Public

CONCLUSION

SUPPLIER & CONTRACT MANAGEMENT GUIDELINE

Author
Roel Gloudemans
(roel.gloudemans@conclusion.nl)

With the cooperation of
Chris Gralike, Ricky Hoots, Artien Bel, Dennis Pieterse, Paul Schoorl, Manfred Anneveld

Status:	Definitive
Version:	1.7
Best before:	2026-05-19

Version table			
Date	Version	Through	Adaptation
21-11-15	0.1	R. Gloudemans	First draft
22-02-23	1.0	R. Gloudemans	Definitive
22-10-04	1.1	R. Gloudemans	R-LM-02a, extension of R-LM-02 to include sanctioned countries and organizations.
22-10-20	1.2	R. Gloudemans	Addition SBOM (R-LM-29 and R-LM-30)
22-12-15	1.3	R. Gloudemans	Adjustment to ISO27001:2022, removal mapping table
23-04-12	1.4	R. Gloudemans	Amendment R-LM-03, added that the certificate must be from an accredited body.
24-05-10	1.5	R. Gloudemans	Update requirement to ISO27001:2022
24-11-24	1.6	E.Aksoy	English Translation
25-05-19	1.7	R. Gloudemans	Spelling/grammar corrections. Backported changes from 1.6 Dutch version. R0LM-29 added

Approval	
Document	Version
Version	1.0
All major versions of this document are approved by at least 5 security officers from different Conclusion companies. Minor changes, such as spelling errors and changes and/or additions to the explanatory notes, are the responsibility of Conclusion's Chief Security Officer	
*This document is classified as **public** information and can be made available (in pdf form) to anyone for whom this policy document may be relevant.*	

Contents

Page

1. Introduction

Conclusion is dependent on the services purchased from others for its services. It is therefore important that the security level of these purchased services is in line with the needs of Conclusion, so that a strong and resilient supply chain is created. So-called "supply chain attacks" can only be prevented by good cooperation between supplier and customer. This includes setting clear requirements.

The requirements imposed on suppliers and products depend on the purpose for which Conclusion uses them. A requirement for ISO certification, for example, makes sense for a supplier who processes data for, or on behalf of, Conclusion and/or its customers, but may be pointless for the supplier of coffee cups.

1.1 Scope

The guidelines in this document only apply to parties who, by providing their services, may be able to influence the confidentiality, integrity or availability of the data under Conclusion's control.

In practice, this concerns all suppliers:

- with which a data processing agreement must be concluded, because they:
  - process (or store) employee data or
  - store data of Conclusion's customers on their systems and/or act based on that data.
- who process or store data on behalf of Conclusion or Conclusion's customers.
- Who communicate via digital means on a regular basis.

Think, for example, not only of suppliers of SaaS services and hosting parties, but also of a communication agency that sets up an employee survey.

This guideline is an addition to the applicable purchasing policy, as used by the Conclusion company in question.

1.2 Objective

The objective of the Supplier Management Guideline is to ensure the privacy & security of data and assets of the organization, as well as the safety and health of personnel.

This guideline is part of the security policy of Conclusion Benelux consisting of:

- Security policy Benelux.
- System of guidelines, of which this guideline is one.

1.3 Target audience

The target group of this document contains anyone who plays a role in the procurement of products and services.

1.4 The role of guidelines

The guidelines at Conclusion indicate the recommended set of controls, linked to the classification of the data. Some of the controls can be implemented immediately, others need to be further elaborated by architects and designers for the context in which the control is to be applied.

Every company within Conclusion is responsible for finding the right balance between taking and avoiding risks. This document will help with that process. The guidelines are a common set of best practices within Conclusion. Failure to comply with a best practice should be considered a vulnerability and explicitly addressed in the company's risk management. This will then show whether there is an associated risk and whether this risk is acceptable.

If a vulnerability leads to an unacceptable risk for Conclusion, steps must be taken to mitigate this vulnerability. Conclusions' Security Office, with the help of the security officers guild, will periodically recalibrate the set of guidelines based on the companies' risk analyses. For example, when this document is reviewed, superfluous guidelines will disappear from the policy and others will be added.

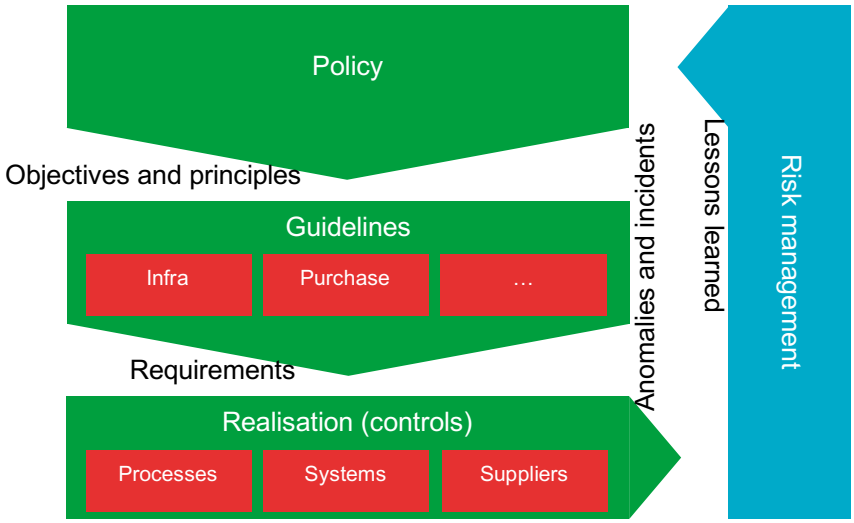

Figure 1, The role of guidelines

2. Controls for suppliers

Suppliers provide products and services to Conclusion. In both cases, it is important that Conclusion can rely on these suppliers for the scope of its services. The criteria used to be able to trust a party increase with the importance of Conclusion's data and associated services that the supplier may be able to influence.

When providing services, only the supplier itself needs to be considered. When purchasing a product, both supplier and manufacturer must be evaluated.

The list of controls below indicates when a supplier/manufacturer may be trusted in the context of the classification of the data that may come in contact with the service or product. These controls are supplemented by the controls from Chapter 4 "Product requirements" or Chapter 5 "Service requirements".

Recap - All data classification levels of Conclusion

Level	Availability	Integrity	Confidentiality
1	Very low	Not checked	Public
2	Low	Correct	Company information
3	Middle	Important	Internal
4	High	Essential	Confidential

The table below shows the controls. A classification is indicated for each control. *The classification relates to confidentiality, integrity or availability.* The higherst classification is the one that counts.

The meaning of the classifications can be found in the "Data Classification Guideline"

Controls for suppliers

#	Control and explanatory notes	1	2	3	4
R-LM-01	**The scope of the trust must be explicitly defined.** A supplier is only trusted for the context in which they deliver their product or service. This scope must be explicitly described, including the data processed within the scope and the classification of this data. The conditions for this trust must be documented. These conditions consist of the controls set out in this document and any specific additional control.	X	X	X	X

Controls for suppliers					
#	Control and explanatory notes	1	2	3	4
R-LM-02	**Only reputable suppliers.** Only reputable suppliers are allowed. These are suppliers who: 1. have not been convicted of or proven to have participated in the provision of data or giving access to customer data or infrastructure to third parties, outside of Dutch or European legislation; 2. In the past 5 years, have not been fined by the Dutch Data Protection Authority for careless handling of personal data or violating the GDPR; 3. are able to submit a VOG-RP; https://www.justis.nl/producten/vog/vog-voor-rechtspersonen.aspx 4. are complying with the GDPR and the Dutch AVG.			X	X
R-LM-02a	**Supplier is not listed or located in blacklisted countries or uses blacklisted products and/or sub-suppliers.** The blacklist consists of countries that have been sanctioned at national or European level because of disrespect for human rights, missing freedom of the press or missing freedom of expression. Think of Russia, North Korea and Iran		X	X	X
R-LM-03	**Supplier must be in possession of a ISO27001:2022 certificate or equivalent** The vendor has an explicit mechanism to improve itself. Alternatives are, for example, NEN-7510:2011 and ISAE-3000. Pay attention to whether the certificate has been issued by an accredited body. This can be checked at http://www.rva.nl The supplier must show the certificate and "statement of applicability", so that the scope of the certification is clear, and it is clear which measures from Annex A apply.			X	X
R-LM-04	**Suppliers are assessed at least annually.** All suppliers are inspected at least annually to ensure that they meet the set requirements.			X	X
R-LM-05	**For every procurement, the security officer must be asked for advice.** Before starting an IT procurement, advice must be sought from the security officer, so that he or she can assess whether the service or product in question fits in the context of Conclusion. For this advice, the security officer will, for example, check whether privacy and security by design principles have been met.		X	X	X

3. Controls for products

Controls for products					
#	Control and explanatory notes	1	2	3	4
R-LM-06	**There is support throughout the entire lifecycle.** If the product is dependent on firm- or software, it must be supported throughout its economic life.	X	X	X	X
R-LM-07	**Critical vulnerabilities in firm or software are usually fixed within a few days.** Determine in advance what the maximum acceptable period is be in relation to the impact of any critical vulnerabilities.		X	X	X
R-LM-29	**Supplier provides a Software Bill of Materials (SBOM).** A Software Bill of Materials specifies which third-party software modules the product depends on. This applies to both software and hardware that is equipped with firmware. The SBOM enables Conclusion to quickly make an inventory of a Log4J type event.		X	X	X
R-LM-08	**A support contract is in place** If the functioning of the component is essential for Conclusion services, the possibility of a maintenance contract must exist. The support contract must include soft- and hardware support.		X	X	X
R-LM-09	**Security tests are allowed** Some products contain a license clause which disallows security and performance testing. Conclusion does not find this acceptable.			X	X
R-LM-10	**Product does not send data to supplier or third party without permission.** Products may only send data to the supplier or third parties with explicit permission.		X	X	X
R-LM-11	**If the product transmits or stores privacy-sensitive data, a processing agreement is mandatory.** A data processing agreement (or something equivalent to it) is mandatory when forwarding or storing privacy-sensitive data.			X	X

4. Controls for services

Controls for services					
#	Control and explanatory notes	1	2	3	4
R-LM-12	**Supplier allows audits** The Supplier allows Conclusion to carry out audits of the infrastructure and services or allows an (independent) third party to do so, whereby Conclusion gains insight into the audit report.			X	X
R-LM-13	**Supplier has ISAE 3402 type II statement** The supplier can provide an ISAE 3402 type II statement every year, for the scope of services. A SOC2 type II or audit report of similar content will also suffice.			X	X
R-LM-14	**Supplier allows security/pentests** The supplier allows Conclusion to carry out security tests or to have them carried out by an independent third party. Conclusion will carry out these in such a way that disruptions as a result are unlikely.			X	X
R-LM-15	**The supplier has set up security monitoring for the scope of the service** The supplier is connected to its own or contracted Security Operations Centre for the provisioning of services. Alternatively, the supplier is willing to cooperate in a link to the SOC of the Conclusion company in question.				X
R-LM-16	**Service can be connected to Conclusion's Identity and Access Management platform.** All services must be linked to the Conclusion IAM system for authentication and preferably also authorization. *This only applies when Conclusion staff must log in to the service.*		X	X	X
R-LM-17	**Supplier uses a clear SLA with service levels that correspond to the data classification at Conclusion** Conclusion needs to be clear about what exactly it expects from the service. To this end, Conclusion itself must analyze the value service chain and formulate which service levels are desirable. These service levels must be in line with the (standard) SLA of the service provider. The Supplier must periodically report to Conclusion on the current/measured value of these service levels.		X	X	X
R-LM-18	**Vendor reports on security** The Supplier regularly reports on any security incidents, vulnerabilities and changes in the security landscape and immediately on incidents with a high risk for Conclusion.		X	X	X

Controls for services					
#	Control and explanatory notes	1	2	3	4
	The security officer concerned will be informed of these reports.				
R-LM-19	**As a rule, critical vulnerabilities are immediately communicated, mitigated and fixed within a few days of disclosure** Critical vulnerabilities that result in the disruption of services from Conclusion are immediately mitigated and resolved as quickly as possible. The exact term must be determined in the context of the service.		X	X	X
R-LM-30	**Supplier provides a Software Bill of Materials (SBOM) or answers the question within one day whether a certain software module is in use.** Supplier must indicate on which third-party software modules the service depends. Alternatively, the supplier may indicate within a day whether there is a dependency on a module that is currently under discussion.		X	X	X
R-LM-20	**Supplier provides full visibility into which data is stored where.** The storage of data must be transparent, comply with the GDPR and fit in with the processing agreements that Conclusion has concluded with others	X	X	X	X
R-LM-21	**Data may only be stored within the EU**			X	X
R-LM-22	**Supplier is transparent about the external parties to whom it may be required to hand over customer data.** Example: U.S. citizens may be required to cooperate with an investigation and hand over data. This is regardless of the location where the data is stored. Conclusion wants to have the risk of this kind of situation under control.		X	X	X
R-LM-23	**Supplier demonstrably complies with Dutch and European laws.** Including privacy legislation.	X	X	X	X
R-LM-24	**The Supplier is prepared to make evidence available if Conclusion requires it by operation of law.** If Conclusion requires forensic evidence in a judicial context, the supplier is willing to cooperate.			X	X
R-LM-25	**It must be possible to export the data.** In the case of Cloud services in which data is stored, it must be possible to extract the data from the service in a structured format (e.g. XML) (preferably automatically). This is for calamity and migration purposes.		X	X	X

Controls for services					
#	Control and explanatory notes	1	2	3	4
R-LM-26	**The exit scenario must be described before the service acquired.** Before Conclusion can acquire the service, the exit scenario must be described. In this exit scenario, it must be described how Conclusion's services can be prevented from being negatively affected by a switch to another service provider or the failure of the existing service provider.			X	X
R-LM-27	**The code and configuration behind the service must be deposited with an escrow agent.** If, due to unexpected circumstances, the supplier is no longer able to provide the service, Conclusion may be able to continue the service independently.				X
R-LM-28	**If the service forwards or stores privacy-sensitive data, a processing agreement is mandatory.** A data processing agreement (or something equivalent to it) is mandatory when forwarding or storing privacy-sensitive data.			X	X
R-LM-29	**Decreasing compliance with this set of controls or failure to meet any security related agreements that were made at the signing of the contract gives Conclusion the right to terminate the contract immediately and without additional cost.**			X	X

CONCLUSION

CONTACT
Roel Gloudemans (CSO)
security@conclusion.nl