CYBER SECURITY
COALITION.be

CYBER SECURITY AWARENESS & CULTURE MANAGER

2022

BACKGROUND

The Certification as 'Cyber Security Awareness & Culture Manager' was created in 2019 by the Awareness Focus Group of the Cyber Security Coalition.

The training programme combines members' best awareness practices in cyber security and tackles the challenges of behavioural and cultural change. Each module consists of both theoretical and practical exercises which will lead the participant to create their own cyber security awareness plan by applying the processes that have been created and refined by the trainers, who are experienced industry experts. Participants who successfully complete the programme receive a Certification supported by the Cyber Security Coalition and the Centre for Cyber Security Belgium (CCB).

A fourth edition of the 'Cyber Security Awareness & Culture Manager' training programme will be organised in the spring of 2022.

1. OBJECTIVES AND SCOPE OF THE TRAINING

LEARNING NEEDS

Employees play a major role in securing an organisation's business. The most efficient way to educate employees on how to fortify the human element of your organisation's security is through cyber security awareness actions. Security awareness is not a project, but a process. To achieve a sustainable change in behaviour, you need to continuously give substance to security awareness.

In this interactive training programme offered by the Coalition, participants learn how to plan, communicate and execute a Cyber Security Awareness Roadmap tailored to their organisation. Building a Cyber Security Roadmap does not have to be laborious or overly theoretical. By beginning with high level objectives and adding details as an organisation progresses and matures, results can be realized in a short period of time.

Another key driver for participating in the Coalition training programme is to meet with and learn from others.

It has to be ensured that participants are able to follow all the different training modules, complete their homework and certification assessment. They need to get the necessary support of their line manager throughout the learning process.

WHO CAN APPLY?

- The training programme is open to all employees of our member organisations.
- Participants do not need to be technically skilled but should have a grasp on the basics of IT, be interested in cyber security and committed to learning.
- Technical experts can also join the programme if they want to learn how to improve the effectiveness of their communication about cyber security issues and solutions.
- Participants must be motivated to combine working with a dedicated training pathway, for which they should have the support of their line manager.

THE SELECTION PROCESS WILL BE AS FOLLOWS

- 25 applicants will be admitted to the training programme.
- Priority will be given to the candidates on the Coalition's waiting list.
- The programme will be launched on **Tuesday, March 3rd**.
- Interested candidates must submit an application form with their motivation by **Thursday, April 14th (5:00 PM)** to info@cybersecuritycoalition.be.
- The Coalition Operations Office will inform all candidates about the selection decision at the latest by **Tuesday, April 19th (5:00 PM)**.

PRACTICALITIES

- The language of the training sessions will be English.
- The online training sessions will be recorded.
- Participants must be able to attend Microsoft Teams meetings for the online sessions.
- The in-person sessions and the Certification ceremony will take place at the BluePoint conference centre, boulevard August Reyerslaan 80, 1030 Brussels. There are parking facilities in the building. The nearest metro station is Diamant.

The evolution of the COVID-19 pandemic is difficult to predict. Consequently, it cannot be ruled out that the planned in-person sessions may be transformed into online sessions as a result of stricter sanitary measures taken by the government.

2. THE TRAINING PROGRAMME

Participants commit to take part in the **6 mandatory** training sessions of the programme. Should they be unable to attend all sessions, they will unfortunately be excluded from the Certification.

MODULE 1: UNDERSTANDING CYBER THREATS

Modality:

Classroom

Objectives:

- Understand the cyber security threats and actors, their modus operandi and manipulation techniques

Kick-off:

- Explain the training programme to the participants
- Clarify required input and expected outcome
- Introduce participants and trainers

Module:

- Understand how to identify cyber threat actors that may target your organisation and what these threat actors are
- Understand prominent cyberattack methods
- Gain sufficient insights into the above to identify what human security risks your organisation is facing

Participants will do exercises during the session and will have to prepare 'homework' for the next session. This homework will help them to build your organisation's 'Cyber Security Awareness Roadmap'. Sufficient time should be reserved for the homework.

Trainers:

- Alexandre Pluvinage, ING Belgium
- Vincent Defrenne, NVISO

MODULE 2: STAKEHOLDER MANAGEMENT & RISK ASSESSMENT

Modality:

Classroom

Objectives:

- Understand the rationale of risk management
- Understand the key concepts and definitions of risk management
- Learn a practical risk management approach for the design of a Cyber Security Awareness Roadmap
- Learn how to keep an up to date overview of the stake-holders relevant for Cyber Security Awareness in your organisation

During the session participants will get guidelines for their homework to be completed for the next session.

Trainers:

- Ann Mennens, European Commission
- Laurie-Anne Bourdain, Isabel Group

MODULE 3: BEHAVIOURAL CHANGE - HACK THE BRAIN

Modality:

Classroom

Objectives:

- Understand which aspects play a role in behavioural change
- Understand why successful behavioural change only comes in stages
- Learn how to develop a programme which takes care of these aspects

Participants will have to do some homework to be completed for module 5.

Trainers:

- Kristien Bergans, BNP Paribas Fortis
- Mercedes Diaz Sanchez, NVISO

MODULE 4: CULTURE

Modality:

Classroom

Objectives:

- Understand what culture is, why it's important and how you can measure it
- Understand how your current culture can help or hinder your programme
- Learn how to create and reinforce habits

There is no homework for this session.

Trainers:

- Emmanuel Nicaise, Approach Belgium
- Richard Atkins, Euroclear

MODULE 5: COMMUNICATION SKILLS

Modality:

Classroom

Objectives:

- Understand where you should focus on before even starting to work
- Learn how to evaluate communicational outcomes based on specific criteria
- Learn which principles to apply when you want to create communication that sticks

Participants will have to do some homework to be completed for the next module.

Trainers:

- Kristien Bergans, BNP Paribas Fortis
- Laurie-Anne Bourdain, Isabel Group

MODULE 6: HOW TO BUILD A CYBER SECURITY AWARENESS ROADMAP

Modality:

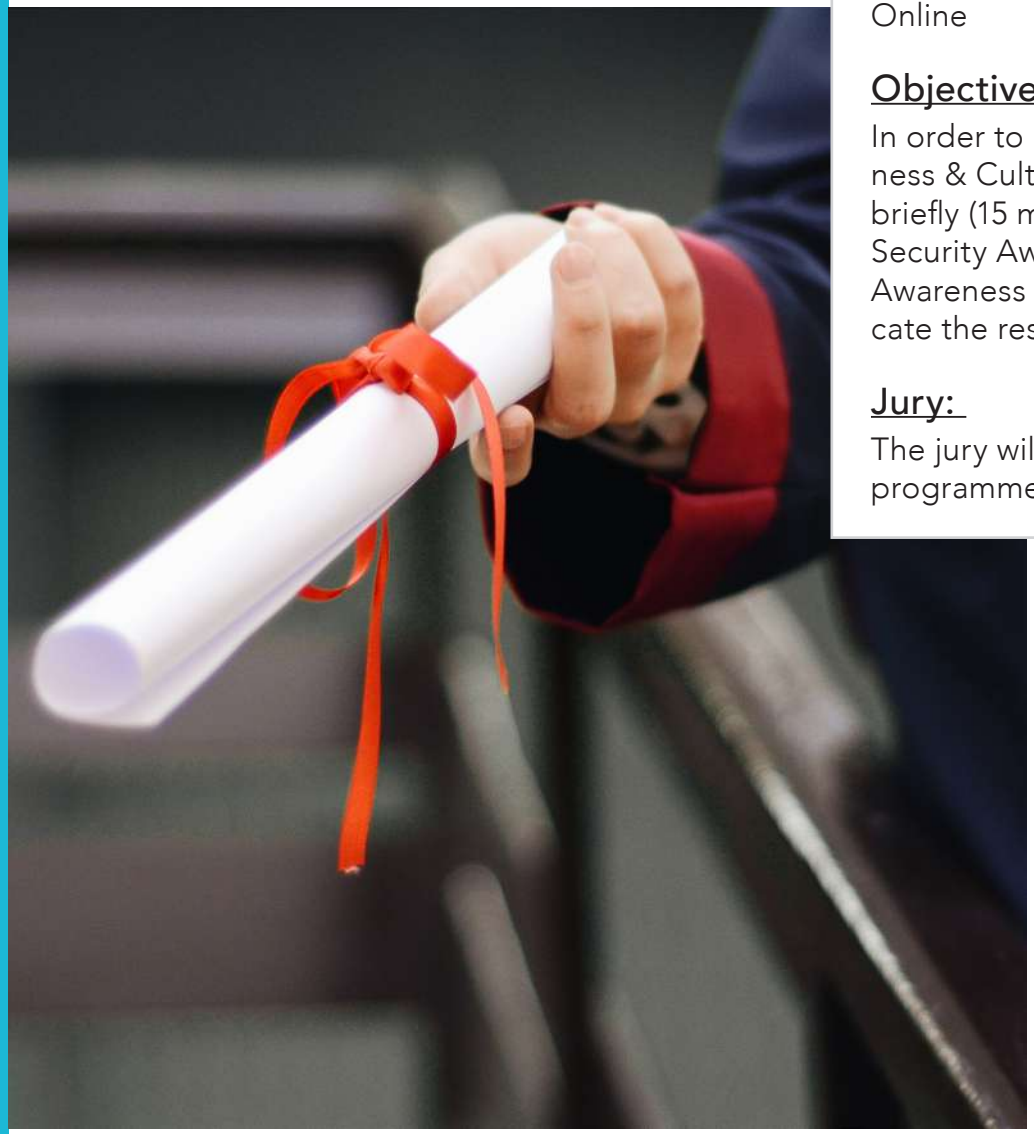
Classroom

Objectives:

- Get insight into a five-step approach to develop your Cyber Security Awareness Roadmap
- Understand the requirements for the final test

Trainers:

- Alexandre Pluvinage, ING Belgium
- Christine Van Dessel, KBC Group



CERTIFICATION DAY: PRESENTATION CYBER SECURITY AWARENESS ROADMAP (TEST)

Modality:

Online

Objectives:

In order to receive the certificate 'Cyber Security Awareness & Culture Manager', participants will be asked to briefly (15 minutes, max. 5 slides) present their Cyber Security Awareness Roadmap before a jury of Security Awareness experts. The next day the jury will communicate the results.

Jury:

The jury will be composed of the teachers of the training programme.

RESULTS CEREMONY

If a participant has passed the test, they will be invited to the Certification cocktail ceremony at the Brussels-based headquarters of BNP Paribas Fortis on **September 13th at 2:00 PM** (subject to COVID-19 sanitary measures).

3. TIMETABLE OVERVIEW

DATES	TIMESLOT	MANDATORY MODULES	HOURS
26 April 2022	1:00 PM – 5:00 PM	Kick-off Understanding cyber threats	1 3
10 May 2022	2:00 PM – 5:00 PM	Stakeholder management & Risk assessment	3
17 May 2022	2:00 PM – 5:00 PM	Behavioural change – Hack the brain	3
31 May 2022	2:00 PM – 5:00 PM	Communication skills	3
7 June 2022	2:00 PM – 5:00 PM	Culture	3
21 June 2022	2:00 PM – 5:00 PM	How to build a Cyber Security Awareness Roadmap	3
29 June 2022	1:00 PM – 4:00 PM	Presentation Cyber Security Awareness Roadmap (test)	0.25 per participant
30 June 2022		Communication of the results	
		Minimum estimate for the homework* and the preparation of the test	12
Total		**Approximately 4 days**	**32**
13 September 2022	2:00 PM – 5:00 PM	Results ceremony	

*Depending on your previous knowledge, you will spend less or more time on your homework. Take into account 1 to 3 hours per session and reserve this time in your agenda.

4. TRAINERS

All trainers boasting years of experience in awareness programmes and activities, they guarantee a quality training programme, that is highly appreciated by our members.

Organisation	NAME	FUNCTION
Approach Belgium	Emmanuel Nicaise	Human-centric Cyber Security Specialist
BNP Paribas Fortis	Kristien Bergans	Security Awareness, Behaviour & Culture expert
Euroclear	Richard Atkins	Group Security Awareness and Culture Manager
European Commission	Ann Mennens	Manager of the corporate Cyber Aware Programme of the European Commission
ING Belgium	Alexandre Pluvinage	Head of Fraud and Online Security Awareness @ ING BE, Podcaster, YouTuber, Keynote speaker
Isabel Group	Laurie-Anne Bourdain	Data Protection Officer, Risk Officer & Awareness Manager at the Isabel Group
KBC Group	Christine Van Dessel	Cyber Security Awareness Specialist
NVISO	Vincent Defrenne	Director Cyber Strategy
NVISO	Mercedes Diaz Sanchez	Cyber Culture (Awareness) solution lead and Strategy consultant

5. APPLICATION FORM
CYBER SECURITY AWARENESS & CULTURE MANAGER

Please, send the application form to info@cybersecuritycoalition.be by **April 14th, 2022 (5:00 PM)**.

YOUR APPLICATION

This document will enable the trainers to be familiar with your profile and expectations. We are looking forward to making your acquaintance.

YOUR RESUME

First name: .....
Last name: .....
Position: .....
Department: .....
Organisation: .....
Size of organisation (number of people): .....

How would you describe your key tasks and responsibilities in a few words?
5-10 lines

YOU AND CYBER SECURITY AWARENESS

Does your position relate to cyber security? If yes, how?
5-10 lines

Does Cyber Security Awareness & Culture exist in your organisation today?
If yes, in what way?
5-10 lines

YOUR MOTIVATION, YOUR EXPECTATIONS

What are your three (or more) expectations from this training?

What tangible improvements do you expect this training will bring to your professional activities and your organisation's Cyber Security Culture?
5-10 lines

Any other message to your trainers can be included below:

CONFIDENTIALITY

All information shared during the sessions or in the preparatory homework is confidential. As a final test, the participants will be asked to set up a Roadmap for their own organisation and to defend it before the jury of trainers. This information will also be considered confidential as a whole.

The Cyber Security Coalition will ensure that any natural person acting under its authority and having access to the data undertakes to respect confidentiality or be subject to an appropriate legal obligation of confidentiality.

INTELLECTUAL AND/OR PROPRIETARY RIGHTS

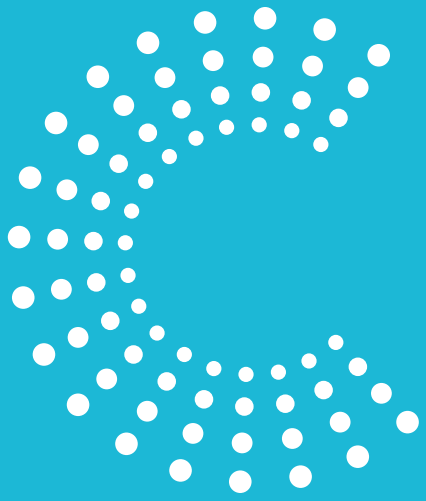
The Cyber Security Coalition reserves all rights on any document handed over in connection to the Cyber Security Awareness & Culture Manager training programme. The documents may not be used without explicit permission. You can contact the Cyber Security Coalition for this purpose via info@cybersecuritycoalition.be.

CANCELLATION

Please inform us immediately in case you cannot participate. We need to receive your completed application form by April 14th at the latest. After this date, we cannot guarantee your participation any longer.

THANK YOU!

Your signature and date:



CYBER SECURITY

COALITION.be