Practical approach to the Supply Chain Security Management

2ND ENISA MARITIME CYBERSECURITY CONFERENCE

– 14 ottobre 2022 –

Flavio Marangi
Senior Manager

Balance Srl

GOALS

GOAL 1

Define a process that is consistent and measurable, which takes into account all the applicable information and produce valid, repeatable and comparable results

GOAL 2

Identify the supply chains **and classify the suppliers** by evaluating the relationship between the organisation and its suppliers

GOAL 3

Create a standardized flexible template of questions to ‘‘Qualify’’ the suppliers and ‘‘Assess its Maturity’’ that can help communicate supplier risk posture

GOAL 4

Check information from supplier’s assessment and compare the result with the criteria of transparency, completeness, accuracy and consistency established

GOAL 5

Analyse the security posture of suppliers by calculate risk and assign ratings to each risk description **to illuminate potential gaps**

GOAL 6

Continuous monitoring and improving must be ensure both from organisation and supplier which should cooperate in order to strengthen the security posture

WHY

Supply chain security management is an **opportunity** to assess the security of those suppliers which support a critical service or critical infrastructure and consider that assessment as part of risk management processes and procurement by taking appropriate measure

WHY?

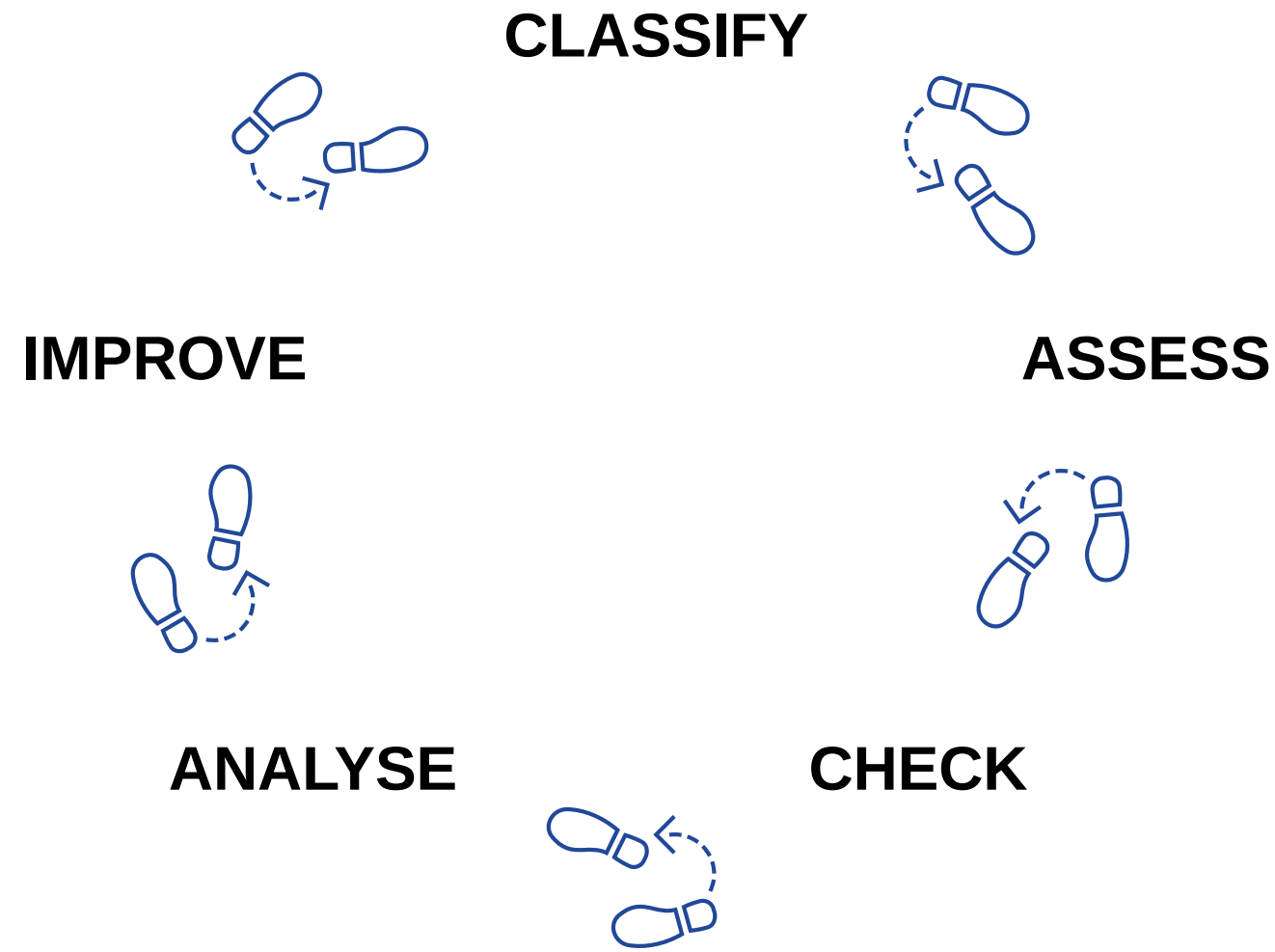
DEFINE A PROCESS

Supply Chain Security Management is a process for **creating** and **protecting** the value of the organisation and as such must be:

- ☐ Globally integrated
- ☐ Structured and dynamic
- ☐ Flexible
- ☐ Inclusive
- ☐ Based on the best information available
- ☐ Inspired by continuous improvement

THE 5 STEPS APPROACH

Managing Supplier Risk to security requires strategy, understanding stakeholders' objectives and support for decision-making



STEP 1: CLASSIFY

One of the biggest challenges when managing the security of the supply chain is being able to have a list of all the suppliers and their relationship with the organization.

Securing organization, particularly supplier info, is a fundamental consideration in risk planning.
People, **processes**, **technologies** and **operations.** This is the exact order of the factors on which to operate and in that order these factors must be analyzed within the classify step.

PEOPLE

Who within supplier owns the relationship with the organization

PROCESSES

What each supplier does for organization

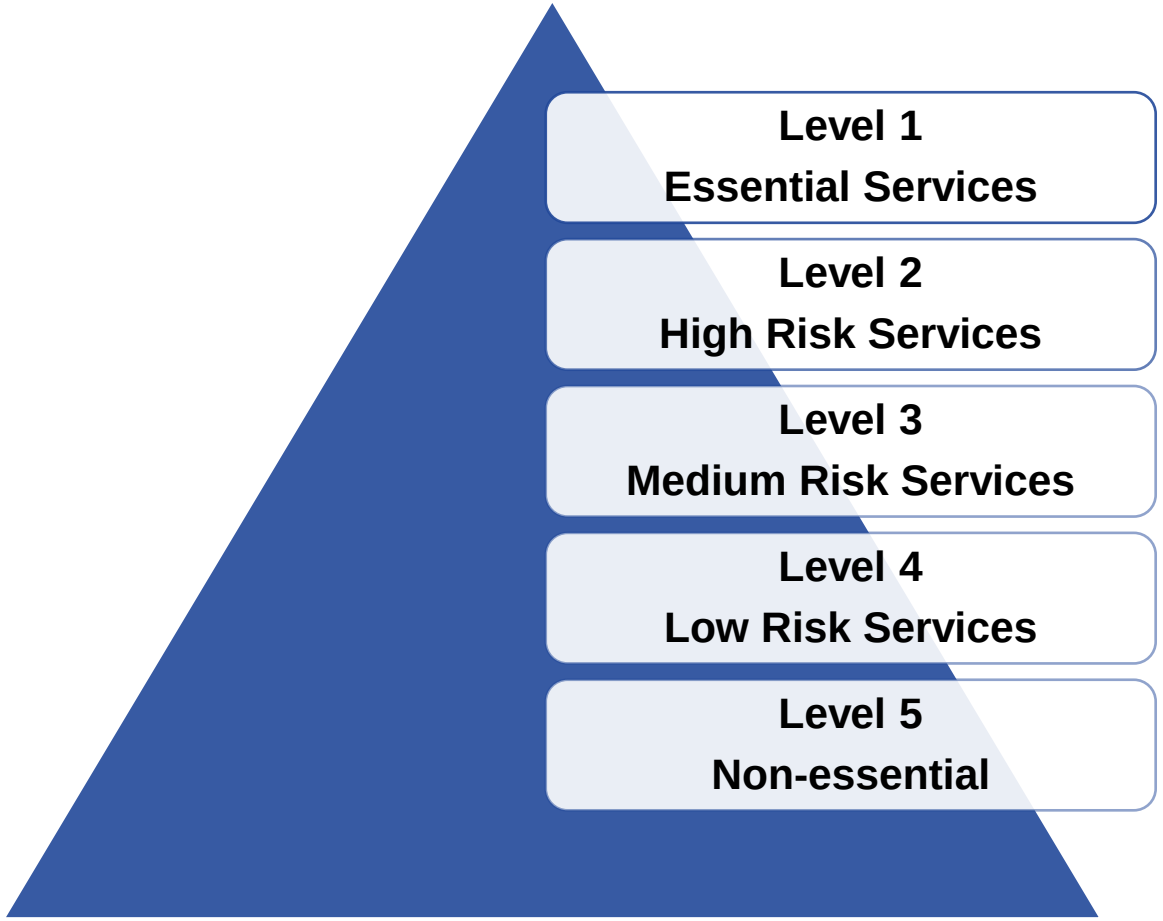
TECHNOLOGIES

Which supplier have access to critical systems and information

OPERATIONS

Whether or not the supplier manages essential business operations

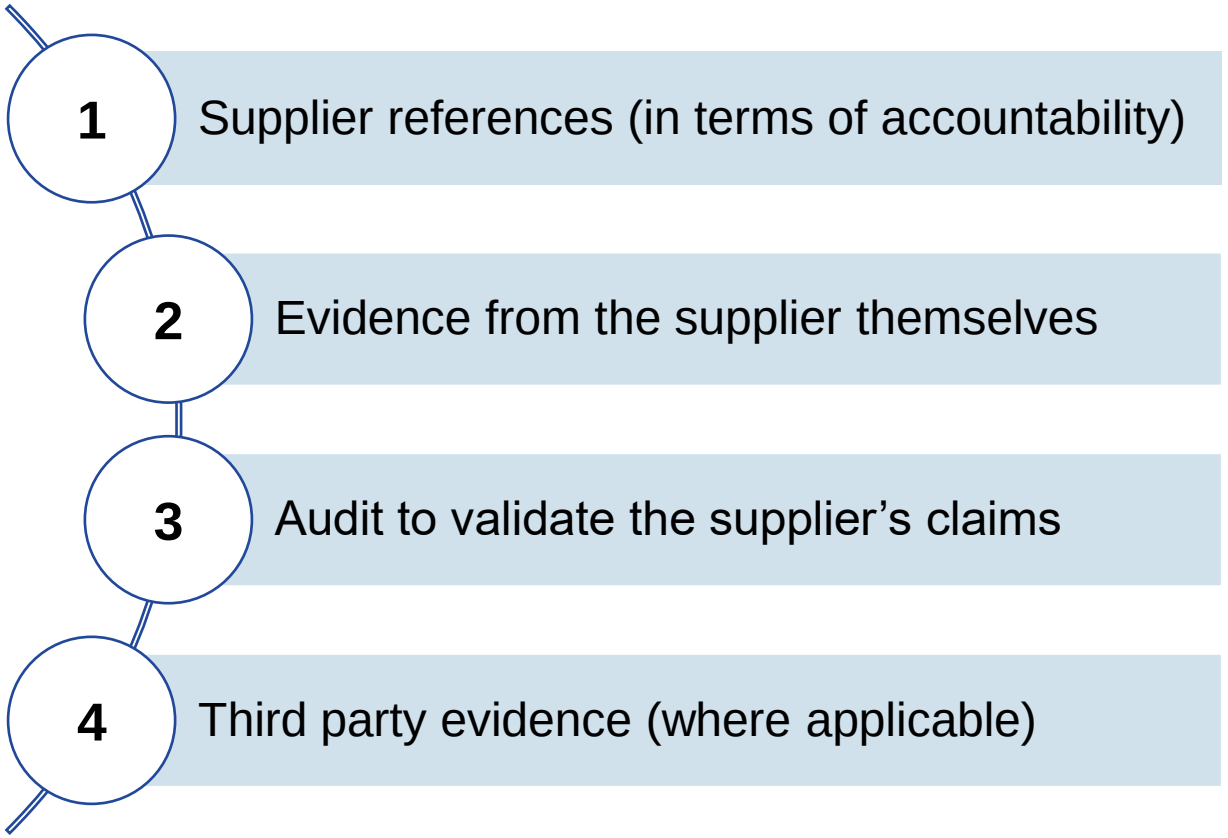
STEP 1: CLASSIFY



By using a scale to rank supplier according to risk, the organization can focus on which of them need tighter security measures, monitoring potential gaps and define assessment life cycles.

STEP 2: ASSESS

Assessing the security risk due to a supplier requires



STEP 2: ASSESS

To reach all these requirements and make the assessment consistent and repeatable, the organization needs to split the assessment in two parts

SUPPLIER QUALIFYING ASSESSMENT

SUPPLIER MATURITY ASSESSMENT

Organisation should consider both the supplier’s security culture and behaviour

SUPPLIER QUALIFYING ASSESSMENT

Questions which supplier can only answer “YES” or “NO” and adding notes in order to be more transparent, complete and accurate.

ID No.	CATEGORY	QUESTION REFERENCE	ADDITIONAL INFORMATION
1.1	Who are your references? Please provide individual names and contact information.		
2.4	Do you have a policy or process to ensure that none of your suppliers or third-party components are on any banned list?		
3.2	Do you have policies for conducting background checks for your suppliers and/or subcontractors?		
6.3	Do you follow operational standards or frameworks for managing Information Security/Cyber security (e.g., NIST CSF 1.1, NIST 800-37, ISO IEC 27001, etc.)		
5.3	Do you have teams or committees that meet regularly on cybersecurity issues?		
9.4	Do you keep a record of security events?		

SUPPLIER MATURITY ASSESSMENT

Questions which supplier can only answer by selecting the maturity level which better fit is security posture. A maturity legend is also provided to the supplier.

ID No.	CATEGORY	MATURITY LEVEL	ADDITIONAL INFORMATION
1.1	Write and implement an information systems security policy (ISSP), which describes all organisational and technical means and procedures, including cybersecurity considerations		
2.3	Asset disposal policy to ensure the secure deletion of data		
3.1	Define a vulnerability management process to identify asset vulnerabilities		
4.3	Implement multi-factor authentication mechanisms for accounts accessing applications and data		
5.2	Improve and keep incident policies and procedures up-to-date by testing them through training exercise		
5.3	Define a process to communicate security incidents affecting our data		

SUPPLIER MATURITY LEGEND

ID No.	CATEGORY	MATURITY LEVEL 1	MATURITY LEVEL 2	MATURITY LEVEL 3
1.1	Write and implement an information systems security policy (ISSP), which describes all organisational and technical means and procedures, including cybersecurity considerations	The supplier has drafted one or more information system security policies (ISSPs), which include cybersecurity considerations, that provide technical guidance and supporting procedures in order to protect information technology and operational technology environments	The supplier has formally codified its ISSPs in an overarching plan that provides tailored guidance to internal functions. Top management have reviewed and approved the supplier's ISSPs.	The supplier regularly reviews its ISSPs to ensure that policies and procedures accord with defined objectives.
2.3	Asset disposal policy to ensure the secure deletion of data	The supplier has established procedures for the asset disposal	The supplier has a policy that establishes asset disposal protocols.	The supplier reviews asset disposal activities, processes, and procedures at least annually to ensure effectiveness.
5.3	Define a process to communicate security incidents affecting our data	The supplier has established procedures to communicate with both internal normal operations and *Organization* to enable rapid incident response actions	The supplier has established and documented rules, plans, policies, procedures, and/or written practices that guide all incident information-sharing activities	The supplier regularly reviews policies, procedures, and/or directives guiding incident information sharing activities.

STEP 3: CHECK

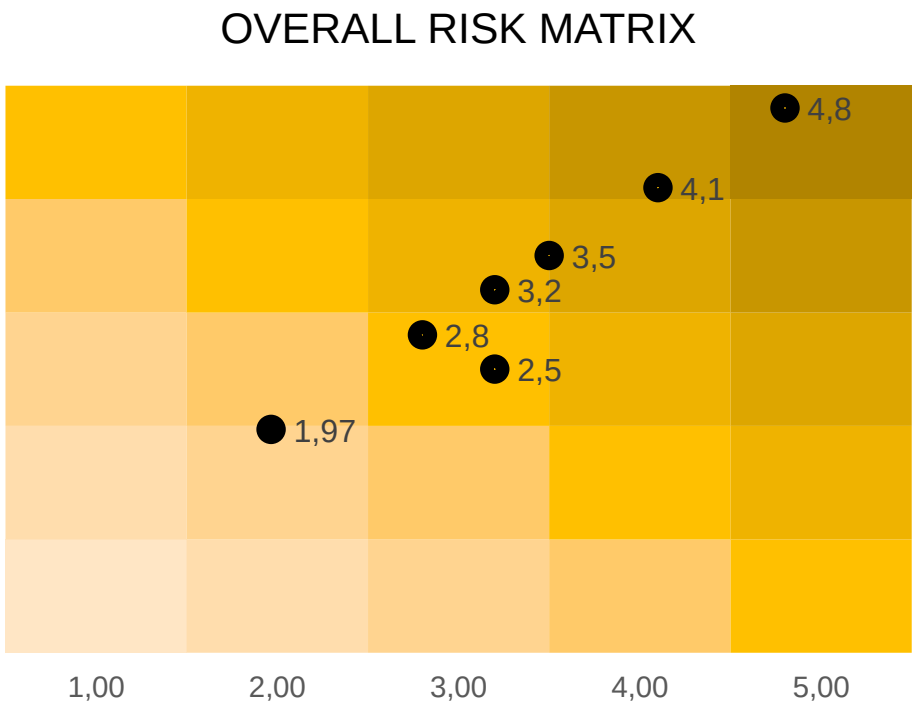
During the **check**, it is important to evaluate:

- ☐ The accuracy of the assessment processes
- ☐ Supplier transparency, openness, and collaboration with the organization
- ☐ Supplier compliance with security obligations and requirements
- ☐ Supplier approach to the risk management
- ☐ Supplier consistency

STEP 4: ANALYSE

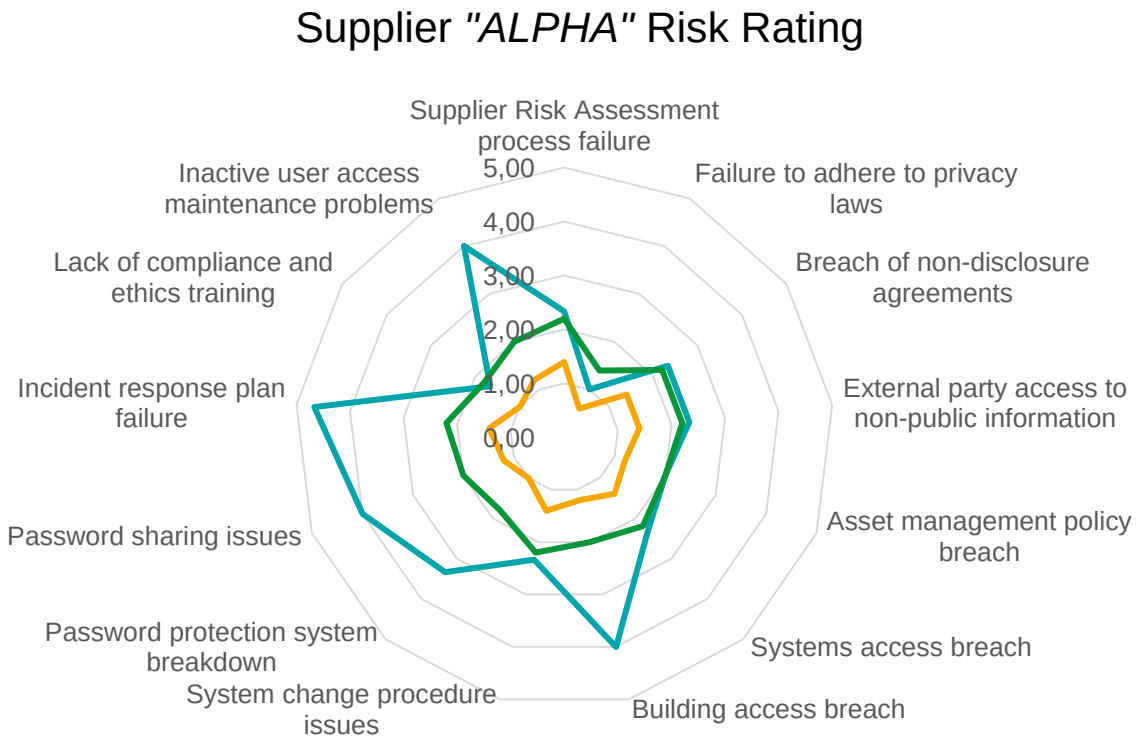
When approaching to analyse step, it is important to bear in mind which kind of reports the organization needs to extrapolate.

An always useful report is an “Overall Risk Matrix” to understand which supplier has the lowest risk rating during the procurement process.



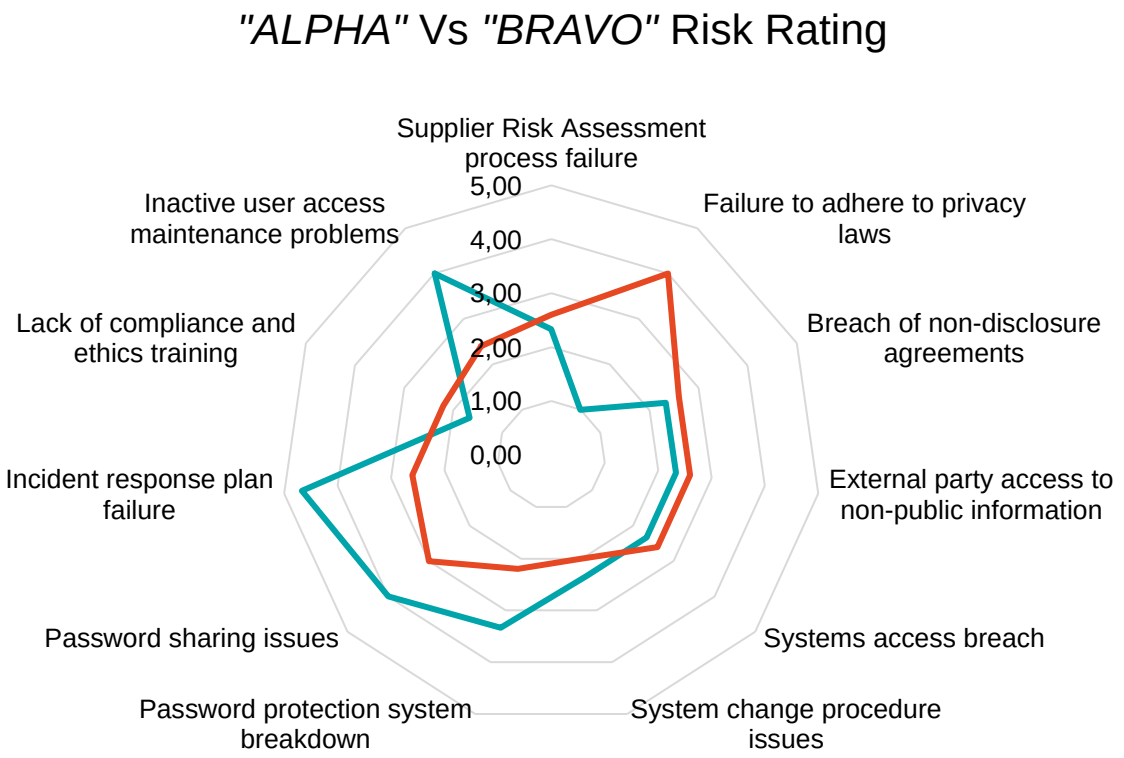
STEP 4: ANALYSE

But the aim of this approach is also to assign ratings to each **risk description** to detect potential gaps and compare the supplier risk posture during the assessment life cycle…



STEP 4: ANALYSE

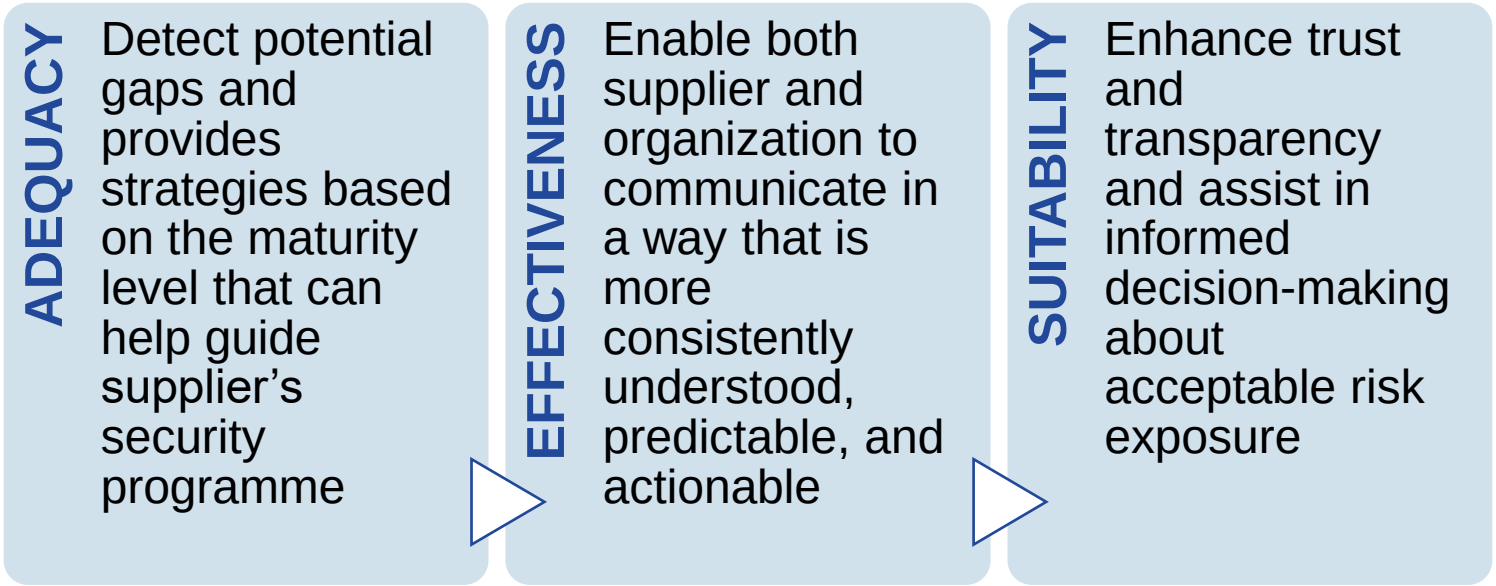
... such as understand the differences in terms of security posture between two or more suppliers for single risk.



STEP 5: IMPROVE

The Improve step consist in a series of considerations made between supplier and organization to continuous monitoring the security posture and continually implement new security measures and/or processes which are able to reduce the risk level.

It is important in this phase ensure cooperation between supplier and organization in order to



BENEFITS

This approach guarantees extreme flexibility in the supply chain risk management

Moreover, it does not collide with any other processes within the organization such as the information security management itself or the procurement process.

In fact, it complements them guaranteeing, based on the accuracy, a delta of more or less wide knowledge of the risk expressed by suppliers, helping in the definition and address of corporate security strategies.

Thank you!

Flavio Marangi
Balance Srl
fmarangi@balancesrl.it