Public

CONCLUSION

SECURITY POLICY
Conclusion Benelux

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

With the cooperation of
Chris Gralike, Ricky Hoots, Artien Bel, Dennis Pieterse, Paul Schoorl, P. Mensink, A. van der Lee, M. Baak, W. Bulte, G. Heysteeg and E. van Boxtel

Status: Final
Version: 1.5 (2025-05-09)
Best before: 2026-05-09

Version table			
Date	Version	By	Adaptation
21-09-13	0.1	R. Gloudemans	First draft
21-10-06	0.2	R. Gloudemans	Review by P. Schoorl, C. Gralike and A. Bel.
21-11-03	0.3	R. Gloudemans	Review by R. Hoots and D. Pieterse. Lessons learned from the most recent cyber exercise; addition of security incident management, security services and improvement of CSIRT control.
21-11-16	0.4	R. Gloudemans	Review P. Mensink
22-01-28	1.0	R. Gloudemans	Review A. van der Lee and M. Baak
22-03-03	1.1	R. Gloudemans	Review G. Heysteeg and E. van Boxtel. Addition of goal "proactive" including principles and performance indicators.
23-06-12	1.2	R. Gloudemans	Updated RASCI (4.4); reporting lines (2.6, ER4); On2I Adjustment of security services (6.4). Review by W. Bulte.
23-09-20	1.3	R. Gloudemans	It has been indicated that risk analyses are not only carried out annually but also after major changes. (5.2). With thanks to A. de Boer
25-11-2024	1.4	E.Aksoy	English Translation
09-05-2025	1.5	R. Gloudemans	Adaption of function titles, limiting the scope to Benelux and correcting a lot of translation errors

Approval
Version: 1.0

Approved by:

E. Verkoren – Managing Director of Conclusion

All major versions of this document are approved by the Managing Director. Minor improvements and/or adjustments are the responsibility of the Director Information Security & Privacy

*This document is classified as **public** information and can be made available (in pdf form) to anyone for whom this policy document is relevant.*

Contents

1 Executive Summary

This is the security policy for the Conclusion ecosystem. This policy should contribute to keeping the business risks associated with information processing at acceptable values.

Conclusion is an ecosystem of independent companies. This means that companies make their own choices when it comes to protecting information and keeping risks under control. The aim of this document is to move companies towards a uniform approach. In this way, information security can contribute to the presentation of a consistent image of Conclusion to the Conclusion customer. The uniform approach simplifies mutual communication and gives all companies a better picture of how we are doing. This improves the resilience of the ecosystem and makes it easier to manage at group level.

Above all, security policies should reflect who we are. As a representation of this identity, the Conclusion Manifesto has been chosen as the basis for the policy.

Chapter 2: "Introduction" is a representation of the Conclusion organization and outlines the elements of the policy.

Chapter 3: "The goals of information security" links the information security goals to the Manifesto. **Based on these goals, several mandatory principles (p. 12) are formulated**. The security policy of the companies must ensure that these goals are also achieved, among other things by meeting the principles. Several risk indicators are also linked to goals so that performance can be made transparent.

Chapter 4: "Management" deals with the responsibilities at group level and to a very small extent at company level. At group level, every company is expected to have a central role for information security; the Information Security Officer (ISO).

Chapter 5: "Information Security Process" is a representation of the process at group level and formulates the **rules for reporting**. Both at group level and from the companies to each other and the group.

The appendix contains the definitions of several terms. The most important of these are **the definition of the risk scale** (p. 28) and the **concept of "Trust"** (p. 26).

2 Introduction

2.1 Source

This policy document and underlying documents referred to in this document can be found on the "Security" page of Start Your Day.
(https://conclusionfutureit.sharepoint.com/sites/StartYourDay/SitePages/Privacy-&-Security.aspx)

2.2 Background and objective

This document describes the goals and set-up of information security within the Conclusion Benelux Ecosystem. The purpose of the information security policy is to support the mission, vision and strategy of Conclusion Benelux (hereinafter referred to as "Conclusion") and that of the individual companies. This is done by setting measurable goals that are a measure of digital resilience and are used to limit Conclusion's information risk exposure to acceptable values.

"Acceptable" is determined by the risk appetite of Conclusion Benelux.

This document is about the goals for Conclusion and the way in which the companies work together to achieve those goals. How the companies achieve these goals is the responsibility of the companies themselves.

Several other documents are available underneath, including a threat assessment. Exactly which documents these are and what the purpose is is mentioned in section 5.6.

2.3 Formation

The security policy is based on Conclusion's Manifesto. A risk-based approach has been chosen, within the framework of laws and regulations, including privacy legislation.

When drafting this and the underlying policy documents, a minimum set of norms and standards was considered, including Conclusion's privacy policy, the GDPR, ISO27001, NEN7510 and the relevant laws and regulations. Additional regulations may apply to individual companies. An overview of relevant laws and regulations can be found in the document "Relevant Laws and Regulations".

The content of this document has been prepared with the help of the Security Officers of the companies and coordinated with the management of Conclusion.

2.4 Scope

This document describes the preconditions that the companies must meet and the division of roles with regard to privacy and security at group level. How the companies implement this is up to the companies themselves.

2.5 Public

Employees who act at group level and the directors and (chief) security officers of the companies.

2.6 Organisational structure

Conclusion is an ecosystem of companies. This means that Conclusion consists of several companies that operate independently and that often seek cooperation. These companies can also consist of several companies. The lines of accountability run at board level.

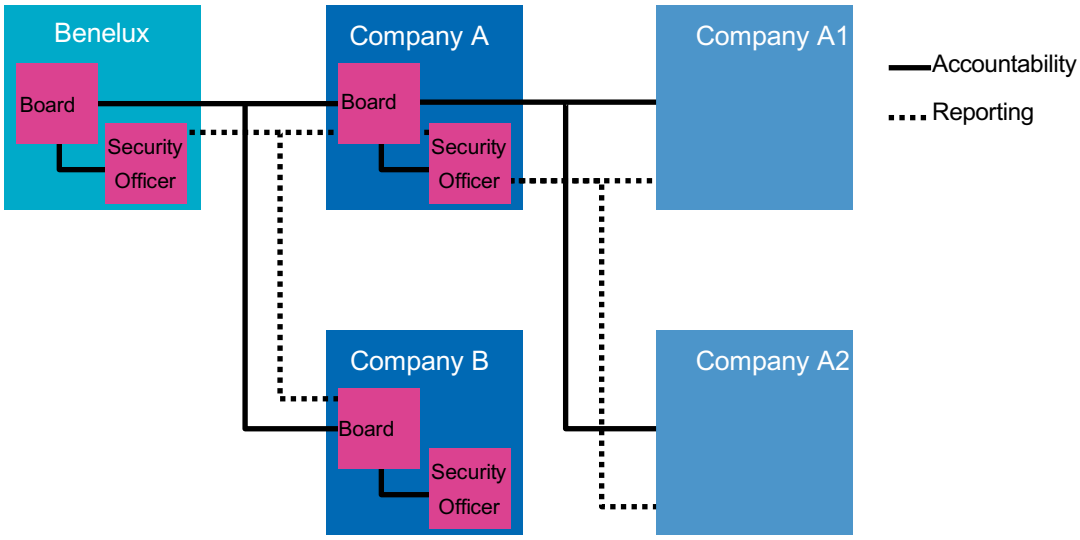

Figure 1, The Conclusion Organization

Security is an integral part of the companies' annual plans and the regular reporting to the group management on this. Based on the report, the Director for Information Security & Privacy (DS&P) will engage the individual company directors to help those companies get and/or keep their information risks under control.

Every company has a security officer who is accountable to its own management. Furthermore, there is regular contact between the security officers of the companies and the DS&P, so that information can be shared optimally and quickly.

2.7 Structure of information security

Conclusion implements information security on three levels. The information security framework is structured as follows:

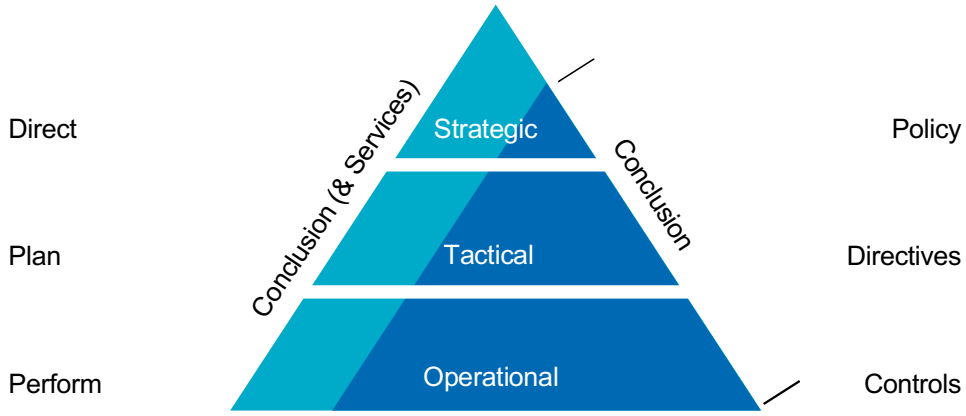

Figure 2, Information Security Framework

This involves a double pyramid. On the one hand, a (light blue) Conclusion wide pyramid that culminates in measures that apply to Conclusion Services' central services to Conclusion companies from the strategy onwards.

On the other hand, for each company there is a (dark blue) pyramid that indicates that each company is responsible for its own information security[1] that must fit into the whole of Conclusion. *Respecting the agreements in and aligning with the structure outlined in this document is an important basis for this.* Through good mutual coordination, Conclusion customers can be offered a consistent whole in terms of security. In addition, the companies also have an interdependence for their security in the form of shared services, such as the Conclusion website.

[1] The company can use its own set-up or copy the Conclusion-wide approach.

2.7.1 Strategic – Policy

At the strategic level, the policy consists of several topics:

1. Benelux Security Policy (this document); This document is aimed at directing information security. It includes the goals, basic principles, tasks and responsibilities as well as the process model, which is used at the group level for security. This document also bridges the gap to Conclusion's risk appetite.
2. Annual Information Security Plan for the group; Every year, a new plan is formulated based on the observations and events of the past year. Where necessary, the companies incorporate elements from the annual plan into their own plans.
3. Threat analysis: this analysis describes which external factors can prevent Conclusion from achieving its information security objectives. These are the threats that apply to all of Conclusion's companies. Each company must supplement this analysis with an analysis for its own context (within its own pyramid).
4. Stakeholder analysis: This document describes the context in which Conclusion operates and the various stakeholders in information security.

2.7.2 Tactical – Directives

For the tactical level, the guidelines are defined for several focus areas. An example of this is the Data Classification Directive. This guideline contains the classification framework. There are also guidelines for infrastructure and processes. The guidelines have been formulated in the most technology-neutral way possible.

The guidelines are defined based on the objectives and structure set out in this document. Where applicable, the directives should be translated into operational measures by those responsible[2].

2.7.3 Operational – Controls

How the guidelines translate into operational measures is sometimes obvious, but sometimes not. It is the task of those responsible for the assets[3] to translate these into operational measures, or to indicate why a directive is deliberately not implemented.

[2] The guidelines that have been drawn up for Conclusion Services can serve as a template for companies that wish to do so.

[3] In this context, an asset can be a process, system, application or dataset. The person responsible for the asset is normally considered to be the owner of the asset.

2.7.4 Overview of all elements

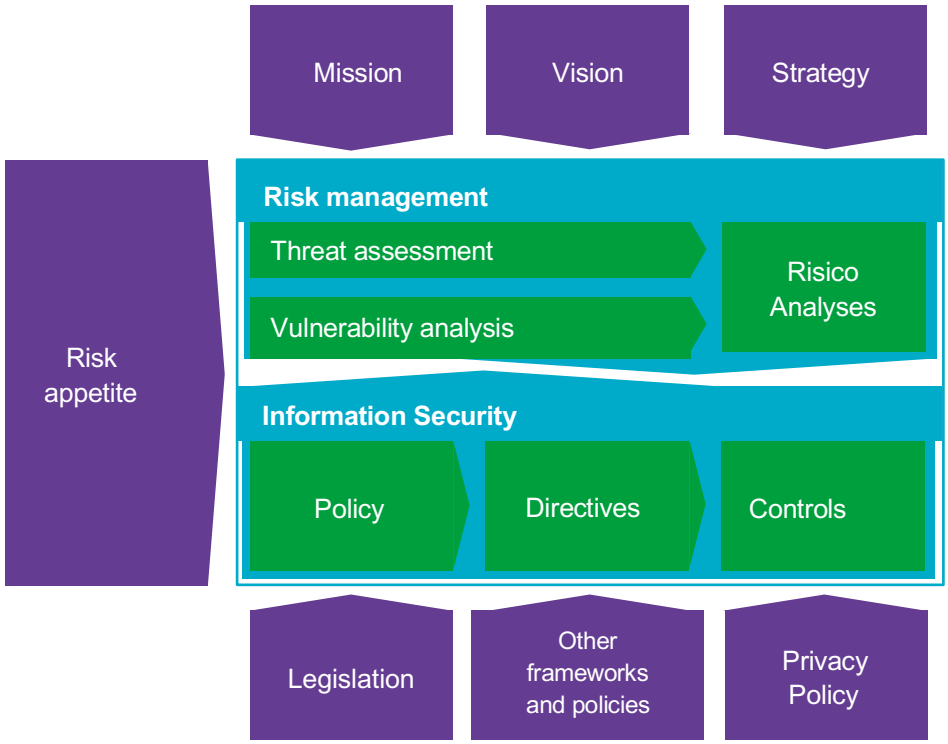

Figure 3, Connection between the elements

Conclusion's risk appetite forms the basis for both (information) risk management and information security. This is translated into policy and resources for risk management and information security using the mission, vision and strategy, in which laws, privacy and other policies are used as frameworks. Risk management and information security interact with each other. Risk-based security and security-based risks.

This results in policy documents, directives and controls, which, if followed, guarantee automatically that the actions are following the strategy and legislation.

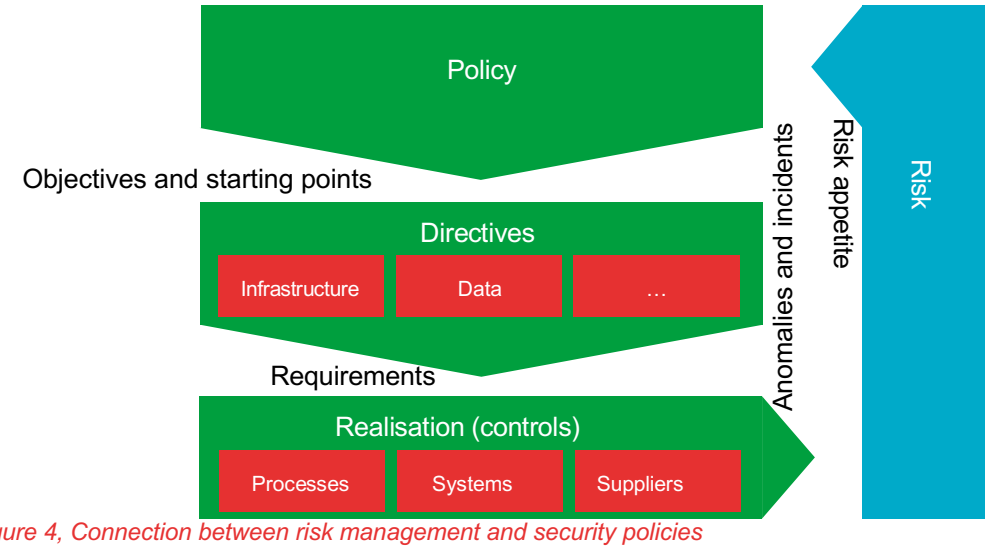

Figure 4, Connection between risk management and security policies

Risk management always takes place based on two elements:

1. The threat assessment consisting of factors that Conclusion cannot control.
2. The vulnerability analysis, in which the vulnerabilities are properties of Conclusion's processes, systems and suppliers. The basis of the vulnerability analysis is formed by the directives that have not been met, supplemented with other vulnerabilities. These other vulnerabilities can be identified, for example, based on incidents and reports.

In a risk analysis, the threat assessment and the vulnerability analysis are combined to formulate risk scenarios that have an impact on the objectives of Conclusion’s business processes.

Subsequently, it is then regularly examined whether information security needs to be adjusted based on the risk scenarios and/or changed frameworks to support Conclusion's mission, vision and strategy more effectively.

3 The objectives of information security

3.1 Structure

The objectives for information security (IS) are defined based on Conclusion's Manifesto. This Manifesto contains nine key concepts that describe the heart of Conclusion. Based on this Manifesto, eight goals for information security have been defined in three core areas. "Who we are", "What we do for our client" and "What we do for each other".

The companies are expected to contribute to achieving these goals.

For each of these eight goals, risk indicators and the basic principles of the Conclusion ecosystem were defined.

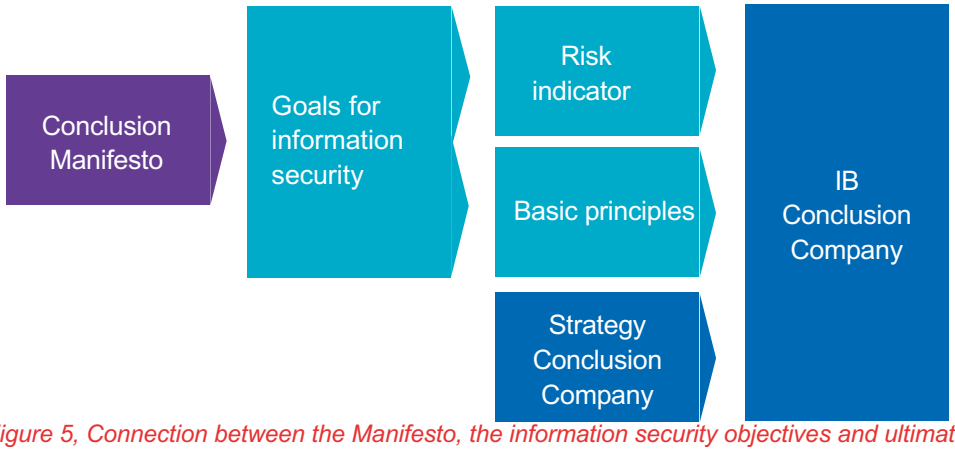

Figure 5, Connection between the Manifesto, the information security objectives and ultimately the information security of the Conclusion companies.

The risk indicators indicate on the one hand to what extent Conclusion as an ecosystem achieves its objectives and, on the other hand, the risk indicators can be used to express the risk appetite, by defining a minimum and maximum and target value for each indicator.

The Conclusion Manifesto can be found at "Start Your Day" (https://conclusionfutureit.sharepoint.com/sites/StartYourDay/SitePages/Manifesto-principes.aspx)

3.2 The objectives of Information Security

#	Objective	Explanation	*Manifesto*
Who we are			
DI1	Companies take their **OWN RISKS**	Each company takes and controls their own risks. The risk appetite of Conclusion is considered. No company constitutes an unacceptable risk to the group.	*Authenticity, Cooperation, How we treat one another*
DI2	we **TRUST** each other.	Conclusion companies must be able to trust each other. That trust is justified because we know what risks each of us takes and how we control these risks. That trust can never be imposed.	*Ecosystem, Collaboration, How we treat one another*
DI3	facilitating **RISK TAKING**	Measures to guarantee privacy and limiting risks contribute to the creation of circumstances in which we can take risks, without this having unacceptable consequences.	*Authenticity, Remaining an authority, Professionalism*
What we do for our customers			
DK1	being **PROTECTED**	Customers, employees and other persons involved are protected when they do business or interact with Conclusion. We are transparent about how we provide protection.	*How we treat customers, What we do for customers, How we treat one another*
DK2	an **EXAMPLE** for our customers	The manner in which we shape and use the risk management, privacy and information security framework is an example for (potential) customers. Our controls align with what we do and how much risk we wish to take.	*Remaining an authority, What we do for customers, Professionalism*
DK3	we are **PROACTIVE**	We do not wait for problems; we actively search for opportunities and are always prepared for what is coming.	*What we do for customers, Remaining an authority*
What we do for each other			
DE1	our organisation is **RESILIENT**	Conclusion is a resilient organisation. This means that our structure can “take a punch” and that if things do go wrong, we are able to pull ourselves together with a minimum impact on the persons involved and the stakeholders.	*Remaining an authority, How we treat customers, Professionalism*
DE2	we do things **FOR EACH OTHER**	We help each other bring our risks under control. In doing so, we make the good ideas and services relating to privacy and information security of one company available to other companies.	*How we treat one another, Professionalism, Business operations*
DE3	we **PROVIDE A FULL-SERVICE SOLUTION** for the ecosystem	Services and standards relating to controlling risks, privacy and information security are handled centrally to provide a full-service solution to the individual companies and in order prevent vulnerable seams from arising in	*Professionalism, Business operations*

3.3 Basic principles for Information Security

#	Principle
Own risks	
ER1	Each company performs at least one risk analysis each year, with the processing of information and privacy as minimal scope. Threats and vulnerabilities are addressed explicitly and the central threat matrix and central guidelines are used among other things.
ER2	Each company provides the risk analyses to the boards of all Conclusion companies. *This improves insight into the risks and places the risk appetite of the individual companies into a broader perspective.*
ER3	Each company has an explicit control framework and includes deviations therefrom as a vulnerability in the risk analyses. *This system of measures may be an own system, but the company may also use Conclusion's central system that is also used for central services or a modification thereof.*
ER4	Each company reports on privacy & security at least once per quarter. *This is an integral part of reporting to the group. In addition, information will be exchanged at the operational level between the Conclusion security officers concerning incidents with a high impact and threats.*
Trust	
Ve1	Risk reports, threats and vulnerabilities are exchanged between the companies of the Conclusion group.
Ve2	Each company carries out an internal audit of all business processes at least once every three years and once every eighteen months for companies with healthcare customers. *This frequency is in accordance with the ISO27001 and NEN7510 requirements. The best practice is to set up a regular audit schedule in which connection a part/process of the organisation is audited every few months.*
Ve3	Audit reports are shared between the boards of the companies of the Conclusion group.
Risk Taking	
Le1	Significant (privacy) risks are always mitigated in to maintain scope for assuming new risks.
Protected ***(note: all principles contribute to "protected")***	
Be1	We comply with laws and regulations ... (comply or explain)
Be2	All companies have their business operations in order to such a degree that ISO27001 or NEN7510 certification can be achieved without much effort.
Example	
Vo1	Each company has laid down its processes in a clear manner, including process objectives, frameworks and RASCI. *Documentation will be made available to help do this in an efficient manner and to ensure that the result contributes to employees' insight into the organisation and their insight into the risks inherent in the process.*
Vo2	Each company has an explicit improvement process

#	Principle
Vo3	Each company is willing to share its information security policy with other Conclusion companies, customers and suppliers. *This is how we build trust among our customers and allows us to communicate more easily with each other, customers and suppliers concerning the measures we have to take together. Note: it is recommended to classify the implemented controls as confidential information.*
Proactive	
Pr1	We talk to our customers about the threats they perceive *Threats to our customers are also threats to our own business operations. That is why we talk on a regular basis to exchange threat information. We recalibrate our own risks based on knowledge gained.*
Pr2	We continuously monitor our vulnerabilities and resolve them as soon as possible if possible. *Vulnerabilities are assessed at least once per year as part of the risk analyses, and the creation of new vulnerabilities at the technical and organisational level is monitored continuously. Vulnerabilities that have arisen recently are considered as soon as possible. We encourage employees to report vulnerabilities identified by them within their own organisation.*
***Resilient** (note: all principles contribute to "resilient")*	
We1	Only explicit and context-dependent trust. *The decision to trust an entity is always an explicit choice. This decision is substantiated with arguments that are commercial and/or business-related in nature. We attempt to prevent the inheritance of trust (such as not trusting the supplier of a supplier automatically) as much as possible. Furthermore, trust is always binary. If we trust an entity, there are no additional controls in addition to the reason for the trust. In such cases, we have the legitimate expectation that everything is already in order within this entity.*
We2	Privacy & security is everyone's responsibility, both at group level and within the companies.
We3	Each company has someone who is responsible for formulating and monitoring compliance with privacy and security policy. This role has a direct reporting line to the company's board. The person who holds this role is usually referred to as the Information Security Officer (ISO) or Privacy Officer (PO)
We4	Each company formulates an annual privacy & security plan.
We5	All privacy & security incidents that have a major impact or incidents that must be reported to the Dutch Data Protection Authority are reported to the DS&P.
We6	Incidents that endanger the services provided to customers or that are related to identified strategic risks are reported to the DS&P. *Conclusion has an overarching security incident management process for this purpose. This process aligns with the companies' local processes.*
We7	All employees of a company are demonstrably skilled in the area of privacy & security with respect to the context in which they work.
For each other	
VE1	Each company cooperates in the Conclusion security officer's guild (CSOG).
Providing a full-service solution	
On1	For each central service that is not purchased, the reasons must be formulated. *For the purpose of supporting the improvement process for central services.*

#	Principle
On2	In case of a Cyber Emergency, each company is required to inform the DS&P so that assistance may be engaged. This may be a Conclusion or an external CSIRT team. *The focus of a CSIRT team is to resume operations as soon as possible with respect for forensic evidence that may be used in the analysis of the incident and the possible prosecution of the offender.*

3.4 Risk indicator

#	Risico Indicator
	Eigen Risico's
PI1	Percentage (%) of companies with a recent (privacy) risk report
PI2	% of companies with defined Privacy & Security risk indicators
PI3	% of companies with a defined risk appetite
	Trust
PI4	% of companies sharing risk reporting
PI5	% of companies with a recent internal or external audit report
PI6	% of companies sharing audit reports
	Courage
PI7	Number (#) of missed deals or deals we have missed due to us, risk, privacy, security of compliance landschap
PI8	# unmitigated high risks and important audit findings (total in the group)
	Protected
PI5	*% of companies with a recent internal or external audit report*
PI8	*# unmitigated high risks and important audit findings (total in the group)*
PI9	% of companies with at least 1 certification in the field of privacy or security
PI10	# of data breaches in the past year (total in the group)
	Example
PI10	*# of data breaches in the past year*
PI11	% of companies using the policy templates
PI12	# presentations for clients on the set-up of the Conclusion framework in the past year
	Proactive
PI12	# conversations about the threat landscape with customers
PI13	% of companies with their own infrastructure that have set up technical vulnerability monitoring for the entire production landscape
PI14	% companies with an explicit improvement process; where all employees can report improvements.
	Resilient
PI15	% of companies with a written and shared process landscape
PI16	% of companies that do the risk analysis at business process level
PI17	% of employees who have successfully participated in the awareness trainings
PI18	# security incidents where service was compromised
	For each other
PI15	*% of companies with a written and shared process landscape*
PI19	% templates that are up-to-date and adapted to what the companies want

PI20# internal audits that the companies have carried out on each other

Providing a full-service solution

PI19 % of templates that are up-to-date and adapted to what the companies want

PI21 average % of companies using a security service

PI22# well-defined security services

4 Management

Conclusion's CEO is accountable for the information security of the ecosystem. The boards of the companies, including Conclusion Services, are accountable for the policy of their own companies. Tactical and operational responsibilities are delegated within the companies. The roles and responsibilities are summarised in a matrix at the end of this chapter in section 4.4.

4.1 Control of information security

Control of information security comprises several tasks. Firstly, the definition and formulation of the information security policy for the ecosystem and derived guidelines for the management of the common service provision. This is the ultimate responsibility of the Managing Director, with the Director Information Security & Privacy (DS&P) being responsible for setting the policies, guidelines and monitoring over them. The DS&P is obliged to do this as much as possible in consultation with the companies.

The directors of the companies are responsible for the implementation of the ecosystem's policies and the definition and implementation of the policies of the companies under their care. This is assisted by the DS&P and its own security officer(s) who fulfil both an advisory and a monitoring role.

Any strategic risks must be reported to Conclusion's Chief Securities Officer.

Conclusion's Data Protection Officer contributes to the management of information security by providing a privacy policy that gives direction to the information security policy.

4.2 Implementation of information security

Every employee has a role to play in the implementation of information security, with the directors and those to whom they delegate the tasks related to security.

The DS&P's task is to ensure that the directors of the companies, the employees and all other relevant stakeholders are aware of the policies of the ecosystem, the guidelines used to implement the shared service. The DS&P will help the internal service providers to apply the guidelines.

The directors, with the help of their security officers, must ensure that the risks within their companies do not exceed the risk appetite, and that the policies and implementation within the company are compatible with the group policy. To demonstrate this, reports are made on a regular basis.

The Data Protection Officer will act in an advisory role with respect to privacy-related issues.

4.3 Protection of Privacy & Security Officers

Privacy & Security officers must be able to report what they observe in accordance with the reporting lines set out in this document without endangering their own position in the company.

1.2 RASCI-matrix

(R) responsible for the implementation;
(A) ultimately responsible and therefore acceptor;
(S) may be supportive/cooperative;
(C) is consulted (mandatory);
(I) shall always be informed of the outcome

	Managing Director	Board Benelux	DS&P/PO	Data Protection Officer.	Company Director	ISO/PO company
Central control						
Information Security Policy Benelux	A	I	R	C/S	I	C/I
Formulation of guidelines	A	C/I	R	C/I	I	C/S
Policy Implementation	A	C/I	R	C/I	I	I
Reporting to management	I	I	A/R	C/S	I	I
Risk management process	A	R[4]/I	C/I	C/I	I	I
Privacy Policy Conclusion broad	A	I	C/I	R	I	I
Inzet Computer Security Incident Reponse Team	A	I	R	I	I	C[5]
Appoint coordinator CSIRT (per incident)	A	R[4]	C/I	I	I	C/I[5]
Management within the companies						
Information Security Policy	I	I	I	I	A	R
Formulation of guidelines			S/I	S/I	A	R
Policy Implementation			S/I	S/I	A/R	C/I
Reporting to your own management			I	I	A	R/I
Risk management process			I	I	A/R	C/I
Risks at the heart of the company and within the companies						
Acceptance of strategic information risks	A	R	C/I		R[6]	C/I
Acceptance of tactical information risks		I	I		A/R	C/I
Acceptance of operational information risks					A/R	C/I
Implementation is key						
Security Architectuur Conclusion Services			A/R	C/I		C/I
Unburdening security services (see also 4.4.3)	S/I	A[4]	R	C	C/I	C/I
Processing register		A[4]	I	R		
Processing agreements		A/R	C/I			I
Implementation locally						
Processing register			I	I		A/R
Processing agreements			I	I	A/R	C/I
Reporting disruptive incidents to the DS&P (see also 4.4.4)			C/I		A	R

[4] CFO

[5] From the company concerned

[6] Information Security Officers inform each other about their reports

4.3.1 Computer Security Incident Response Team (CSIRT)

The Computer Security Incident Response Team (CSIRT) is a crisis organisation targeted at getting back in control. Conclusion does not have it's own CSIRT, but relies on external vendors. The CSIRT team can be invoked via the cyber security insurance policy. The DS&P and the Director Legal have information on the policy. The phone number is listed in the calamity plan.

The task of the CSIRT is to overcome imminent serious impact on the primary processes after a cyber calamity and/or to restore the primary processes as quickly as possible. During the work, the CSIRT can temporarily take over the role of "asset owner" within any Conclusion company, to be able to act quickly and decisively.

This means that if the emergency is still in force, the CSIRT determines what happens to the affected systems, processes and services.

After remedial work because of an incident that has severely disrupted the primary processes:

- the coordinator of the CSIRT (by default the DS&P, unless otherwise agreed) for that incident) shall be accountable for the actions taken to the directors concerned.
- have the DS&P have the CSIRT perform a root-cause analysis.

4.3.2 Internal Auditor

The role of the internal auditor is to check that the state and operation of information security is in order and that processes and measures function as described.

The auditor reports periodically and directly to the director and ISO of the Conclusion company in question. Regarding this report, the auditor enjoys a protected position. She/he must be able to report freely, without jeopardizing the auditor's position in the company.

The internal audit role is typically a supporting role for an employee. A precondition for this is that an internal auditor may never carry out an audit within his or her own management/staff department.

It is encouraged that the Conclusion companies carry out each other's internal audits in order to learn from each other.

4.3.3 Commodity security services

Setting up a good security landscape requires customization. The building blocks with which the customization is built are often standard. That is why Conclusion Services offers several standard services, which are either supplied to all companies, or are available on request.

Examples of this are the monthly Internet scan, the password manager and the security monitoring of frequently used suppliers. These services are managed by the DS&P. The DS&P is responsible for continuously mapping out the needs of the companies and ensuring that the central security services meet the needs of the companies on the one hand and the risk appetite of the group on the other.

4.3.4 Incident management

Incidents that may pose a threat to the continuity of services and/or primary processes must always be reported by the security officer to the DS&P as soon as possible via https://conclusion.inbisco.nl/IRIS. The DS&P can then determine whether the incident also poses a danger to the other companies within the ecosystem, or whether the use of the CSIRT is necessary.

The incident can only be closed when the source cause is clear and when any necessary improvements have been accepted and planned.

Incidents at customers: The handling of this is part of the normal service/business processes. *If the incident could potentially spread to Conclusion, or if it could potentially lead to reputational damage for Conclusion, the DS&P must be informed by the security officer via https://conclusion.inbisco.nl/IRIS*.

Incidents at suppliers; See customer incident handling.

5 Information Security Process

5.1 The life cycle

Conclusion sees information security as a continuous process and emphatically not as a one-off activity.

The starting point of the process is the Manifesto and the information security objectives, risk indicators and basic principles linked to it. This is the basis for the cybersecurity chapter in the annual risk assessment and analysis. The result of this analysis is included:

- determining/recalibrating the right goals and basic principles;
- the annual security plan with the security activities to be undertaken;
- determining/recalibrating the guidelines for the common service provision.

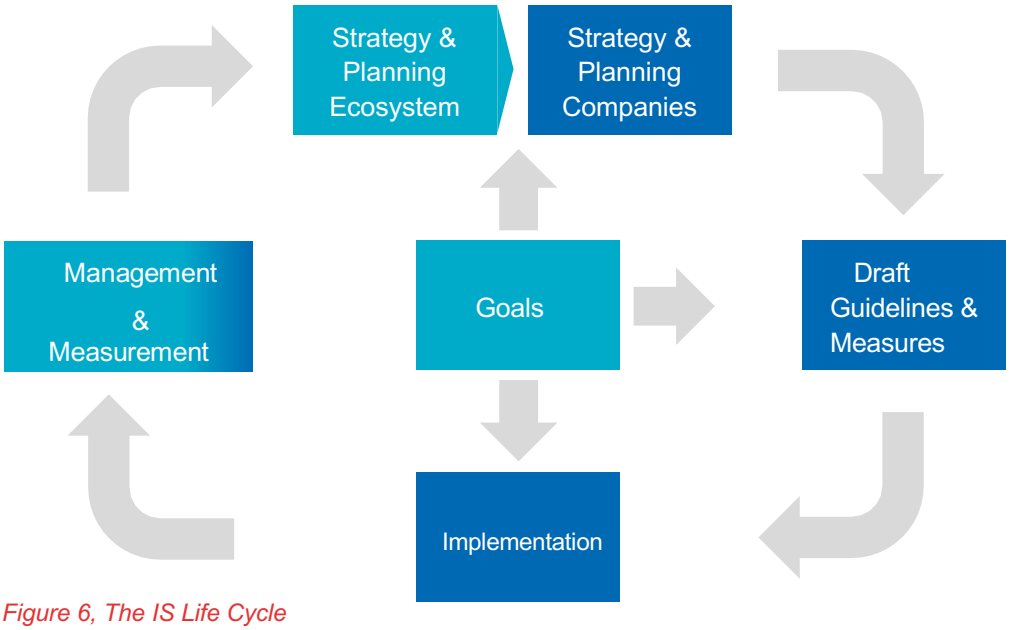

Figure 6, The IS Life Cycle

5.2 Risk analyses

A strategic risk assessment at ecosystem level is performed annually. Every year, a risk inventory and analysis are made at ecosystem level. As far as the information/cyber part is concerned, it is fed by the risk analyses of the individual companies. These risk analyses must include both the context of the companies (security) and that of the data subject (privacy). Because the companies share relevant threats and vulnerabilities with each other, the impact that the companies have on each other also becomes visible.

The risk analyses should take place on the business processes, so that a risk is always linked to a business goal. Failure to comply with guidelines, measures and (legal) frameworks must be explicitly included as a vulnerability. The risk analysis must also be updated for every major process change.

The DS&P may (mandatorily) advise to carry out a risk analysis at an earlier than the regular time, if he/she believes that the risk exceeds the willingness.

5.3 Reporting

The DS&P will draw up a report for the Conclusion board at least once every 4 months[7]. This report is compiled on the basis of the reports issued by individual companies, status of the performance of the annual plan, plus any observations on part of the DS&P.

[7] The reporting months are typical: February, June and October. In special circumstances, more frequent reporting will take place.

The report contains at least the following subjects:

1. notable incidents within Conclusion and other matters;
2. the status of the central security plan;
3. values of the risk indicators;
4. the most important risks.

This report is available for inspection by the directors of the Conclusion companies and the Information Security Officers.

5.4 Revision intervals

The DS&P uses the following lifecycle for the following policy documents:

- The set of policy documents is reviewed at least once every 3 years;
- reporting to the management on the implementation of the security plan takes place once a quarter;
- Reporting to the management on the risk indicators takes place once a quarter place;
- the tactical guidelines are reviewed at least once a year (for the purpose of the central service);
- Risk analyses of the processes for the central services must take place at least annually and/or after major changes in the process.

All documents are provided by the DS&P, except for the risk analyses which are the responsibility of the process owners.

5.5 Verification of the implementation of controls

Conclusion Benelux is responsible for internal control of the implementation of the policy, guidelines and measures. These checks are part of the regular processes as much as possible. In consultation with or on the initiative of the DS&P, a so-called special internal audit or external audit can be carried out at all of Conclusion's companies. The DS&P supervises the implementation of this.

The Conclusion companies themselves are responsible for monitoring the operation of the measures they have put in place. The results of audits should also be made available to the DS&P of Conclusion.

5.6 Approval of documents for policy and guidelines

There is a set of guidelines under this policy. The guidelines are specific to certain goals and can be adjusted regularly based on advancing insight. The guidelines apply to the central service provision, must be used for the identification of vulnerabilities in risk analyses and have been drawn up in such a way that the Conclusion companies can, if they wish, use this documentation as a template for their internal security.

Before the policy for the ecosystem is established, all security officers and company directors are given the opportunity to review the document, after which the adoption is made by the general manager of Conclusion.

The guidelines documents are approved by the DS&P, with the condition that the documents have been reviewed by at least four other security officers of the Conclusion companies and that the comments have been satisfactorily processed. Progressive insight is incorporated into the guidelines documents as soon as possible.

Minor changes to the documents are the responsibility of the DS&P of Conclusion.

All policies and guidelines, documentation are classified as public information and may be distributed to stakeholders in PDF form.

6 Appendices

6.1 Definitions

6.1.1 Availability (continuity, response time).
The extent to which information systems and the information within the organization are in operation at the time a user needs information.

6.1.2 Integrity (correctness, completeness, timeliness, permissibility).
The extent to which the information within the information systems is complete and accurate. Completeness should also be understood to mean that no more than the necessary information is included in the system.

6.1.3 Confidentiality (exclusivity).
The extent to which access to and acquaintance with the information is limited to a defined group of users, all of whom have declared in writing that they will handle the information systems, and the information contained therein in a correct and careful manner.

6.1.4 Cyber emergency
Event in which an external actor manages to gain control of part of the Conclusion infrastructure. This is the case, for example, of Malware, such as a cryptolocker.

6.1.5 Cyber Security
That part of information security that is about the protection of information that is accessible by digital means. Cybersecurity is therefore a subfield of information security.

6.1.6 Security incident
Any incident that jeopardizes the continuity of the service or the organization. This includes not only incidents relating to the reliability and accuracy (integrity) of information, but also its availability.

6.1.7 Resilience
The ultimate purpose of this policy, to keep the information risks associated with Conclusion's processes within acceptable limits, is highly dependent on the recognition of risks.

The fact is that not all risks are recognized. That is why it is important to focus on digital resilience in the measures. Digital resilience is the organization's ability to respond to unforeseen events.

Resilience			
	People	Process	Technology
Prevention Limiting			
Impact			
Know what's happening Ability			
to react quickly			

To achieve this, measures are needed in terms of people, process and technology, and these measures should not only focus on prevention, but also on limiting the impact when things go wrong, disseminating information, so that it is clear what the expectations are

and so that exceptions can be detected and to be able to respond quickly to events.

6.2 Elaboration of the concept of trust

In basic principle We1 it is stated "Only explicit and context-dependent trust". This section outlines some of the characteristics of trust in the information security context.
These characteristics are decisive in the discussion and application of the concept of trust in the underlying guidelines and the modelling of trust in architecture.

6.2.1 Trust is binary

Trust is a binary concept. Something is or something is not familiar. By default, nothing is trusted. Only after evaluation, for example of implemented measures, can a decision be made to trust something. This trust should be re-evaluated periodically.

Taking measures does not automatically mean that something can be trusted. Border control does not mean that everyone within the country's borders is trusted. In that case, the status is "not trusted, but checked".

If information is transported from a trusted to a non-trusted context, or between untrusted contexts, there must always be a control/measure at the time of transition.

6.2.2 Trust is context-dependent

The concept of trust can be applied in the following contexts, among others:

Persons
Within Conclusion, people are trusted for their role in the business processes for which they are deployed. A person can be an employee or an external person in this regard. The employee or external party in question is not trusted with data from business processes in which he/she has no role. This principle therefore gives rise to a "least privilege" policy in the field of employees.

Organizations
External organisations are never trusted, unless there is an agreement and associated measures that make trust possible. This agreement should make it clear that the interests of the parties overlap sufficiently, and measures should be in place to check whether the trust is justified (e.g. audits).

A data processing agreement is an example of such an agreement, in which an organization is trusted for a certain dataset. This means that the basis of this trust must be checked.

Infrastructure
Infrastructure can be trusted when:

- Measures have been implemented to enforce that trust;
- only components managed by Conclusion can be found in that infrastructure, which means that Conclusion is 100% in control of this infrastructure.

If these two rules are not met, it is still possible to choose to trust an infrastructure, for example if it is managed by a trusted party and agreements have been made about the management of this infrastructure

Data sources
Data in a trusted data source is taken for granted. The content of trusted data sources is regulated through established and measurable processes.

If these conditions are absent, then:

- It may be that the data from this source needs to be verified in a different way

before it can be used in the Conclusion's business processes;
- data from a trusted data source may not be transferred to this data source exported. This depends on the confidentiality and integrity requirements of the information in the trusted data source.

Hereditability
Trust is inherited by nature. For example, if Conclusion chooses to trust a supplier, then the supplier's suppliers are also trusted in this context.

Conclusion takes an explicit and context-dependent approach to trust. Conclusion only allows a direct connection between two entities when they have the same trust status. In this way, inheritance is avoided as much as possible.

Conclusion applies compartmentalisation in the areas of infrastructure, application, data and physical landscape in order to give substance to this.

Example: An employee is not allowed to connect an untrusted Bring Your Own laptop to a trusted network. Otherwise, the laptop would inherit the trusted status. That is why there is a separate network compartment that is not trusted, but where additional measures are taken to enable working against acceptable risks.

6.2.3 Consequences of the concept of "Trust"

The correct application of the concept of trust leads to lighter, more workable and therefore cheaper measures in exchange for reduced control.

The concept of trust has the following implications:
- In all architectures and information flows, it must be indicated in which context of trust the processing or processing is carried out;
- In all procurement processes, the desired and ultimate trust status of to be declared to the supplier.

Mutual trust means that after establishing that an entity is trusted (identification), no additional controls are needed in addition to those already in place.

Example; An employee identifies himself at the front door. There, it is determined that the employee is a trusted entity. The employee is then allowed to move freely in the building within the context of the generally accessible areas. Additional measures are taken for a visitor in this context (e.g. that the visitor must be accompanied).

Summary of the mentioned consequences of this principle:
- Least privilege;
- compartimentation;
- without agreement and measures with another party, there is no trust;
- preconditions for the exchange of data;
- Trust must be made explicit.

6.3 Risk clasification

This policy prescribes a risk-based approach. Taking risks enables Conclusion to realise services at an acceptable cost in the relatively short term.

To ensure that the risk appetite is not exceeded uncontrollably, risks must be classified so that it is clear who is allowed to decide on taking a risk.

Conclusion refers to:
- Strategic risks and the impact of these risks:
    - jeopardize Conclusion's long-term planning, identity and strategic

objectives;
    - jeopardise the continuity of Conclusion Benelux;
    - critical services are unavailable for an extended period of time.
- Tactical or project risks such as:
    - the impact of the risks has a detrimental effect on Conclusion's (critical) services, where there are no alternatives in the short term.
    - when it concerns the execution of a project, or a single customer Impact remains limited within a Conclusion company.
- Operational risks, when the impact on service provision is limited.

The decision to take strategic risks is always a matter for Conclusion's management. Directors of Conclusion companies are free to take tactical and operational risks. Within the context of the Conclusion company, a different risk rating scale can be used. For example, in the context of a single Conclusion company, a Conclusion-wide tactical risk may be strategic.

6.4 Implementation and setting up security within the Conclusion companies

Conclusion consists of a large collection of companies with different sizes and risk exposures. Some companies, with a high-risk exposure, have a good overview of the business processes, an extensive system of measures in place and one or more security officers.

Other companies rely on the Conclusion Services organisation for a very large part of their information and business processes and only have one or two of their own business processes, such as sales and recruitment.

The bulk of businesses fall somewhere between these two extremes.

To help these companies keep information risks under control, there is the **Security Copilot** (SeC) service. This service is adapted to the needs of the company.

When a company has outsourced as many supporting processes as possible to Conclusion services, the time commitment will be much less than in the case that the company keeps the supporting processes in its own hands. In the first case, it will even be possible to join the certification of Conclusion Services, which can save on audit costs and effort.

The framework of measures and methods of Conclusion Services is used for the implementation. These do not have to be drawn up by the purchasing companies themselves.

The service is offered at cost price, with the aim of staffing as much as possible with its own staff.

Please note: *the ultimate accountability for the information security of the company is not transferred to Conclusion Services. The management of these companies must therefore continue to focus on the results that must be delivered by Conclusion Services.*

6.4.1 RASCI matrix SeC services

	Director Company	Process-owner	Security Co-Pilot
Information Security Policy	A	I	R
Formulation of guidelines	A	I	R
Policy Implementation	A	For discussion	
Reporting to your own management	A	C/I	R
Risk management process	A/R	I	R
Making risk analyses	A	R	C/S
Risks at the heart of the company and within the companies			
Acceptance of strategic information risks	R	C/I	C/I
Acceptance of tactical information risks	A/R	C/I	C/I
Acceptance of operational information risks	A	R	C/I
Implementation locally			
Processing register			A/R
Processing agreements	A	R	C/I
Reporting disruptive incidents to the DS&P (see also 4.4.4)	A		R

CONCLUSION

CONTACT
Roel Gloudemans
Director Information Security & Privacy
roel.gloudemans@conclusion.nl
+31-6-13372217