

IMPLEMENTATION OF COE ACTIVITIES IN 2019



NRD Cyber Security

is an

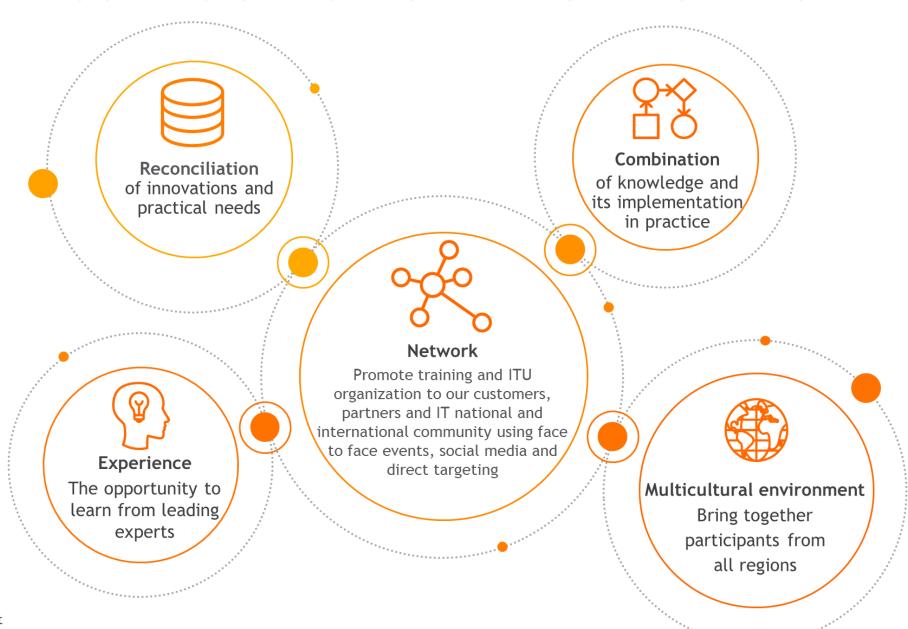
ITU Centre of Excellence

2019-2022





OUR VISION AS A CENTER OF EXCELENCE



NETWORKING



TRAINING COURSE: GOVERNING CYBER SECURITY AT NATIONAL LEVEL

PESIGNED FOR: senior and top-level officials from state administration and governmental bodies which have a mandate for or are involved in establishing, developing, coordinating and implementing national cybersecurity strategy and other relevant projects.

- DATES AND PLACE: Spring 2020, Vilnius, Lithuania
- SHORT DESCRIPTION: this course aims to deliver insights regarding the best cybersecurit practices at the national level, including methods, practical examples and lessons learned material is based on illustrative real-life cases and their analysis that will be delivered by t prominent experts. The training will be delivered in English.
- AFTER THE COURSE, PARTICIPANTS ARE EXPECTED TO BE ABLE TO:
- Initiate, lead and contribute to national cybersecurity strategy development and impleme
- Structure mandates of stakeholders in national cybersecurity;
- Manage cybersecurity incidents handling process in multi-stakeholder environments;
- . Identify, justify and lead improvement initiatives within the national cybersecurity framework.
- Argue different alternative methods to be applied in national cybersecurity management

THE COURSE WILL BE DELIVERED BY:









RIMTAUTAS CERNIAUSKAS Technical cybersecurity consult investigator



SIGITAS ROKAS

Questions about the course? Drop us a note at itucoe@nrdcs.lt

CENTRE OF EXCELLENCE (COE) MISSION AND ROLE

By utilising the latest developments in telecommunications, ITU is aiming to develop the technical standards that ensure networks and technologies seamlessly interconnect and strive to improve access to ICTs to underserved communities worldwide. However, with the advancement of technology, hand in hand go issues such as the speed of technology absorption or cyber security threats. Hence, constant training on technological skills and cyber resilience is required. For this purpose, ITU appoints CoEs in various regions which help to develop and improve the skills and competencies of ICT professionals worldwide.



NRD CYBER SECURITY AS ITU CoE

After a thorough selection process, NRD Cyber Security has been appointed as one of the six CoEs in Europe for the 2019-22 cycle. The company will be providing training courses in areas such as national cyber security governance, cyber security incident management and Open Source Intelligence (OSINT).

The programme of the courses is composed not only to enhance skills, but also to bring mutual benefits by knowledge sharing and networking. The high-calibre experience and knowledge of the attendees will be an incredibly valuable contribution to the discussions and talks during the training.

In addition to the training, we highly promote to take the opportunity to discover Vilnius and, if possible, other regions in Lithuania. The country is a modern Central European state with great focus on technological advancement, yet there are a lot of authentic culture, history and nature experiences to enjoy.



NRD Cyber Security

More about NRD Cyber Security at www.nrdcs.lt or let's connect via info@nrdcs.lt



NETWORKING





TIMETABLE



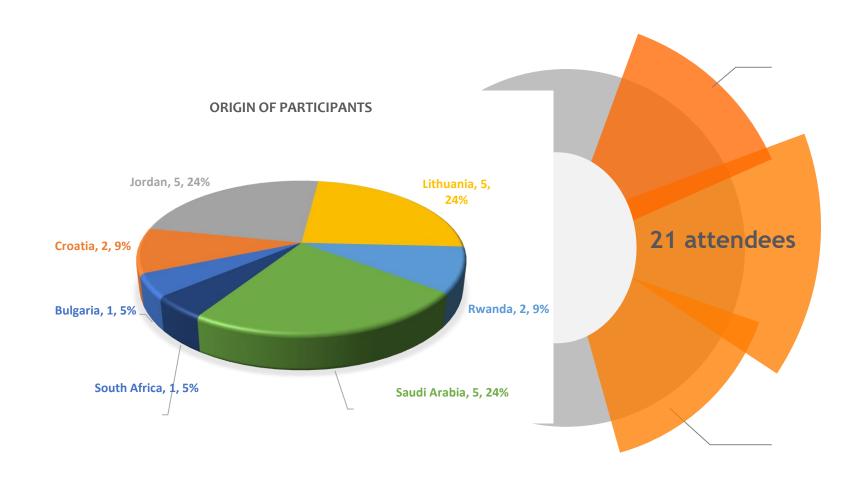


Governing cyber security at the national level





Incident response practice





Incident response practice



TRAINING REPORTS







Atene Ateneov	Bulgaria	ustanaucv@Se-gov.hg
lyjor Ljubil	Crosstile	lgor.[ub@puprasu.hr
Koelo Roberković	Crosstile	kreus rozenkovic@morh.hr
Noor Abed	Josefan	morabed@kh(gov.jo
Ahmad Barti Daya	Jordan	abunimus Elginali.com
Yageed Al-Abadieh	Jordan	yapercisbacleh@gmall.com
Thurner Sabahin	Jostian	dramerus@yafroccom
Zlad M. Zublidah	Jostian	ziaci,zubiciah@pymail.com
Durká Legus	Lithuaria	darkaslegas@Wirkask
Durks Minispikes	Lithuada	datusminlaukw@virtus.h
Durka Yallecka	Littrauria	D.Vielecka@barriberg/rkLlt
Rytis Jarkovičius	Littrauria	ryth.jarkeviclus@bilirks.k
Santrus Kontilus	Lithwate	serune Sikorcka R
Jean d'Amour Inflimwe	Rivanda	(Whitness@brr.rw
Richard Rugina	Rivanda	mugica@brr.nv
Abdullah Masoud Alghandi	Saud Arabia	abd.mgbgg@grwil.com
Alaa Allogynani	Sout Arabia	alse as 2000 (Chotmell.com
Caseb Alothi	Sout Arabia	algasebe@lgmall.com
Fahld Aldosani	Sout Arabia	f.m.ei-dreey@hotmeil.com
Sultan Sweet Mohammed Alshahradi	Sout Arabia	abodhermog@grwl.com
Peter Chan	Shout Africa	kritantilicalr.cn.za





NRD Cyber Security

Besides the final test score (Std) of total), participants were evaluated reflecting quantity of time spent on the training (20%).

Overall training outcome

Training course was very successful and exceeded our expectation in number of participants.

The training was almed at providing structurally focused knowledge on most common incidents and how their must be handled. This knowledge was gained during everal related projects implementation in different countries. It was expected that after the course, participants would be able to:

- apply incident majorane general verifitors principles;

 the substantial majorane principle by substantial majorane substantial majorane principles by substantial majorane substantial majorane substantial principles substantial pr

According trainers reports all topics were covered fully and well received by participants and the results. of final text is as the prove of that. Nevertheless, after the course trainers see some noom space for training material allying to training topics and practical esercises.

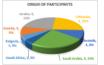
Big variety of participants' experience and job title as well as level give us an indication slightly change the course and prepare is more targeted in specific audience. It is rureated that the description of the training shands be very elaborated, and clear in order to get right participants and meet their

21 participants are quite hig group for hands-on training, then the programme was too interalies,

From 21 participants if were from Europe, to from Asia and 3 from Africa.

organisations (including Public sector organisation), 2 from the Regional Organisation and one from Operator.

5 participants belong to Manager level, 2-Executive and to Staff level.





All participants took participation in all training course activities but not all wished to attend social events after the course. Note likely the problem was atgrical whether for some participants originated.



(SCORE RENGE, NUMBER OF PARTICIPANTS, 1) Only few participants were shy and not very strong in linglish then caused their passive All attendees successfully passed the Final Test.

NRD Cyber Security

Please first evaluation matrix of all participants:

	Score (In II)			Weighted Score	
Name	Attendance	Exam	Attendance (200)	(Sot)	Total score
Abdullah Masoud Alghamdi	900	36	20	60	Sq.
Ahmad Bari Doa	933	95	20	75	96
du districti	933	99	20	75	96
Atena Atenacy	933	98	20	73	93
CONTRACTOR	933	39	20	67	E)
Darke Michaelou	933	64	20	51	31
Derka Vallecka	933	- 54	20	73	93
United State	933	51	20	73	93
Guetolithi	933	68	20	55	75
Igor Udd	933	No.	20	fig.	165
Jean County of the A	933	- 51	20	73	93
Selection desired	933	95	20	75	98 89
Noor Abed	933	36	20	69	
Peter Char	933	95	20	75	96
Richard Rugina	933	73	20	55	28
COC-LICENSION	933	Na.	20	65	255
Santrus Kontilus	933	- 51	20	73	93
Sulten Seeed Mohermed Abbabasi.	933	36	20	69	89
Usuar Sciolic	933	95	20	75	96
CHECK A COLUMN	933	- 54	20	73	93
Zlad M. Zubidah	933	55	20	75	93

Participants feedback

Unfortunately, not all participants gave feedback, only ty attendess used provided ITU templates. Overall assessment of the training lays between "Neutral" and "Strongly Agree". Students liked the most: professionalism and approach of trainers, hands on part (esercises) as well as

real life ecomplex.

The hospitality of organiser was appreciated also, but some of participants were unhappy with some logistics expects of the training, especially related to food (possibility to have hold type food).

Two participants found the training course description misleading and mentioned that it need an





NRD Cyber Security

Please we detailed surrup of the review bellow.

	Small	Dhagne	Neutral	NO.	(fluid
Relevance of training					
Relevance of course content to my work.			3	7	7
Topics being in line with my expectations	\neg	1	4	9	3
Counse relevance to current technology trends	\top		5	9	4
II. Training delivery		_		_	
Number of days allocated to the course	\Box		3	9	5
Delivery method used	\top	1		5	6
Training materials and training aids	\top	1	2	10	4
Facilitator's knowledge of the subject matter	\top	1	1	5	10
Facilitator's preparecines and presentation skills	-	1		ă	ă
Logical sequence of the topics	-	1	1	9	6
Bustrations, examples and practice sessions.	-	-	3	7	7
Tirrer allocated for learners to discuss and ask questions	$\overline{}$		3	ā	6
Knowledge gained during training	-	1	5	ā	5
C. Logistics				_	
Information provided to help with logistics for attending the			1	6	10
truiring course	1		1	ı	I
Redistration process	$\overline{}$	-		-	-

NRD Cyber Security

Payment process (where applicable) Usenfriendliness of the ITU website	+	7	1	-
	-	- 5	19	7
Support during training	-	1	0	0
Information provided to help with logistics for travel and accommodation		,	5	12
Training venue	-	4	5	100
Training rooms		5	3	2
Meals	2	5	4	6
D. Overall The overall delivers and content of the course				

The same up of answers to the question what could be improved in the future training is like this more exercises, more examples directly related to topics.

Proposed future training courses

Only few of participants commented on this section with following remarks:

- CERT/SOC governance
 Ethical Hacker
 Network

- Egovernment
 Cybernecurity for executives
 Forensic and big data technologies.

The bigginst surprise was the appearance of four unregistered participants in the totaling, From the last training experience, we were ready for last mission articularly or participants but not all a. Hoready, I are not sure of the measures that could prevent this hoppening, most likely that any additional last not aure of the measures that could prevent this hoppening, most likely that any additional last not sure of the probabilistic field probabilistic before the training in murclastery does

Sincere thanks to ITU Academy colleagues for the flexibility and support managing participants'



LESSONS LEARNED

CONSENT

- Do you really know how many participants will be in your class?
- Are you sure that all participants agree to be "revealed"?
- To what extent do meals influence participants' satisfaction on the course?
- Close cooperation and communication with ITU team helps a lot!

the participant of the training course "Incident response practice" cyber Security and ITU, held from 17th to 20th September 2019 in Vilni That NRD Cyber Security may use the photograph/video taken at an training course (including social events related to the training) in other media material produced or used including but not limite invitations, reports, brochures, etc. to receive further information related to the next NRD Cyber securi-NRD Cyber security are processing personal data according GDPF Security Privacy Policy. TRAINING COURSE INCIDENT RESPONSE PRACTICE 17-20 September 2019





CONTACT US

Phone: +370 5 219 1919

E-mail: itucoe@nrdcs.lt

Address: Gynėjų str. 14, Vilnius, Lithuania

CEO: Dr. Vilius Benetis vb@nrd.no

Training Coordinator: Rūta Jašinskienė

rj@nrdcs.lt

