CERT insurance sector covenant

2017

DUTCH ASSOCIATION OF INSURERS

Agreement between Affiliated insurers in respect of a cooperation and the Computer Emergency Response Team for the Dutch insurance sector (i-CERT)

Considering that:

- insurers are increasingly faced with (new) threats and risks associated with the growing digitization of both society and their own internal business processes;
- insurers are part of, and to a large extent dependent on, a broader IT-supply chain environment that is fragmented and complex, and in which the central management of information security is more or less absent;
- insurers in this supply chain environment are and remain responsible for a great many, and diverse, types of (privacy-sensitive) information, as well as for adequate and continuous service provision to consumers;
- a review and analysis of data exchange and the sector's IT-landscape show that insurers are relatively vulnerable to (the consequences of) digital violations and data leakage;
- cyber incidents cause major business damage (disruption, advice, recovery, penalties, etc.) and can also lead to significant reputational damage;
- a viable, fast, operational cooperation and mutual sharing of information are necessary in order to improve the digital resilience of insurers and manage the aforementioned risks;
- insurers can in this way achieve considerable synergies in the (non-competitive) areas of cyber security, and better manage the rapidly rising costs associated with the requisite security measures and solutions;
- insurers have therefore decided, through the Board of the Verbond van Verzekeraars (Dutch Association of Insurers), to establish a cooperation and a sectoral Computer Emergency Response Team (CERT), on the basis of a feasibility study conducted for this purpose (see circular LV-2015-40 — Dutch only);
- on 15 December 2016, the Board agreed to set out this operational cooperation in this covenant, and to put in place the conditions for evolving towards a more mature CERT model;
- by means of this CERT as a single point of contact within the industry, insurers can also make use of the products & services of the National Cyber Security Center (NCSC), and receive relevant information from other sectoral CERTs.

1 Definitions

In this covenant shall be understood by:

i-CERT	[insurance-CERT] the central service within the insurance sector, which continuously informs and advises Affiliated insurers on digital threats, vulnerabilities and incidents. The i-CERT also acts as a single point of contact for insurers, and a channel for operational cooperation and information exchange with partner organizations outside the sector.
Affiliated Insurer	Any insurer or insurance group that has signed up to this covenant and who, provided the conditions here described are met, may make use of the i-CERT service.
Contact Point	The department or employee of an Affiliated insurer designated to maintain operational communication with the i-CERT.
Participant	An Affiliated insurer that complies with the criteria set out in Article 2.2.3 and is therefore deemed able to perform in their turn the i-CERT service. Affiliates who also qualify as 'Participants' have additional rights and obligations within this cooperation.
Active Participant	A Participant who, in accordance with the established rotation model, its turn is to carry out the i-CERT tasks described in Articles 3 and 7.1.
Partner Organisation	The NCSC, another sectoral CERT, or any other organization outside the insurance sector with which the i-CERT has made a collaborative agreement.
Internal SOC	[Security Operations Center] the specialized department *within* the organization of an Affiliated insurer that monitors and/or acts on incidents, by means of, amongst other things, (real-time) monitoring, detection and analysis of the digital environment.
Internal CERT	The CERT (or CSIRT - Computer Security & Incident Response Team) *within* the organization of an Affiliated insurer.
Trade Association	Any representative association of private insurers in the Netherlands.
Chain Party	Any external party with which an Affiliated insurer maintains a business relationship and exchanges digital data — such as suppliers, intermediaries, platforms, medical advisers, etc.
Supervisory Body	Any supervisory authority with which an Affiliated insurer might have to deal.

2 General

2.1 Objectives

2.1.1 Affiliated insurers together aim with this covenant:

a) to enhance their digital resilience;
b) manage damage caused by information security incidents;
c) slow down the rising costs generally associated with cyber security (to stimulate cost-efficiency);
d) improve information security in the supply chain;
e) increase the confidence of clients and stakeholders within the sector.

2.2 Cooperation

2.2.1 Affiliated insurers will work together in accordance with this covenant to facilitate the i-CERT service. In addition, they may, on the basis of this covenant, develop other joint activities that contribute to the objectives.

2.2.2 The establishment, support and execution of the i-CERT service takes place primarily through, and as the responsibility of, Affiliated insurers who meet the criteria to be deemed a Participant.

2.2.3 An Affiliated insurer is also considered a Participant if they:

a) are a member of the Dutch Association of Insurers (hereafter 'the Association'), or of any other trade association that subscribes to the contents of this covenant for its members;
b) According to the data held by the Centrum voor Verzekeringsstatistiek (Center for Insurance Statistics — CVS), belong to a concern that represents a share of 5% or more of the total Dutch insurance market;
c) has an internal CERT and/or SOC, or a department with a similar role;
d) can reasonably comply with the obligations set forth in this covenant and shows no compelling evidence to the contrary.

2.2.4 The Participants jointly, on a rotation basis, will carry out the intended services provided by the i-CERT as referred to in Article 3.1.

2.2.5 All Affiliated insurers, and expressly including insurers who do not qualify as a Participant, will cooperate as required to ensure the effective implementation of the i-CERT service.

2.2.6 The Participants, individually and collectively, actively commit to:

a) further development and professionalisation of the i-CERT service;
b) establishing collaborations with partner organisations that will further develop the available information and effectiveness of the i-CERT.

2.2.7 An insurer who complies with the criteria set out in Article 2.2.3 may only join the cooperation as a Participant.

2.2.8 For management and operation of the i-CERT, the policy framework and objectives set out by the Association at sector level are leading.

3 Tasks

3.1 Services

3.1.1 The i-CERT service has, as a minimum, the following tasks:

a) continuously collect and receive information regarding incidents that are (potentially) relevant to insurers;
b) continuously collect and receive what are for insurers (potentially) *current and urgent* vulnerabilities, threats or Indicators of Compromise;
c) the (proactive and targeted) sharing of this information with Affiliated insurers and Partner Organizations for whom it is (potentially) relevant;
d) pro-actively identify incidents concurrently affecting multiple Affiliated insurers and, if desired by the parties concerned, in such cases coordinating joint actions;
e) developing and offering *situational awareness* in the sector and the supply chain environment;
f) monitoring and sharing of market-specific know-how in the field of cyber security.

3.1.2 In addition to the above tasks, the i-CERT is also free to carry out the following tasks:

a) provide business perspectives and/or advice on the handling of incidents;
b) signal more general (non-urgent) common vulnerabilities and provide solutions to these.

3.1.3 Explicitly excluded from the i-CERT services are:

a) providing capacity for assistance in the solving of and/or dealing with specific security incidents. This is and remains the sole responsibility of each Affiliated insurer;
b) reporting any data leaks and/or IT incidents under the relevant legislation;
c) establishing or maintaining contact with Supervisory Bodies;
d) establishing or maintaining contact with supply chain parties in response to information received. Following coordination by the i-CERT as under Article 3.1.1 (d), such action may — only with the consent of the other parties involved — be assigned to the Active Participant, on condition that they themselves have a business relationship with the supply chain party and the issue needs to be resolved in that role.

3.2 Accessibility, response times and working language

3.2.1 For Affiliated insurers and Partner Organizations, the i-CERT is, within the scope of the tasks under Article 3.1.1, routinely available during office hours (Mondays to Fridays from 9am to 5.30pm, except public holidays, by telephone or e-mail).

3.2.2 The i-CERT will usually respond to messages received by e-mail within one business day. This stands separate from the various terms for processing received information (see Article 7.1.5 below).

3.2.3 Only within the scope of Article 3.1.1 (a) and (b), and only in the case of incidents that in the opinion of the notifying party have a high priority, is the i-CERT also available and operational outside office hours (24 hours a day, 7 days a week, 365 days a year, by phone only).

3.2.4 Operational communication by and with the i-CERT — insofar as it falls within the scope of the above-mentioned services — always takes place in English. Other languages are in principle not responded to. More general communication about, for example, the activities and administration of the i-CERT can also be carried out in Dutch.

4 Other collaborative projects and activities

4.1.1 The Affiliated insurers will strive to develop, on a registration basis, other joint activities that are not directly related to the implementation of the i-CERT, but nevertheless contribute to the objectives of this covenant as set out in Article 2.1.1. In this context, this might include:

a) joint purchase of security services or products, with due observance of competition law;
b) organization and/or development of awareness activities;
c) organization of workshops and training courses to enhance the knowledge and expertise of (IT) security staff;
d) organization of *cyber resilience* exercises;
e) participation in incident simulations and exercises at a national level (NCSC).

5 Rights

5.1 Affiliated insurers

5.1.1 All Affiliated insurers:

a) may use i-CERT services as described in Article 3;
b) will be informed in good time of any (planned) projects or activities undertaken by the Steering Committee of this Covenant under Article 4, and be given the opportunity to participate in them;
c) may, via the Operational Consultation Group, make proposals to improve the i-CERT service;
d) may, via the Steering Committee, make proposals for projects or activities within the framework of Article 4.

5.2 Participants

5.2.1 In addition to that outlined in Article 5.1.1, all Affiliated insurers who also qualify as Participants:

a) are authorized, via the Steering Committee and in accordance with Article 8.1, to decide on the implementation, development and management of the i-CERT service;
b) are authorized via the Steering Committee to initiate projects and activities within the scope of Article 4, and to set (pre-) conditions for them;
c) will have, only in the event that the i-CERT is aware of critical information of interest to multiple insurers, priority in accordance with Article 3.1.1. (c).

6 Responsibilities

6.1 Affiliated insurers

6.1.1 All Affiliated insurers will:

a) provide information to the i-CERT about any internally known incidents that may be relevant to other insurers as quickly and comprehensively as possible;
b) provide information to the i-CERT on *current and urgent* vulnerabilities, threats and Indicators of Compromise that are (potentially) relevant to other insurers as quickly and comprehensively as possible;
c) ensure that any information supplied to them by i-CERT is not price- or competition law-sensitive (e.g. business-sensitive data, details about insurance products or prices, etc);
d) ensure information provided to the i-CERT contains only facts and no personal details;
e) notify people internally of the department or employee who, as Sole Point of Contact, will carry out all operational communications with the i-CERT. This role should preferably be given to the internal SOC/CERT;
f) provide the i-CERT with technical data about their own IT landscape, including in-use domain names, URLs, IP addresses/ranges, and any AS numbers;
g) provide the i-CERT with up-to-date contact details of their Point of Contact, including at least one (default) email address and phone number;
h) ensure that their Point of Contact is accessible during office hours (Monday to Friday from 9am to 5.30pm, excluding public holidays);
i) on receiving information from the i-CERT, have primary responsibility for further internal processing and any necessary measures/follow-up actions;
j) ensure information received from the i-CERT is only shared within their own organization with the designated employee(s) and/or Information Security Officers who, under section 6.1.1. (e), demonstrably need this information in order to adequately deal with it (*need-to-know* basis);
k) cooperate to the best of their ability in response to requests from the i-CERT for (additional) information;
l) in respect of the i-CERT be obliged to follow all other agreed procedures, and to use the tools and resources provided;
m) review the intake process as described in Article 9.1.1.

6.2 Participants

6.2.1 In addition to that outlined in 6.1.1, Affiliated insurers who also qualify as Participants will:

a) in their turn, and in accordance with a rotation model yet to be developed, as an Active Participant be responsible for carrying out the i-CERT service;
b) designate within their internal SOC and/or CERT, employee(s) who have a full mandate to perform the relevant tasks — where possible within existing business operations — in accordance with Article 7;
c) ensure that these employees are sufficiently qualified and informed to be able to perform these tasks effectively;
d) ensure that, during their turn of duty, the i-CERT service is accessible and operational at all times (including back-up in the case of illness/disaster);
e) ensure at all times that the resources and tools for the implementation of the i-CERT service as agreed upon under Article 7 are internally available and operational;
f) provide a proportionate financial contribution in the event that the Steering Committee unanimously decides to jointly purchase certain resources and/or tools for the i-CERT service;
g) review the intake process as described in Articles 9.1.2 and 9.2.

7 Implementation

7.1 Active Participant Activities

7.1.1 The employee(s) designated by the Active Participant(s) shall carry out the work required under Article 3.1, Article 7 and the working instructions/procedures specified above.

7.1.2 These activities must be done fully, adequately and in a timely manner.

7.1.3 Information-gathering under Article 3.1.1 (a) and (b) will be routinely sourced from pre-agreed sources. The Active Participant will monitor these sources as much as possible in real-time, during office hours. They are free to use additional (own) sources in this context.

7.1.4 Part of the work is to maintain operational contact with Affiliated insurers and Partner Organizations, including the management of a Point of Contact database and the passing on of the technical data of Affiliated insurers to the NCSC for monitoring purposes.

7.1.5 Distribution and/or targeted communication of relevant information within the framework of Article 3.1.1 (c) will occur — depending on the classification of the information — within the stipulated deadlines, in accordance with the following table:

Classification/Type	Timescale	To	How
Critical (including as a minimum NCSC-information on 'infected' domain names, URLs, IP addresses/ranges and any AS numbers).	7 x 24: within 1 hour of receipt	Exclusively to Affiliated insurers to whom the information relates.	Report by phone within set period. Thereafter, additional notification via the standard communication channel.
High	On receipt during office hours: within 1 hour and on the same day.	All Affiliated insurers	Via the standard communication channel.
Medium	On receipt during office hours: within 4 hours.	All Affiliated insurers	Via the standard communication channels
Low	Weekly	All Affiliated insurers	Via the standard weekly report ('end of week')

7.1.6 Prior to the communication/distribution of information within the scope of Article 3.1.1 (c), there should in principle be no further filtering or other interpreting of the information.

7.1.7 Information relating to an incident reported by an Affiliated insurer is to be distributed anonymously. Only with the consent of a primary source (whether or not on request), will the i-CERT provide the identity of the affected party.

7.1.8 Within the framework of Article 3.1.1. (e) and (f), the Active Participant will provide an 'end of week' report. Following a fixed format, this will give a concise summary of developments identified by the i-CERT, relevant general threats, developments within the market and publicly-known incidents.

7.1.9 For the purposes of management reports, and based on a (limited) number of agreed key indicators, a register will be made of information received and resolved, and executed activities.

7.1.10 At the end of their turn of duty, the Active Participant will ensure a satisfactory transfer of work to the following Participant whose turn it is to perform the i-CERT service.

7.2 Uniformity

7.2.1 Participants are required together to make concrete the agreements made in this covenant in corresponding uniform procedures, work instructions and resources. These shall be determined via the Governance referred to in Article 8.

7.2.2 In order to promote uniformity in implementation, the employees carrying out the work on behalf of the Participants will at least once a year participate in a 'Calibration Workshop' organized by the Operational Consultation Group.

7.3 Tools and resources minimum requirements

7.3.1 For the implementation of the i-CERT service, Participants will ensure there is a standard communication channel that complies with relevant laws and regulations in the area of privacy and data protection, and provides adequate safeguards for confidential data exchange.

7.3.2 To ensure the accessibility of the i-CERT in the event of high priority incidents, the Association will make available a central phone number. This number will always put one though to (the responsible employee of) the Active Participant.

7.3.3 For normal accessibility, and the provision of good quality information on i-CERT's services and procedures, the Association will provide a central e-mail address and a website with a recognizable domain name.

8 Governance

8.1 Steering Committee

8.1.1 Decision-making about, and management and supervision of, the i-CERT service is a responsibility of the Participants. The Participants will jointly interpret the delivery of this responsibility via the Steering Committee. The Steering Committee will operate within the policy frameworks established by the Association.

8.1.2 The Steering Committee may use independent powers, responsibilities and funds made available by the Participants in order to provide the information outlined in the objectives described in Article 2.1.1.

8.1.3 The Steering Committee monitors adherence to this covenant and, in particular, compliance with competition regulations during the implementation of the i-CERT service (as provided for in Article 6.1.1 (c) and (j).

8.1.4 The Steering Committee will report annually to the CBV Committee of the Association and advise (whether requested or not) on desirable actions or policy changes at sector level for the effective implementation of the i-CERT service.

8.1.5 Each Participant is obliged to be represented on the Steering Committee by a single management level employee. Preferably the CISO or Head of the Internal SOC/CERT.

8.1.6 The Steering Committee is chaired by a majority-elected representative of one of the Participants.

8.1.7 An advisor of the Association also has a seat on the Steering Committee, fulfilling the role of Secretary.

8.2 Operational Consultation Group

8.2.1 Monitoring of the uniformity and quality of i-CERT's operational services will be carried out by the Operational Consultation Group, which will be set up for this purpose and report to the Steering Committee.

8.2.2 The Operational Consultation Group will make proposals regarding the procedures, work instructions and resources needed to implement this Covenant effectively; flag up improvements from work practice, as well as relevant developments and trends; and offer advice in terms of the multi-year planning of the Steering Committee.

8.2.3 The Operational Consultation Group will report to the Steering Committee any non-adherence to this covenant and, more specifically, non-compliance with Article 6.1.1 (c) and (j).

8.2.4 The Operational Consultation Group consists of the designated employees of the Participants as appointed under Article 6.2.1 (b).

8.2.5 All Participants are required to be represented by at least one employee at each Operational Consultation Group meeting.

8.2.6 The Operational Consultation Group is chaired by a member of the Steering Committee (lynch-pin role).

8.2.7 The Operational Consultation Group will meet 4 times a year (at least twice a year physically and twice a year via a conference call).

8.2.8 The exact tasks of the Operational Consultation Group will be determined in greater detail by the Steering Committee.

8.3 Sounding Board Group

8.3.1 Feedback and advice from all Affiliated insurers regarding the functioning of the i-CERT service will be gathered via the Sounding Board Group.

8.3.2 All Employees of Affiliated insurers designated as a Contact Point under Article 6.1.1 (e) may participate in the meetings of the Sounding Board Group.

8.3.3 The Sounding Board Group will be chaired by a member of the Operational Consultation Group.

8.3.4 The Sounding Board Group will meet at least once a year.

9 Joining, intake and resignation

9.1 Joining the i-CERT service

9.1.1 An insurer who does not qualify as a Participant may use the i-CERT service provided:

a) they have signed this covenant using the enrolment form (Appendix 1) designated for this purpose;
b) they have completed an affiliation form providing, amongst other things, the details requested under Article 6.1.1. (d), (e) and (f), and forwarded this to the Active Participant;
c) the Steering Committee, acting on the advice of the Operational Consultation Group, concludes that the applicant meets, or can meet, all the requirements set out in Article 6.1;
d) one year has elapsed since the Board of the Association has approved the first version of this covenant (in line with the growth model, the first year is seen as an ‘induction period’ for the Participants).

9.1.2 In addition to the provisions under Article 9.1.1, an insurer who does qualify as a Participant can use the i-CERT service provided:

a) on signing up to this covenant (via the enrolment form in Appendix 2), they state their intention within 6 months both to comply with the conditions set out in article 6.2 and to take responsibility for the first time for performing the i-CERT service;
b) the Steering Committee, acting on the advice of the Operational Consultation Group, concludes that the insurer will do all it can to meet this deadline and, in this context, follow up on the actions required under Article 9.2.

9.2 i-CERT service intake implementation

9.2.1 In order to be able to implement the i-CERT service within 6 months, a Participant must undergo the following intake process:

a) the Participant receives a complete and up-to-date overview of the required procedures, work instructions, resources and tools;
b) the Participant makes a written inventory of the extent to which the required (organizational and technical) resources are already available and employable within their organization, and reports on this to the Operational Consultation Group;
c) a member of the Operational Consultation Group visits the Participant's organization. During this visit, the inventory is discussed, the Participant receives advice, and jointly it is determined what actions are still necessary to comply with the (pre-)conditions for carrying out the i-CERT service;
d) the Participant makes clear to the Operational Consultation Group how and when they expect to have completed these actions;
e) after 6 months, or earlier if possible, the Steering Committee will decide on the advice of the Operational Consultation Group whether the Participant is ready to carry out the i-CERT service for the first time;
f) in the event of a negative decision, the Steering Committee may grant the Participant a maximum 2-month postponement during which to meet the set (pre-)conditions. If they fail to do so, in principle the Participant loses their right to use the i-CERT service.

9.3 Resignation

9.3.1 An Affiliated insurer that does not qualify as a Participant may withdraw from this covenant with immediate effect, by notifying the Chairman of the Steering Committee in writing and giving their motivation for this decision.

9.3.2 An Affiliated insurer that does qualify as a Participant may withdraw from this covenant in accordance with a 6-month notice period, by notifying the Chairman of the Steering Committee in writing and giving their motivation for this decision. The Steering Committee will report on this to the management board of the Association and the CBV Committee.

9.3.3 In the interests of the continuity of the i-CERT service, a resigning Participant will continue to comply with their (implementation) obligations under this covenant, until up to a maximum of 6 months after the date of their written notice of retirement.

10 Other provisions

10.1 Public communication

10.1.1 Public statements about the activities of the i-CERT will only be done in coordination with the Association and with the approval of any other stakeholders.

10.2 Liability

10.2.1 A Participant cannot, with regard to the duties and responsibilities of all Affiliated insurers as stipulated in Article 6, be held liable for damages resulting from carrying out the i-CERT service, unless they can be shown to have deliberately given incorrect/misleading information or been seriously negligent in respect of their duties under Article 6.

10.3 Dispute resolution

10.3.1 Disputes concerning the interpretation or implementation of this covenant will be presented directly to the Steering Committee.

10.3.2 If the Steering Committee cannot reach a unanimous judgement, the matter will be submitted with a majority view to the CBV Committee of the Association.

10.4 Non-compliance and sanctions

10.4.1 If an Affiliated insurer/Participant believes that another Affiliated insurer/Participant is failing to comply with this covenant, this may be brought directly to the Steering Committee.

10.4.2 The party lodging the complaint must provide the Steering Committee with information and where possible evidence supporting their complaint. At the initiative of the Steering Committee, a hearing will take place with the complained-against party.

10.4.3 During the handling of the case within the Steering Committee, the parties concerned lose any voting rights. If the Steering Committee fails to reach a unanimous judgement, the matter will be submitted with a majority view to the CBV Committee of the Association.

10.4.4 If a majority of the Steering Committee finds that a party is systematically failing to comply, it may propose to the CBV Committee (temporarily) excluding this party from the i-CERT service.

10.4.5 In all cases where the CBV Committee is asked for a ruling, the complained-against party will be informed at management board level of the outcome and any sanctions.

10.5 Evaluation

10.5.1 No later than two years after approval by the Board of the Association, an evaluation of the design and operation of the first version of this covenant will take place. Further evaluations will take place at least every three years.

10.6 Changes to the covenant

10.6.1 The Board of the Association may, on the advice of the Steering Committee and the CBV Committee, decide to amend this covenant.