



# Report on Second Training Workshop

IST-2001-39118

**Training of Network Security Incident Teams Staff**

**TRANSITS**



**Deliverable no. D3**

Project Manager: Karel Vietsch

TERENA, Singel 468 D, 1017 AW Amsterdam, The Netherlands

Phone : +31 20 5304488  
Fax: +31 20 5304499  
Email: vietsch@terena.nl

Date: 21 June 2003

## CONTENTS

<b>Executive Summary</b>	<b>3</b>
<b>1. Workshop Objectives and Background</b>	<b>3</b>
<b>2. Workshop Preparations</b>	<b>3</b>
2.1. Selection of Venue	4
2.2. Choice of Presenters	4
2.3. Workshop Announcements and Selection of Participants	4
2.4. Financial Arrangements	5
2.5. Workshop Materials	6
<b>3. Workshop Delivery</b>	<b>7</b>
3.1. Participants	7
3.2. Programme	8
3.3. Experiences of Presenters and Trainees	9
3.4. Results from Feedback Forms	10
<b>4. Actions Arising</b>	<b>11</b>

*Annex I*

*Second TRANSITS Training Workshop materials*

## **Executive Summary**

The second TRANSITS training workshop was held at the offices of NASK, Warsaw, Poland, on May 27<sup>th</sup> and 28<sup>th</sup>, 2003. The workshop was judged a great success by both trainees and presenters with everyone contributing to a very useful exchange of information. As with the previous workshop, a mailing list for the participants has been set up to help them communicate with each other in future. A number of the trainees at this workshop had been recommended to participate by people who had attended the first TRANSITS workshop in October/November 2002.

## **1. Workshop Objectives and Background**

Increasing the proportion of European networks that have Computer Security Incident Response Team (CSIRT) services is a major part of improving the dependability of networks and promoting public confidence in the Internet. The objective of the TRANSITS project is to promote the creation of more, professional CSIRTs and the strengthening of existing CSIRTs.

Operating a CSIRT takes rare and specialist skills; currently there are only a few hundred experts in Europe who have the necessary knowledge and experience. The TRANSITS project addresses this problem by providing specialist training to staff members of new CSIRTs and new staff members of existing CSIRTs.

Before the start of the TRANSITS project, course materials had already been prepared, but these need to be edited, maintained and updated during the lifetime of the project. A try-out presentation of the course was made in January 2002 in a workshop hosted by Telia at its headquarters in Farsta near Stockholm, Sweden. After the start of the TRANSITS project in July 2002, the earlier material and the feedback from the try-out presentation of the course were taken as inputs for preparing the first edition of the course material. That work was completed in September 2002, and the result was submitted to the European Commission as TRANSITS deliverable no. D1.

During the lifetime of the TRANSITS project the course materials will be presented six times, and it is intended to spread the locations of these six training workshops over various regions in Europe. The first training workshop took place in Oegstgeest, the Netherlands, on October 31<sup>st</sup> and November 1<sup>st</sup>, 2002 and was reported on in TRANSITS deliverable no. D2. The present deliverable reports on the preparations for, and the delivery of the second training workshop.

## **2. Workshop Preparations**

The training workshop required careful preparations. The two TRANSITS project partners, TERENA (the Trans-European Research and Education Networking Association) and UKERNA (the United Kingdom Education and Research Networking Association), were both involved in this. TERENA's Raquel Corredoira and Karel Vietsch took responsibility for identifying a suitable location, arranging accommodation and arranging financial support to

trainees if needed. UKERNA's Andrew Cormack took charge of ensuring the availability of teachers and preparing the contents of the workshop materials. The course was advertised jointly by both organisations, and Andrew Cormack and Karel Vietsch together took responsibility for the selection of trainees, asking for the advice of prominent members of TERENA's task force TF-CSIRT when needed. TERENA staff took care of having the printed workshop materials produced.

### **2.1. Selection of Venue**

In view of the intention to spread the locations of the six TRANSITS training workshops over various regions in Europe, it was decided at the start of the project to organise the first workshop in Western Europe and the second workshop in Central/Eastern Europe, with the third workshop (autumn 2003) possibly to be held in Southern Europe.

The NASK (Research and Academic Computer Network) organisation, which houses CERT Polska, one of the most active CSIRTs represented in TF-CSIRT, kindly offered the use of suitable meeting rooms in its modern offices on the outskirts of Warsaw. Hotel accommodation was arranged at the *MDM Hotel* closer to the city centre. NASK staff members provided much assistance to the TERENA staff in preparing the various logistic arrangements, and took care of solving practical problems during the event.

### **2.2. Choice of Presenters**

Lecturers were recruited from the most experienced staff members and former staff members of major professional CSIRTs. A number of members of task force TF-CSIRT have committed themselves to contribute to the TRANSITS materials and to act as teachers of course modules at a number of the training workshops. Some of the available volunteers had been co-authors of the original training course materials and/or had presented at the try-out workshop in January 2002 or the first TRANSITS training workshop in October/November 2002.

It was therefore not difficult to find a sufficient number of very well qualified presenters. The following team was chosen:

Andrew Cormack	UKERNA	United Kingdom
Jan Meijer	CERT-NL	Netherlands
Klaus Möller	DFN-CERT	Germany
Gareth Price	BT Ignite Secure Business Services	United Kingdom
Jacques Schuurman	CERT-NL	Netherlands

### **2.3. Workshop Announcements and Selection of Participants**

On February 20<sup>th</sup>, 2003 the announcement of the training workshop was published on the TRANSITS website ([www.ist-transits.org](http://www.ist-transits.org)). This announcement contained a course summary, an explanation of the pre-requisites, information about the time and venue and the costs, and instructions on how to apply for participation. At the same time the announcement was sent

via the appropriate mailings lists to the members of TF-CSIRT, the FIRST membership and the research and education networking organisations in Europe (the TERENA membership). Reminders were sent to the same communities early April. Two new mailing list were used to spread the announcement: a general TRANSITS announcement list to which any interested person can subscribe to receive TRANSITS news (see [www.ist-transits.org/maillinglist.php](http://www.ist-transits.org/maillinglist.php)), and the mailing list of participants in the first TRANSITS workshop. The announcement was also spread in various other ways, through personal contacts. In view of the venue of the workshop in a location that is central to a number of European Union accession states, special attention was given to spread the announcement in those countries.

The following time schedule was mentioned in the workshop announcements:

11 April 2003	Deadline for sending in applications
23 April 2003	Applicants will be notified whether a place has been reserved for them at the workshop
14 May 2003	Deadline for payment of the accommodation costs and the registration fee. In case payment would not have been received before this date, the place at the workshop might be assigned to another applicant.

By the time of the deadline, 26 applications had been received. Because the workshop was planned to accommodate two groups of ten trainees, not all applications could be accepted.

Two applicants, from the Romanian Ministry for Telecommunications, were interested from a policy and managerial perspective in the establishment of a CSIRT, but were not themselves potential future CSIRT staff members. It was therefore decided to reply to them that participating in the training workshop would not suit their objectives very well, while at the same time offering them support from the TF-CSIRT community to learn more about the process of creating a CSIRT. It was rewarding to see that the other 24 applications were of high quality: all applicants satisfied the pre-requisites for participation in the course and all were employed by organisations that either were providing a CSIRT service or had serious and advanced plans to set up such a service. Therefore none of the applications could be dismissed on grounds of quality or relevance.

After careful consideration it was decided to give priority to applicants from Central and Eastern Europe, and to applicants from CSIRTs that had not any of their staff members participate in a training workshop before. The applicants who could not be assigned a place at the second training workshop were guaranteed a place at the autumn 2003 workshop in case they would apply again then.

All twenty accepted candidates confirmed their participation and met the requirement of timely payment of accommodation costs and registration fee.

#### **2.4. Financial Arrangements**

As described in the TRANSITS project workplan, all trainees were expected to pay their own accommodation costs at the *MDM Hotel* as well as a (symbolic) fee of 100 euro. Participants

were asked to pay these sums to TERENA no later than twelve days before the event. This arrangement not only simplified financial administration, but it also reduced the risk of no-shows.

All participants paid their accommodation costs and fee on time, but establishing and maintaining contacts with participants in order to be certain that their payment would arrive took a lot of time and effort from TERENA staff. The same problem had been encountered in the preparations of the first TRANSITS training workshop, and for the second workshop it had therefore been decided to allow not two but three weeks between the notification of acceptance of application and the deadline for payment. It turned out that this longer period contributed little to solving the problem: the complexities of the international banking system and most of all the bureaucratic procedures within the organisations of some of the participants are such that the financial transactions will apparently always take considerable attention of the training course organisers.

Within the TRANSITS budget, TERENA manages funds to cover part of the travel and subsistence costs of training workshop participants from economically less-developed countries in Europe. This financial support will always cover only part of the total costs of these participants and will be limited to trainees from non-commercial, non-profit organisations. In the workshop announcements it was mentioned that such partial reimbursements of costs could be made available to participants from countries that are qualified by the World Bank as low-income economies, lower-middle-income economies or upper-middle-income economies.

Seven of the participants in the second TRANSITS workshop applied for reimbursement of part of their costs from these funds, as compared to only one participant in the first TRANSITS training course. This reflected the larger participation from EU accession states, which generally rank among the economically less-developed countries.

Within the TRANSITS budget, UKERNA manages funds to cover the travel and subsistence expenses of the lecturers who are not UKERNA or TERENA employees. These costs will be reimbursed after the event on the basis of invoices sent by the presenters to UKERNA.

## **2.5. Workshop Materials**

The course was presented using the latest version of the TRANSITS materials, which had undergone various updates after the previous TRANSITS workshop. Participants received a workshop pack containing printed copies of the slides, exercises and supporting documentation. Digital copies of these materials were provided on the workshop CD-ROM, which also included the CSIRT Handbook (with thanks to the copyright holders, Carnegie Mellon University) as well as RFCs relevant to CSIRT work. Each participant pack also included a copy of the book *Incident Response* by Kenneth R. van Wyk and Richard Forno (published by O'Reilly & Associates, Inc.) and a Guidance Note on writing advisories published by UKERNA.

Shipping the course materials from the Netherlands or the United Kingdom to Poland turned out to be a complicated matter because of complex and unpredictable customs procedures. In

the end, the only solution for this problem turned out to be for TERENA staff members to take the bulky and heavy materials with them to Warsaw in their personal luggage.

As the course materials cover rapidly developing topic areas and benefit continuously from feedback, some slides were modified immediately before and even during the workshop. These will be e-mailed to participants in due course.

### **3. Workshop Delivery**

#### **3.1. Participants**

Twenty trainees attended the course, from thirteen countries:

Lauri Anton	EENet	Estonia
Nuno Dias	FCCN	Portugal
Adam Gowdiak	POL-34 CERT	Poland
Pavel Kácha	CESNET	Czech Republic
Kristine Kaula	LATNET	Latvia
Johanna Kinnari	CERT-FI	Finland
Uldins Koskins	LATNET	Latvia
Tichomir Kotek	Technical University Košice	Slovakia
Vytautas Krakauskas	LITNET-CERT	Lithuania
Andrea Kropacova	CESNET	Czech Republic
Tomas Martisius	Vytautas Magnus University	Lithuania
Michael Müller	T-Com CERT	Germany
Ervin Nemeth	HUNGARNET	Hungary
Nuno Nielsen	DK-CERT	Denmark
Tomasz Nowocien	POL-34 CERT	Poland
Pascal Panneels	BELNET	Belgium
Lino Santos	FCCN	Portugal
Aleksandras Spiridenkovas	Vilnius University	Lithuania
Jakub Sucharkiewicz	T-Com CERT	Germany
Han van Thoor	KCSIRT	Netherlands

The organisers were particularly pleased to welcome no less than twelve participants from seven EU accession states: the Czech Republic, Estonia, Hungary, Poland, Latvia, Lithuania and Slovakia. Of the trainees, fourteen work for existing CSIRTs and six were from organisations in the process of creating a new CSIRT. Four of these organisations had not participated in European CSIRT activities before. The majority of the organisations represented are associated with research and/or education networks, although one commercial and one government CSIRT were represented. With the presenters also having experience of academic and commercial sectors, this gave good opportunities to share knowledge between the sectors.

### **3.2. Programme**

The objectives of the training workshop were:

- to understand where CSIRTs fit into the organisation
- to understand the tasks and tools that are necessary to perform their function
- to develop and practice the skills that are needed by a CSIRT team member
- to understand the external issues (both legal and technical) that may effect the operation of a CSIRT.

The course consisted of five modules. Some of these included exercises that the trainees had to complete and discuss, while others included time for discussion among the whole class. The modules were:

- **CSIRT Organisation**

Describes how CSIRTs fit into their organisations; planning the CSIRT, defining the constituency of the team and gaining management authority for it, deciding the services the team will offer, working with those outside the organisation, staffing the CSIRT, funding. Trainees discussed their own organisation and how their team fits into it.

- **Technical Aspects**

Understanding how intruders attack systems; intruders and their motivations, network protocols and how they can be abused, operating systems and services, types of vulnerability, information gathering, breaking in, hiding traces, denial-of-service attacks. A number of exercises were used to show how these appear in practice.

- **CSIRT Operations**

Describes the facilities, systems and tools needed by CSIRTs to operate successfully; housing the CSIRT, equipment, e-mail, remote access, information and contacts, servers and networks, incident response plans and procedures, tracking systems. As an exercise trainees discussed and developed incident response plans for their own teams.

- **Legal Issues**

Looks at the areas of legislation that are likely to affect CSIRTs in their work and that team members need to be aware of; origins of computer legislation, problems, data protection, computer misuse, working with law enforcement, monitoring, evidence, European developments.

- **Working with Vulnerabilities**

Discusses the roles that CSIRTs may decide to play in distributing and producing information about vulnerabilities; why do vulnerabilities exist, what should CSIRTs aim to do, sources of information and how to use them, advisories – distribution, interpretation, investigation and co-ordination.

The modules were presented in parallel in two groups. In order to encourage interaction with participants not known to them earlier, trainees were divided over these groups such that people from the same organisation were not in the same group and in each group the number of participants with the same mother language was minimised.

The time schedule of the two workshop days was as follows:

### Tuesday May 27<sup>th</sup>

Time	Group 1 in room A	Group 2 in room B
09.30	Welcome and introductions in room B	
10.00	Organisational Issues	Operational Issues
12.30	Lunch	
13.30	Organisational Issues (report back)	Operational Issues (report back)
14.30	Legal Issues	Technical Issues
16.30	Vulnerabilities	Technical Issues (cont.)
18.00	Close	
19.30	Dinner	

### Wednesday May 28<sup>th</sup>

Time	Group 1 in room A	Group 2 in room B
09.00	Operational Issues	Organisational Issues
12.30	Lunch	
13.30	Technical Issues	Legal Issues
15.30	Technical Issues (cont.)	Vulnerabilities
17.00	Close	

**Group 1:** Kaula, Kotek, Kropacova, Martisius, Müller, Nielsen, Nowocien, Panneels, Santos, Spiridenkovas

**Group 2:** Anton, Dias, Gowdiak, Kácha, Kinnari, Koskins, Krakauskas, Nemeth, Sucharkiewicz, Van Thoor

### 3.3. Experiences of Presenters and Trainees

The workshop was judged a great success by both presenters and trainees with everyone contributing to a very useful exchange of information. The participants asked that a mailing list for the group be established to help them to communicate in future, and many indicated that they would be recommending that their colleagues attend future workshops.

The venue contributed significantly to the success of the workshop. Three adjoining rooms were available, of which two were used for training sessions and one for refreshments. The formal sessions were presented to groups of ten trainees, with two tutors attending each session. Informal discussions were encouraged during breaks and over lunch, which was taken in a restaurant a short walk from the NASK building. This provided a useful break in the middle of the day, but additional time needed to be allowed so that everyone could get to and from lunch. Accommodation and evening meals were near the centre of the city, about 30 minutes away by underground. Travel was arranged very efficiently with each participant having the necessary tickets in their workshop pack. However, the journey meant that participants tended to split into small groups and may have missed some opportunities for discussions.

A wireless network was provided in the training area by NASK; this was very useful as it allowed tutors and trainees to consult websites for up-to-date information in order to answer

questions raised. Good network connectivity also makes it easier for lecturers, who volunteer their time, to keep in touch with their organisations.

Every trainee was asked to fill in a feedback form during the course to rate the content and presentation of each of the modules, and the workshop organisation and venue. Written comments were also sought to help in developing the materials and organising future workshops. Marks were requested for each module for level and quantity (from 1, trivial, to 5, excessive), for usefulness, organisation, visuals and delivery (from 1, low, to 5, high). Marks on the latter scale were also requested for workshop announcements, application and selection process, pre-workshop information, meeting rooms, Internet connectivity, hotel rooms, meals and support staff. Twenty completed feedback forms were returned. Overall the results were very positive, with the modules averaging between 3.4 and 4.0 for level and quantity, 3.5 to 3.9 for usefulness, and 3.9 to 4.2 for the presentation aspects. Logistics scored between 3.8 and 4.4 and the venue between 3.9 and 4.6.

These scores are higher than those for the previous workshop in Oegstgeest, indicating that feedback is helping the materials and the presenters to improve. The operational exercise, which has been rewritten since the last training course in order to give more guidance, worked much better. The technical module is still a little too long for its allotted time: for the next training workshop it will be considered whether it would help to present it on the same day as the legal and vulnerabilities modules, which tend to have some spare time. This would allow the lunch break to be taken in the middle of the longest module of the course.

There were not many written comments, but these and the oral comments were positive about the course. The comment “especially useful to those who are starting their own CSIRT” is encouraging, because starters are one of the main target audiences for the course.

### **3.4. Results from Feedback Forms**

Mean scores were as follows (all scores on a range from 1 to 5 – see section 3.3 for details):

<b>Module:</b>	<b>Organisation</b>	<b>Legal</b>	<b>Vulnerabilities</b>	<b>Operational</b>	<b>Technical</b>
Level	3.48	3.48	3.38	3.52	3.90
Quantity	3.52	3.57	3.38	3.67	4.05
Usefulness	3.48	3.76	3.57	3.90	3.67
Organisation	4.00	4.10	4.05	3.90	3.90
Visuals	3.95	3.95	4.00	4.05	3.86
Delivery	4.24	4.05	3.86	4.24	3.90

<b>Logistics</b>	
Announcements	4.05
Application & Selection	4.00
Pre-workshop information	3.79
Meeting rooms	4.21
Internet connectivity	4.57
Hotel	4.26
Meals	3.95
Support	4.39

#### **4. Actions Arising**

The following action items will be taken up in the TRANSITS project as a result of the experiences from the second training workshop:

- The course modules will all be revised in the light of comments from trainees and presenters during the course.
- An alternative ordering of modules will be considered for the next training course, to allow more time and breaks for the technical module.
- A mailing list will be created for the trainees and presenters from the course to enable discussions to continue. Updated versions of the course materials will be distributed to the delegates through this list.
- The successful and less successful aspects of this venue will be considered in the choice of venue for future workshops.