TOREON

Threat Modeling Practitioner

In-Company Training Brochure
Version: 3-Apr-2024

♦ Training Brochure ♦

Table of content

1 Build more secure products!

We teach threat modeling based on practical experience and have been offering our training annually at OWASP since 2016 and Black Hat Trainings since 2017. Our Black Hat training average score is 4.7/5 with excellent feedback!

Get a **Threat Modeling Practitioner Certificate**

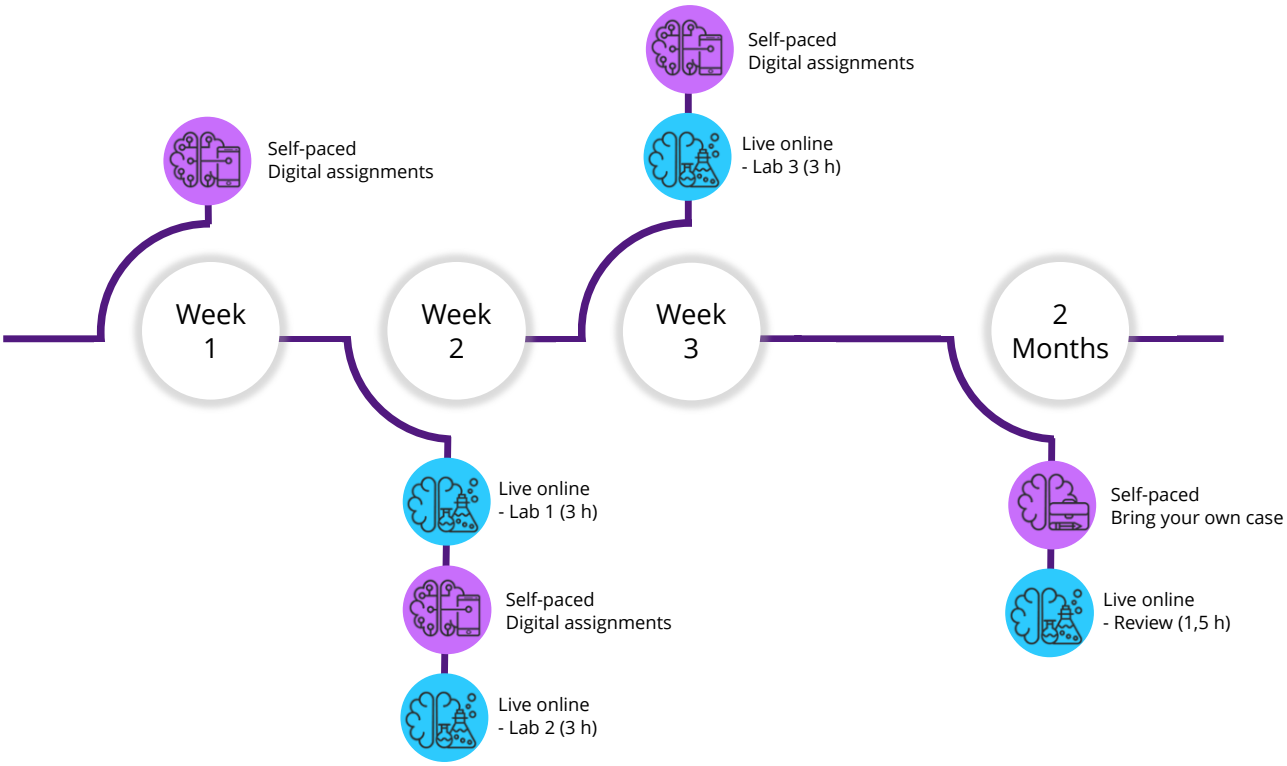
You can get your Threat Modeling Practitioner Certificate with our internal training options: the **20-hour "Threat Modeling Practitioner" blended course (this training)** or the 2-day "Agile Whiteboard Hacking". You will also receive our Threat Modeling Playbook, one-year online learning access, and a one-hour personal coaching session.

We can adapt this training to fit your technology stack, products, or way of working. Contact us by reaching out to:
Sebastien Deleersnyder, CTO Toreon, seba@toreon.com, +32 478 504 117
Or schedule a call directly: https://calendly.com/seba-dele/30min

2 Threat modeling practitioner journey (hybrid online)

This hybrid online training gives you the tools you need to become a threat modeling practitioner, teaching you how to threat model and build in security as an integral aspect of your secure development practice. This training is based on Toreon's international rewarded whiteboard hacking training. It's a course that blends self-paced digital work with action-packed, hands-on live labs run by our seasoned threat modeling experts.

Taught in English, this course is a blend of 8 hours of self-paced training and 12 hours of online live labs over 8 weeks.



Threat modeling is the best method for avoiding application and system-related risks from the get-go. Without threat modeling, any security measure is just a shot in the dark; you'll only really know what your vulnerabilities are after they've already been exploited. Another bonus? Threat modeling also gets your team on the same page with a shared security vision.

Our hands-on threat modeling challenges get you to apply the different stages of threat modeling to real-world scenarios. A fundamental part of that is learning the ropes of Toreon's risk-based unified threat modeling practice. You'll discover how to keep that aligned with your business objectives using an iterative and repeatable playbook that's also compatible with Agile and DevOps practices.

Master the basics of threat modeling, learn how to diagram what you are building, identify threats using the STRIDE method, and find out how to address every threat. We've adapted our Black Hat training to produce an action-packed hybrid of self-paced learning and live labs with engaging, hands-on workshops. In this course, we'll cover real-life use cases so that you understand how to perform practical threat modeling.

At the end of the course, Toreon awards you with a Threat Modeling Practitioner certificate and one-year access to our threat modeling templates and resources.

2.1 Target participants

Wondering if this course is for you? Toreon's threat modeling practitioner training targets software developers, architects, product managers, incident responders, and security professionals. If creating or updating a threat model is essential to your line of work, then this course is for you.

2.2 Learning goals

What you'll learn in a nutshell:

- The why, what, how, and when of threat modeling
- How to create and update a threat model
- How to create an actionable threat model with your stakeholders
- How to organise and prepare efficient threat modeling workshops
- How to explain the methodology and need for threat modeling to others
- Diagramming techniques, including Data Flow Diagramming
- Threat identification techniques, including STRIDE and attack trees

- How to carry out technical risk rating using the OWASP risk rating methodology
- How to mitigate security and privacy threats with standard mitigations
- The soft skills that will make you a better threat modeler

2.3 Educational approach of this course

As highly skilled professionals with years of experience under our belts, we're intimately familiar with the gap between academic knowledge of threat modeling and real-world practice.

We developed a two-month hybrid learning journey for threat modeling practitioners to help bridge that gap. You'll get a one-year account on our aNewSpring hybrid learning platform. It's been selected for its excellent blended, adaptive, and social learning features. Your hybrid learning journey starts way before the first live lab. It begins with the self-paced digital work you do to get you lab ready. And that goes hand-in-hand with live online sessions and regular mentoring. By the end of the course, you'll have created your own threat model and gotten valuable personalised feedback from your trainer.

The course is a blend of practical use cases based on real-world projects and mentoring. Each use case includes an environmental description, questions, and templates for building a threat model.

Participants are challenged in virtual breakout rooms of three to four people to carry out the different stages of threat modeling on the following:

- Diagramming web and mobile applications, sharing the same REST backend
- Threat modeling an IoT gateway with a cloud-based update service
- Get into the attacker's head – modeling points of attack against a nuclear facility
- Threat mitigations of OAuth scenarios for an HR application
- Threat modeling the CI/CD pipeline

The results are discussed after each hands-on workshop, and participants receive a documented solution.

2.4 Why take this course?

By the end of this threat modeling practitioner course, you'll understand:

- How threat modeling relates to a secure development lifecycle
- The benefits of threat modeling
- The different threat modeling stages
- The STRIDE model
- Secure design mitigations
- Risk rating

And you'll be able to:

- Create and update your threat models with an incremental technique
- Identify design flaws in your software
- Use threat modeling as an awareness tool for your team and stakeholders
- Get your team on the same page with a shared security vision

2.5 Practitioner package

To obtain your Threat Modeling Practitioner certificate, you need to:

- Complete all the self-paced activities
- Actively participate in the live labs
- Hand in your own (viable) threat model

Your bonus training package includes:

- One year of access to the e-learning platform
- Access to our live lab recordings
- Presentation handouts
- Tailored use case worksheets
- Detailed use case solution descriptions
- Threat model documentation template
- Template for calculating identified threat risk severity
- Threat modeling playbook
- STRIDE mapped on compliance standards

2.6 Course outline

Week 1: Threat modeling introduction (self-paced)

- Threat modeling in a secure development lifecycle
- What is threat modeling?
- Why perform threat modeling?
- Threat modeling stages
- Different threat modeling methodologies
- Documenting a threat model

Week 2: Diagrams – what are you building? (self-paced & live lab)

- Understanding context
- Doomsday scenarios
- Data flow diagrams
- Trust boundaries
- **Hands-on: Diagramming web and mobile applications, sharing the same REST backend**

Week 2: Identifying threats – what can go wrong? (self-paced & live lab)

- STRIDE introduction
- Threat tables
- **Hands-on: Threat modeling an IoT gateway with a cloud-based update service**
- Attack trees
- Attack libraries
- **Hands-on: Get into the attacker's head – modeling points of attack against a nuclear facility**

Week 3: Addressing each threat (self-paced & live lab)

- How to address threats
- Mitigation patterns
- Setting priorities through risk calculation
- Risk management
- Threat agents

- The mitigation process
- **Hands-on: Threat mitigations of OAuth scenarios for an HR application**
- **Hands-on: threat modeling the CI/CD pipeline**

Week 3: Threat modeling tooling and resources (self-paced)

- Open-Source & free tools
- Commercial tools
- Hard copy
- Online resources
- Threat modeling community
- Example threat models

Month 2: Bring your own case (self-paced & live lab)

- Bring your own threat model
- Transfer activities
- Mentoring
- Review session

3 Threat modeling introduction journey (self-paced online)

Supporting the practitioner training, we created a **2 h self-paced threat modeling introduction** for people who will be involved in threat modeling.

This self-paced training prepares involved stakeholders to understand with threat modeling is, the benefits of threat modeling and how they will be involved. Typically, this will be made available for involved testers, developers, security roles, administrators, DevOps engineers, architects, project managers, product owners and management (CxO).

Week 1: Threat modeling introduction (self-paced)

- Module 1: Welcome
  - Introductions
  - Personalizing your journey (knowledge and experience)
- Module 2: Why threat modeling?
  - Real life impact of threat modeling
  - What's in it for me?
- Module 3: What is threat modeling
  - Introduction to threat modeling
  - Involvement and expectations
- Module4: Follow-up
  - Personalizing your journey (review)
  - Experience review

4 Training options

4.1 Training customization

Optionally we provide the possibility to use your applications or systems for the training exercises.

Adapting the training with your own applications has considerable benefits:

- The attendees will relate to the exercises, as it covers a real application of your organization.
- The security awareness of the attendees on security design will increase, as the attendees will be exposed to your own organization risks.
- The implications of doing threat modeling and how to integrate that in your project methodology and technology stack will be better understood by the participants.
- During the exercises some extra security threats and design flaws might be discovered for the selected applications.

As input for this option, we will need the following information for the representative and selected application:

- Business context and value
- Use cases
- Applicable security and regulatory requirements
- A diagram, with a detailed description of the components and flows.
- Any known security or privacy risks identified so far
- A contact to ask questions and review the exercise

The outcome will be the adapted exercises of the training based on your application.

4.2 Threat modeling coaching

An important next step after our training is to put your trained knowledge into practice. Therefore, we propose to complement your training with our threat modeling coaching.

Our threat modeling coaching consists of the following activities:

- Introduce threat modeling templates in your development tooling
- Align threat modeling with your project methodology and security governance
- Facilitate and support threat modeling workshops with your teams
- Be a soundboard for your security champions and architects on threat modeling
- Validate new or updated threat models
- Start and improve threat model risk patterns for your organization
- Assist in selection and introduction of threat modeling tools

Our goal is to measure, start and improve your threat modeling practice towards the level that is appropriate for your organization risk exposure and appetite.

5 Threat Modeling Trainers

Our experienced Threat Modeling trainers share their practical threat model experience:

- **Sebastien (Seba) Deleersnyder** is co-founder and CTO of Toreon and a proponent of application security as a holistic approach. He started the Belgian OWASP chapter, was an OWASP Foundation Board member, and has given numerous public presentations on Application Security. Seba also co-founded Belgium's annual BruCON security & hacker conference and training sessions. With a development background and years of security experience, he has trained countless developers to create more secure software. Having led OWASP projects such as OWASP SAMM, he has genuinely helped make the world a safer place. What's he currently up to? Right now, he's busy adapting application security models to the evolving field of DevOps and is also focused on getting the word out on Threat Modeling to a broader audience.

- **Steven Wierckx** is a seasoned software and security tester with 15 years of experience in programming, security testing, source code review, test automation, functional and technical analysis, development, and database design. Steven shares his web application security passion by writing about and through training on testing software for security problems, secure coding, security awareness, security testing, and threat modeling. He's the OWASP Threat Modeling Project Lead and organises the BruCON student CTF. Last year, he spoke at Hack in the Box Amsterdam, hosted a workshop at BruCON, and provided threat modeling training at OWASP AppSec USA and O'Reilly Security New York.

- **Thomas Heyman** is an application security expert with 14 years of experience in academia and industry. He has a PhD in secure software engineering and has worked in threat modeling, secure architecture and coding, secure design reviews, and assessing the performance and scalability of distributed systems. He co-founded a software product company that helps highly regulated companies apply data analytics to improve their identity and access management. Thomas is passionate about application security and firmly believes that good security requires a holistic perspective, which should always have a sound threat model at the base.

- **Georges Bolssens** embarked on his coding journey in the early 1990s and delved into the realm of application security in 2017. With an inherent passion for teaching,

Georges is not only a seasoned developer but also an adept communicator. His unique talent lies in simplifying intricate subjects through relatable analogies, making him an engaging and effective speaker. Having undertaken numerous consulting assignments, Georges has assumed the role of a cybersecurity educator for a diverse spectrum of professionals. His guidance has illuminated the path for individuals ranging from legal experts at renowned "Big 4" consulting firms to ethical hackers and all those in between.In his capacity as an Application Security Consultant at Toreon, Georges has been instrumental in assisting numerous clients in constructing comprehensive threat models for their digital assets.

6 Get in touch!

We can adapt this training to fit your technology stack, products, or way of working. Contact us by reaching out to:

Sebastien Deleersnyder, CTO Toreon, seba@toreon.com, +32 478 504 117
Or schedule a call directly: https://calendly.com/seba-dele/30min

7 Supplier Information

Name:	Toreon
Legal Entity:	BV
Nationality:	Belgian
Address:	Grotehondstraat 44 1/1 B-2018 Antwerpen Belgium
Administrative email:	administratie@Toreon.com
VAT:	BE 0542.795.568
IBAN:	BE10 0017 1351 5104
Financial Institution:	BNP Paribas Fortis
Telephone:	+32 3 369 33 96
Contract Responsible(s)	**SEBASTIEN DELEERSNYDER**
Mail Address:	sebastien.deleersnyder@toreon.com
Telephone:	**+32 478 504 117**

8 Toreon – Business driven cyber consulting.

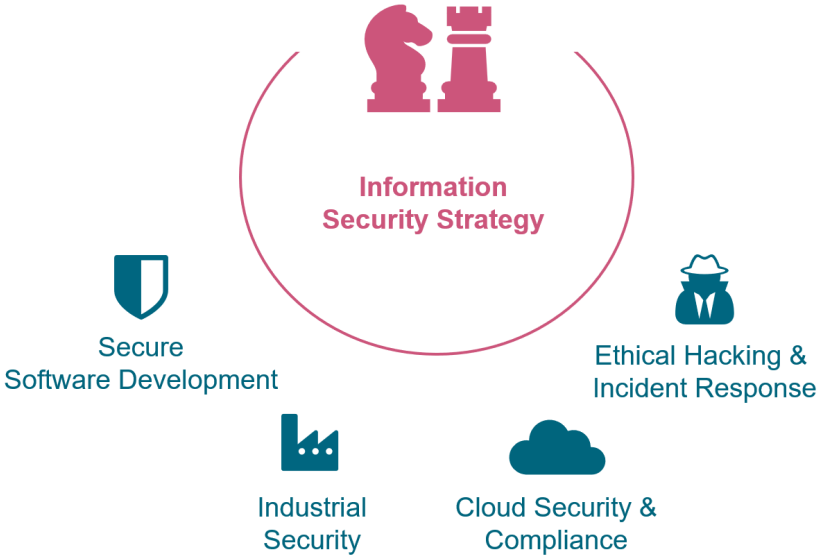
Toreon is completely focused on security. We are independent from vendors and technical security integrators and provide unbiased expertise and advice to our clients.

We start our security engagements from the needs of the business and its strategy. We create security policies and roadmaps that help your business to achieve its goals. We don't stop your digital progress but rather enable it.

Most of our competitors, in contrast, see security as a means to eliminate as much risk as possible and will aim to always provide the highest security level possible – stopping you in your tracks.

We don't see security as a goal in itself, but rather as a business enabler, as an accelerator. Security is the brakes on the car that allow it to drive faster. We align security policies to your business needs, expectations and risk appetite and implement what is needed. No more, no less. **We call this 'minimum security' – but with 'maximum impact'.**

Our engagement with you as a client is long-term. We create and support your corporate security policy and make sure it lands and gets adopted in your digital environment. We create a roadmap as a guide to activate the security policy and help you to reach a higher security maturity, at a level that fits your needs.



Our Governance, Risk and Compliance (GRC) team is the backbone of our company. They are CISOs with business, legal and technical backgrounds. They are used to talking with the business to understand their goals. They create a security strategy that aligns to these goals and are able to execute that strategy at our clients.

Our Application Security Experts help to govern security in the development process. Whether aimed at small independent software developers or development teams in large organizations, our Appsec experts coach and train security champions in different teams to upgrade their security maturity. We use the OWASP SAMM framework for governance. (In fact, our people co-created the framework at OWASP)

Our OT Security Specialists speak the language of process engineers and operators and understand their needs. They translate the corporate security policy to industrial terms and make sure critical processes stay up and running.

Our Cloud Security Team starts from a Zero Trust vision and makes sure the corporate security policy is reflected in the cloud tenant. We specialize in protecting Identities and Data, especially in the Microsoft 365 and Azure cloud.

Our technical team of ethical hackers and incident responders knows how a hacker thinks and works. They can test your systems – before a hacker does – and they are your best bet again these hackers when they break into your systems. They are available night and day.

9 References

These are some of our Threat Modeling (TM) reference customers. Further details are available upon request.

- Euroclear – TM coaching
- Standard Chartered Bank – TM training
- Banque Lombard Odier & CIE SA – TM training
- Lloyds Banking Group – IriusRisk TM training and coaching
- BP – TM training
- Sage – IriusRisk specific TM training
- Costco Wholesale – TM training
- Accenture USA – TM training
- LinkedIn – TM training
- Booking.com – TM training
- SD Worx – TM execution
- Barco - AppSec Support / TM training
- ENTSO-E – Appsec Support / Threat Modeling
- Atlas Copco - Appsec Support / Threat Modeling
- UCB - Appsec Support / Threat Modeling / TM training
- Blackhat USA and Europe 2017 - 2023 – TM trainings
- O'Reilly, OWASP, BruCON, … – TM Trainings

10Terms & Conditions

1 Object

Toreon delivers services in accordance with the General Sales Conditions and the specific conditions set out in the offer. The agreement between the Client and Toreon consists of the General Sales Conditions and the Toreon offer (“Agreement”).

2 Toreon offer and purchase order

The Toreon offer is valid for a maximum period of thirty (30) calendar days. This version of the offer prevails over earlier versions. It supersedes all prior agreements, whether oral or written, between the parties with respect to such matter.

The Client accepts the Toreon offer by signing a purchase order or by the acceptance of the commencement of the performance of the services.

3 Rights and obligations

3.1 Information. The Client shall make all information, files, documents and other relevant material required for proper performance of the Agreement available to Toreon no later than two (2) Working Days (any day except a Saturday, Sunday or official Belgian holiday) after receipt of a request from Toreon.

3.2 Cooperation. The Client shall provide immediately upon request of Toreon all facilities, assistance, and cooperation for the proper performance of the Agreement.

The Client shall give access to the premises, buildings, or other facilities during and after normal office hours for the purposes of performance of the Agreement.

The Client shall provide to Toreon the security procedures and instructions and prepare the environment to enable the delivery of services, prior to the performance of the Agreement.

The Client shall appoint a contact person, who will be responsible for the communication with Toreon and who shall take the decisions related to the execution of the Agreement in a timely fashion.

3.3 Toreon material. The Client shall be liable for the loss of or damage to Toreon’s material used in the execution of the Agreement, except if the loss or damage results exclusively from fault or negligence by Toreon.

4 Delivery and acceptance

4.1 Delivery. Toreon undertakes reasonable commercial effort to deliver services at the agreed point in time.

4.2 Acceptance. The Client has accepted the services unless he has notified Toreon in writing of any problem within five (5) Working Days as from delivery.

5 Prices and payment

5.1 Prices are quoted in EURO. The prices mentioned in the Toreon offer do not include VAT or any other expenses or duties. Toreon may adapt the prices if the costs for the services increase before the placement of the purchase order by the Client.

5.3 Additional administrative cost. The Client shall make a separate payment per invoice, clearly stating the invoice number. If payments are lumped together, Toreon may charge an administrative cost of €65.

5.4 The Client shall bear all costs due to the payment of the invoice. In the event of overdue payment, Toreon shall be entitled to interest at the legal rate without prior written notice. Should the Client not pay timely, Toreon may suspend the performance of the Agreement until full payments has been made or may consider the Agreement as terminated.

5.5 The Client shall have accepted the invoices, unless Toreon has received Client’s complaint related to the invoice within fifteen (15) calendar days of invoice date.

5.6 Travel and stay expenses outside of Belgium will be invoiced at cost with an additional 8% administration cost with a minimum of 100€ per one-way trip per person. Travel time of consultants will be billed at 60% of agreed hourly tariffs.

6 Intellectual property

6.1 Intellectual property rights. All intellectual property rights related to the products/services shall vest in Toreon or its suppliers. It is understood that Client receives no title or ownership of intellectual property rights, unless otherwise explicitly specified in the Agreement.

6.2 Software licenses. All software shall be delivered subject to the software license agreement of the manufacturer of the software.

7 Copyright and intellectual property

All software, programs, studies, systems, and all other documents developed in the framework of the present Agreement shall be deemed to be property and will stay property of Toreon.

The Client will provide the necessary ownership and user rights when Toreon is considered to use software, or other material, subject to copyrights, owned by the customer. The Client shall indemnify Toreon completely of any expenses and/or costs (incl. Legal expenses) and damage that occurs from a third-party claim with regards to ownership and copy- and user rights of software or material as described above.

8 Confidentiality

Parties shall undertake all reasonable measures to treat the confidential information exchanged in the frame of the Agreement ("Confidential Information") in a confidential manner. Parties shall not disclose Confidential Information to third parties without the prior written approval of the other party. Confidential Information may be disclosed only to staff and/or subcontractors of the receiving party who reasonably require access to such information for the purpose of the performance of the Agreement.

Confidential Information does not include: (i) information received outside the scope of the Agreement and without restriction on disclosure; (ii) information independently developed by the receiving party; (iii) information which is publicly known.

9 Liability

Toreon's liability under the Agreement shall be limited to the total amounts that the Client paid over the 6 months preceding the cause of the damage. Toreon shall not be liable for unforeseeable or indirect damages, including but not limited to suspension of Client's activities, loss of revenue, loss of information, data, or programs, third party claims.

Any claim for damages should be filed ultimately six (6) months after occurrence of the damages and ultimately six (6) months after termination of the Agreement.

10 Termination

If the term of the Agreement is indefinite, either party may terminate the Agreement by notice in writing to the other party with a notice period of 3 months.

Either party may terminate the Agreement at any time, directly without referral to the courts, by notifying the other party, if the latter seriously violates any of its essential obligations under this Agreement and the violation is not rectified within thirty (30) calendar days of written notification thereof.

The Agreement shall automatically be terminated if one of the parties ceases its activities, becomes insolvent or bankrupt, is dissolved or is subject of a similar procedure.

11 Miscellaneous

11.1 Toreon may entrust performance of its obligations under this Agreement to a subcontractor or transfer all or part of its rights and obligations under this Agreement without Client's prior consent.

11.2 The Client to whom Toreon delivers services, shall not engage directly or indirectly any of Toreon employees or any subcontractor who is or has been directly involved in the performance of the Agreement without the prior written consent of Toreon, independent of whether the Client had direct contact with the employee or subcontractor. This prohibition applies during the Agreement and for a period of six (6) months after the termination of all contractual agreements between Toreon and the Client.

In the event of non-compliance with the aforementioned prohibition, the Client must pay Toreon compensation equal to twelve times the global monthly cost that Toreon bears for the performance of the relevant employee or subcontractor. The global monthly cost is determined based on the average of the months, limited to a period of twelve months, prior to the violation of the prohibition, subject to Toreon's right to claim a higher compensation claim if the actual damage suffered would be greater.

11.3 The Agreement replaces any previous agreement, oral or written, between the parties with respect to the purchase order.

11.4 The fact a party does not exercise his rights under this Agreement, shall not be interpreted as a waiver of that party's rights.

11.5 Either party shall be excused from the performance of any of its obligations under the Agreement, if the performance is prevented or delayed by a cause beyond the affected party's control which, without limitation, includes fire, flood, accident, storm, natural disaster, war, riot, act of government or strike. The obligations of Toreon under the Agreement shall be extended by a reasonable period.

11.6 Communications under the Agreement shall be in writing and sent by registered mail, courier, fax, or e-mail, handed over to the general counsel at the registered office of the party to whose attention the message is sent.

11.7 The Agreement shall be governed by Belgian law.

In case of a dispute between both Parties concerning the Agreement, which cannot be solved by negotiations, both Parties commit themselves to resolve the dispute by mediation by means of the instruction guide of bMediation (Louizalaan 500 – 1050 Brussel).

In the event of a dispute which cannot be resolved by mediation within a month of the first request for mediation, the Antwerp courts have the exclusive jurisdiction.