



# Report on Third Training Workshop

IST-2001-39118

**Training of Network Security Incident Teams Staff**

**TRANSITS**



**Deliverable no. D5**

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: 6 November 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>4</b>
2.1. Selection of Venue	4
2.2. Choice of Presenters	5
2.3. Workshop Announcements and Selection of Participants	5
2.4. Financial Arrangements	6
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*                      *Third TRANSITS Training Workshop materials*

## **Executive Summary**

The third TRANSITS training workshop was held at the Castello di San Gaudenzio, near Milan, Italy, on October 30<sup>th</sup> and 31<sup>st</sup>, 2003. As with the previous workshops, a mailing list for the participants has been set up to help them communicate with each other in future. A number of the participants at this workshop were colleagues of people who had attended previous TRANSITS workshops, which is an encouraging indication that trainees find the courses valuable and are recommending them to others in their organisations. At the same time, the third workshop also had a number of trainees from organisations and countries that had not been represented at TRANSITS workshops before.

### **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 second TRANSITS workshop was held in Warsaw, Poland, on May 27<sup>th</sup> and 28<sup>th</sup>, 2003 and was reported on in deliverable no. D3. The present deliverable reports on the preparations for, and the delivery of the third training workshop.

The next milestone in the TRANSITS project will be a major revision of the course materials, which is planned to be completed by March 2004.

## **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 Karel Vietsch and Carol de Groot 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. TERENA's Dick Visser installed Internet connectivity at the workshop venue.

### **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 to be held in Southern Europe.

Criteria for the selection of the venue included:

- A location at a reasonable travel distance from a major international airport. Many of the workshop participants have busy diaries and it was felt to be important to keep travel time as limited as possible.
- A secluded venue with the necessary meeting rooms, hotel rooms and facilities for meals in one location. Since the training benefits strongly from personal interactions, also outside the formal sessions, it is important to make intensive use of the 48 hours that trainees and lecturers are together.
- Moderately priced accommodation. While room hire, meals for workshop participants and travel and subsistence costs of the lecturers are paid by the TRANSITS project, trainees are expected to cover their own travel and hotel costs. Some of their employers are not-for-profit organisations with limited means.

The first TRANSITS workshop had taken place at a location that met all these criteria. The second training course was held at a venue that offered additional benefits but did not satisfy completely the second criterion. In the evaluation of the previous workshops it was decided to attach more weight once again to having a secluded venue and all facilities in one location when selecting future workshop venues.

After considering several options in Spain and Italy and more deeply investigating possible locations near Rome and Milan, it was decided to hold the training course at San Gaudenzio castle in Cervesina near Voghera, Italy, about 60 kilometres from Milan. TERENA took care of the arrangements with *Castello di San Gaudenzio*.

## **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 two TRANSITS training courses.

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
Klaus Möller	DFN-CERT	Germany
David Parker	UNIRAS	United Kingdom
Jacques Schuurman	SURFnet-CERT	Netherlands
Don Stikvoort	Stelvio BV	Netherlands

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

On July 7<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). Three additional 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 lists of participants in the first and second TRANSITS workshops. Reminders were sent to the same communities at the end of July and in early September.

The following time schedule was mentioned in the workshop announcements:

15 September 2003	Deadline for sending in applications
29 September 2003	Applicants will be notified whether a place has been reserved for them at the workshop
17 October 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.

Three days after the deadline, 22 applications had been received. This posed a small problem, because the workshop was planned to accommodate two groups of ten trainees. After re-investigating the available meeting facilities and negotiating additional hotel rooms with the conference centre, it was considered possible to accept all applications.

All 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 *Castello di San Gaudenzio* 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, although establishing and maintaining contacts with participants in order to be certain that their payment would arrive took considerable time and effort from TERENA staff. However, this problem was less substantial than on the previous two occasions.

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.

Only one of the participants in the third TRANSITS workshop applied for reimbursement of part of his costs from these funds, as compared to seven participants in the second TRANSITS training course. This reflected the limited participation from the EU accession states that qualify as upper-middle-income economies, which was no doubt related to the location of the workshop venue.

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 workshops. 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.

The course materials were shipped from the TERENA Secretariat office in the Netherlands to the subsidiary office of GARR (the Italian national research network) at the University of Milan. The workshop organisers would like to thank GARR and the University of Milan for their assistance on this matter, as well as for providing dial-up facilities for Internet access during the training course.

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 were e-mailed to participants after the course.

### **3. Workshop Delivery**

#### **3.1. Participants**

Twenty-two trainees attended the course, from fourteen countries:

Sante Bartolomei	ESA	Italy
Anne-Laure Bouillot	CERT-IST	France
Cecilia Catalano	ISTAT	Italy
Lorenzo Cavallaro	University of Milan	Italy
Øyvind Eilertsen	UNINETT-CERT	Norway
Girts Folkmanis	LATNET	Latvia
Carles Fragoso	CESCA	Spain
Carlos Fuentes	IRIS-CERT	Spain
Ian Hurst	UNIRAS	United Kingdom
Christian Kagerhuber	T-Online	Germany
Adrian King	SI-CERT	Slovenia
Jan Klever	DFN-CERT	Germany
Christos Koutsoupiis	University of Cyprus	Cyprus
Jacco Ligthart	GOVCERT.NL	Netherlands
Mattia Monga	University of Milan	Italy
Gustavo Neves	FCCN	Portugal
Amir Rasti	IPM	Iran
Daniel Sayk	T-Com CERT	Germany
Janusz Siwek	Information Security Centre	Poland
Maria Sole Scollo	GARR-CERT	Italy
Aron Vrtala	ACOnet CERT	Austria
Michael Westphalen	T-Com CERT	Germany

The trainees included four persons from EU accession states: Cyprus, Latvia, Poland and Slovenia. Of the participants, fourteen work for existing CSIRTs and eight were from organisations in the process of creating new CSIRTs. Three of these organisations had not participated in European CSIRT activities before. The majority of CSIRTs represented are associated with research and/or education, although two commercial and three government organisations were represented. The lecturers represented all three sectors, and trainees were able to learn from a broad range of expertise. Between them, the presenters have more than thirty years' experience of working in the CSIRT community.

### **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 course was presented using the latest version of the TRANSITS materials. Following comments at previous presentations that the module on Technical Issues was overwhelming when presented in a single session, the order of modules was changed to split the Technical Issues over a lunch break. Both presenters and trainees considered this change to have been a success, with the module on Technical Issues being rated more acceptable for quantity as a result.

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

#### Thursday October 30<sup>th</sup>

Time	Group 1 in Sala Cesare Taverna	Group 2 in Sala Azzurra
09.30	Welcome and introductions in Sala Cesare Taverna	
10.00	Organisational Issues	Legal Issues
11.30		Technical Issues
12.30	Lunch	
13.30	Organisational Issues (report back)	Technical Issues
14.30	Operational Issues	
16.30		Vulnerabilities
18.00	Close	
19.30	Dinner	

#### Friday October 31<sup>st</sup>

Time	Group 1 in Sala Cesare Taverna	Group 2 in Sala Azzurra
08.30	Legal Issues	Organisational Issues
10.00	Technical Issues	
12.00	Lunch	
13.00	Technical Issues	Operational Issues
15.00	Vulnerabilities	
16.30	Presentation and Close in Sala Cesare Taverna	

**Group 1:** Bartolomei, Catalano, Folkmanis, Fuentes, Kagerhuber, Klever, Monga, Neves, Rasti, Sayk, Siwek

**Group 2:** Bouillot, Cavallaro, Eilertsen, Frago, Hurst, King, Koutsoupi, Ligthart, Scollo, Vrtala, Westphalen

### 3.3. Experiences of Presenters and Trainees

The workshop venue worked very well and the local staff did everything they could to help the event run smoothly. Two rooms were used for teaching sessions, with a number of others available for exercises and individual discussions. Meals and accommodation were in the same building, so tutors and trainees had ample opportunity for discussions throughout the period of the workshop. These discussions are seen to be particularly valuable in an area such as Incident Response where there is rarely a single "correct answer". A number of participants suggested that it would have been useful to have more time for discussion of issues and ideas that had arisen during the formal sessions. The teaching sessions were presented to groups of eleven participants each, with two tutors attending each session.

A wireless network was installed in the teaching rooms, although the thickness of the castle walls meant this did not extend to other areas. Unfortunately, because of unexpected lack of some local facilities that had been promised, the connection to the outside Internet was not as good as had been expected, which led to occasional problems with long download times. Having a network is very useful for teaching, as questions can often be answered from documents published on the World Wide Web. Connectivity also makes it easier for the lecturers, who volunteer their time, to keep in touch with their own 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-two completed feedback forms were returned. Overall the results were very positive, with the modules averaging between 3.2 and 3.7 for level and quantity, 3.4 to 3.7 for usefulness, and 3.8 to 4.4 for the presentation aspects. Logistics scored between 4.1 and 4.6 and the venue between 4.4 and 4.7.

These scores suggest that feedback is improving the course with each workshop: level and quantity of all modules is now well within the "just right" range, with the model on Technical Issues clearly benefiting from the new schedule. Logistic arrangements scored particularly well and the venue was the highest rated of the three workshops so far.

There were not many written comments, but all were very positive: "really interesting", "overall excellent" and "very productive" were three participants' comments on their experience.

### **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	3.35	3.35	3.36	3.55	3.65
Quantity	3.65	3.17	3.27	3.73	3.39
Usefulness	3.48	3.43	3.55	3.73	3.65
Organisation	4.00	4.30	4.09	4.14	4.04
Visuals	3.83	4.09	3.95	3.95	3.96
Delivery	4.00	4.43	4.14	4.19	4.04

<b>Logistics</b>	

Announcements	4.09
Application & Selection	4.09
Pre-workshop information	4.48
Meeting rooms	4.61
Internet connectivity	3.07
Hotel	4.74
Meals	4.35
Support	4.65

#### **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.
- Suggestions, from this workshop and previous ones, for new areas to cover will be considered in the major review of the materials that will take place over the next few months.
- The revised order of modules will be used in future, and consideration given to how to incorporate more time for discussion.
- A mailing list has been created for the trainees and presenters from the course to enable discussions to continue.
- The successful and less successful aspects of this venue will be considered in the choice of venue for future workshops.