then identifies what needs to be done on top of compliance to protect against more specific threats or contexts.
Risk or compliance analyses are extremely complex activities that require thought and rigor. They are very formal and structured. But we must not forget that in the end, it is always the human who decides, who judges the level of potentiality, impact or risk. Methods and tools ensure a good level of confidence in the result as well as a certain degree of repeatability, but they do not absolve humans from making choices and assuming them.

Contact us

FOR MORE INFORMATION:
Airbus Protect

FRANCE
Metapole 1, boulevard Jean Moulin
CS 40001 / 78996 Elancourt Cedex
France

GERMANY
Willy-Messerschmitt-Str. 1
82024 Taufkirchen /
Germany

UNITED KINGDOM
Quadrant House / Celtic Springs /
Coedkernew - South Wales NP10 8FZ
United Kingdom

contact@airbus-protect.com
airbus-protect.com