

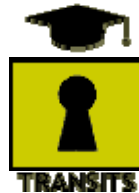


Final Report

IST-2001-39118

Training of Network Security Incident Teams Staff

TRANSITS



Deliverable no. D12

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: 25 October 2005

CONTENTS

Executive Summary	2
1. Description of the TRANSITS Project	3
1.1. Objectives and Summary	3
1.2. Work Packages	4
1.3. Milestones and Deliverables	6
2. TRANSITS Course Materials	8
3. TRANSITS Workshops	10
3.1. Organisation of the Workshops	10
3.2. Feedback	13
3.3. Experiences and Lessons Learned	18
4. Other Deliveries of the Course Materials	23
4.1. Other Training Workshops	23
4.2. Training Workshops in Other Continents – Collaboration with FIRST	25
5. Follow-up of the TRANSITS Project	27

EXECUTIVE SUMMARY

The TRANSITS (Training of Network Security Incident Teams Staff) project was funded with an amount of almost 250,000 euro by the European Commission as an Accompanying Measure in the Information Society Technologies (IST) Programme of the European Union's Fifth Framework Programme for Research and Technological Development. The project started on 1 July 2002 and was completed on 30 September 2005. The project consortium consisted of TERENA (the Trans-European Research and Education Networking Association) and the JNT Association trading as UKERNA (the United Kingdom Education and Research Networking Association).

Increasing the proportion of European networks and organisations that have CSIRT (Computer Security Incident Response Team) services is a major part of improving the dependability of networks and promoting public confidence in them. The objective of the TRANSITS project was to promote the creation of more, professional CSIRTs and the strengthening of existing CSIRTs by addressing the problem of the shortage of skilled CSIRT staff members.

The TRANSITS project has addressed this problem by providing specialist training to staff members of new CSIRTs and new staff members of existing CSIRTs. The project has been highly successful: as a direct result of the TRANSITS project, the number of people in Europe with the skills to be a CSIRT staff member has been increased by 75% in three years' time. Indirectly, through further dissemination of the course materials, the TRANSITS project has led in the same period to a further doubling of the pool of people with these scarce but essential skills.

These targets have been achieved by providing two-day training courses in the organisational, operational, technical, market and legal issues involved in providing CSIRT services. Course materials have been developed and maintained by the TRANSITS project, and seven TRANSITS training workshops were organised during the lifetime of the project. These workshops have provided training to 153 persons from 32 countries.

The TRANSITS materials have also been used at various other training events during the lifetime of the project. Through copyright ownership it is being ensured that a wide use of the course material is not obstructed by monopolisation of information or commercial exploitation by other parties. Collaboration was established between the TRANSITS project and FIRST (the Forum of Incident Response and Security Teams), the world-wide organisation of CSIRTs. The TRANSITS course materials have been used for training workshops organised under the auspices of FIRST in Latin America and the Asia-Pacific region.

The TRANSITS project partners have taken responsibility for creating a suitable permanent framework after the completion of the project for delivering further training courses and regularly updating the material. This has been implemented through a Memorandum of Understanding between TERENA and FIRST.Org, Inc. The latter organisation has committed resources for the further maintenance and updating of the course materials, and will continue to organise training workshops outside Europe, in particular in Latin America and the Asia-Pacific region. TERENA and FIRST will jointly organise further training workshops in Europe.

1. DESCRIPTION OF THE TRANSITS PROJECT

The TRANSITS (Training of Network Security Incident Teams Staff) project was funded as an Accompanying Measure in the Information Society Technologies (IST) Programme of the European Union's Fifth Framework Programme for Research and Technological Development. The project started on 1 July 2002 and was completed on 30 September 2005. The project consortium consisted of TERENA (the Trans-European Research and Education Networking Association) and the JNT Association trading as UKERNA (the United Kingdom Education and Research Networking Association).

1.1. Objectives and Summary

The Information Society is increasingly transforming our life. The social and economic impact of information and communication technologies is far-reaching and represents key opportunities and challenges for individuals, industry and governments. These technologies introduce new forms of doing business, but also contribute to improving the quality of life. Examples are in education and new opportunities for information sharing for culture and leisure.

Because of the social benefits, the European Union has decided to give priority to the development and introduction of the Information Society in Europe. Networks and information systems are now supporting services and carrying data to an extent that was inconceivable only a few years ago. Their availability is critical for other infrastructures such as water and electricity supply. As many businesses, private individuals and public administrations want to exploit the opportunities offered by communication networks, the security of these systems is a prerequisite for further progress.

Network and information security can be defined as the ability of a network or information system to resist, at a given level of confidence, accidental events or malicious actions. Such events and actions can compromise the availability, authenticity, integrity and confidentiality of stored or transmitted data as well as related services offered via these networks and systems. Handling and preventing security incidents needs an active approach, and CSIRTs (Computer Security Incident Response Teams) play an important role in this.

The formation of an effective CSIRT has huge benefits for all the users of a network, by increasing the reliability and confidence in the network as a tool for both business and commercial work. CSIRTs have been clearly demonstrated to be an instance in best practice in improving trust in networks.

In Europe, CSIRTs have been established mostly in the private sector, by research and education network organisations, institutions for research and higher education, commercial network operators and vendors. During the lifetime of the TRANSITS project, CSIRTs have increasingly been established in the government sector as well. The communication and collaboration between existing CSIRTs in different sectors (research networks, commercial network operators, government) is very good, and the TRANSITS project has been able to build on that collaboration.

Increasing the proportion of European networks and organisations that have CSIRT services is a major part of improving the dependability of networks and promoting public confidence in them. The objective of the TRANSITS project was to promote the creation of more, professional CSIRTs and the strengthening of existing CSIRTs by addressing the problem of the shortage of skilled CSIRT staff members.

Operating a CSIRT takes rare and specialist skills. At the start of the TRANSITS project, there were only 200-250 experts in Europe who had the necessary knowledge and experience to create and operate a CSIRT. Sometimes new teams were created by recruiting staff from existing CSIRTs, thereby only shifting the problem. Also, existing teams continuously need to make a substantial effort in educating new team members. Before the TRANSITS project, there was no training material available that was suited for training CSIRT staff members in Europe.

The TRANSITS project has addressed these problems by providing specialist training to staff members of new CSIRTs and new staff members of existing CSIRTs. As a direct result of the TRANSITS project, the number of people in Europe with the skills to be a CSIRT staff member has been increased by 75% in three years' time. Indirectly, through further dissemination of the course materials, the TRANSITS project has led in the same period to a further doubling of the pool of people with these scarce but essential skills.

These targets have been achieved by providing two-day training courses in the organisational, operational, technical, market and legal issues involved in providing CSIRT services. In addition to the material taught and the hands-on exercises, the trainees have received further reference materials and information. Together this has qualified them as competent members of a security incident response team.

Course materials have been developed and maintained by the TRANSITS project. Before the start of the TRANSITS project, course materials had already been prepared, but these were edited, maintained and updated during the lifetime of the project. At intervals during the project, reviews were held to reflect comments from trainees and teachers as well as changes in the external environment.

Seven TRANSITS training workshops were organised during the lifetime of the project. The locations of these seven training workshops were spread over various regions in Europe. Each workshop required logistic support: identifying a suitable location, advertising the course and selecting the trainees, arranging financial support for teachers and trainees if needed, and arranging accommodation. Lecturers at these workshops were partly staff of the project partners and partly experienced CSIRT staff members from other organisations who had committed themselves for these tasks. Each training workshop was rounded off with a report on the workshop, its preparations, its contents and the experiences of the presenters and the trainees.

The course materials have been put in the public domain. Through copyright ownership it is being ensured that a wide distribution of the material is not obstructed by monopolisation of information or commercial exploitation by other parties.

The TRANSITS project has encouraged the use of the course materials for other training workshops, for example at a national level. The TRANSITS materials have been used at various training events during the lifetime of the project, and this is expected to continue. Collaboration was established between the TRANSITS project and FIRST (the Forum of Incident Response and Security Teams), the world-wide organisation of CSIRTs. Based on these agreements, the TRANSITS course materials were used for training workshops organised under the auspices of FIRST in Latin America and the Asia-Pacific region.

Finally, the TRANSITS project partners have taken responsibility for creating a suitable permanent framework after the completion of the project for delivering further training courses and regularly updating the material. This has been implemented through an agreement with FIRST, which has been laid down in a Memorandum of Understanding between TERENA and FIRST.Org, Inc. The latter organisation has committed resources for the further maintenance and updating of the course materials, and will continue to organise training workshops outside Europe, in particular in Latin America and the Asia-Pacific region. TERENA and FIRST will jointly organise further training workshops in Europe.

1.2. Work Packages

The TRANSITS project was organised in four work packages:

- WP0 Project management and dissemination
- WP1 Course materials
- WP2 Logistics and organisation
- WP3 Course delivery

WP0 (Project management and dissemination) was led by TERENA. Its objectives were to ensure that the project was carried out according to plan and time schedules, to prepare the reports and deliverables to be submitted to the European Commission, and to disseminate information about the project's activities and receive feedback.

Karel Vietsch was appointed by TERENA as the Project Manager in charge of the day-to-day management of the project. His duties included planning, review of progress towards milestones, direct supervision of the TERENA staff working in the project, and liaison with project partner UKERNA, where Andrew Cormack was in charge of the TRANSITS work. The Project Manager was in charge of the correspondence with the Commission and the supervision of the execution of the project contract. He was responsible for the reporting to the Commission, including progress reports and cost statements. Karel Vietsch and Andrew Cormack represented the TRANSITS project at the annual project review meetings, which were organised by the European Commission.

TERENA and UKERNA staff members working on the project had intensive communication by email and phone. They met regularly – at least five times per year – adjacent to other events, such as TRANSITS training workshops and TF-CSIRT¹ meetings. In addition there were two face-to-face project meetings per year. Quality assurance, control of changes and resolution of problems were handled in these contacts.

The Project Manager was responsible for the liaison with TF-CSIRT. He has reported three times per year in the TF-CSIRT meetings about the progress of the TRANSITS project, and TF-CSIRT has provided feedback from the CSIRT community that has been taken up in the TRANSITS work.

TERENA staff have set up and maintained a website (www.ist-transits.org), where the TRANSITS training materials and workshops have been advertised, and the public project deliverables have been published. A mailing list was created for interested persons to receive regular updates on the TRANSITS activities and in particular announcements of forthcoming TRANSITS training workshops. In addition, mailing lists were created for the participants in each of the workshops, to enable them to stay in contact after the event. The website and the mailing lists have been used to receive feedback from the CSIRT community.

WP1 (Course materials) was led by UKERNA. Its objective was to develop and maintain materials for training workshops for CSIRT staff.

Before the start of the TRANSITS project, course materials already had been prepared in a collaborative effort in the context of TF-CSIRT, but they needed to be maintained and updated during the lifetime of the project. During each training workshop trainees were asked to fill in feedback forms and these were reviewed immediately afterwards. Throughout the project, the course materials were continuously reviewed and updated to reflect comments from trainees and teachers as well as changes in the external environment.

At the start of the project, the materials developed earlier and the feedback from the try-out presentation² were taken as inputs for preparing the first edition of the course material. This work was completed in the first three months of the project, and the first edition of the training materials was submitted to the European Commission on 30 September 2002.

A second milestone in WP1 was a major revision of the course materials after three TRANSITS training courses had taken place. This led to a second edition of the course materials, which was submitted to the Commission on 30 March 2004.

Using the inputs from many different people, most of the work for WP1 was carried out by Andrew Cormack of UKERNA.

¹ TF-CSIRT is the TERENA Task Force on Collaboration of Security Incident Response Teams

² The try-out presentation of the course materials took place in the offices of Telia in Farsta, near Stockholm, on 22-23 January 2002.

WP2 (Logistics and organisation) was led by TERENA. Its objective was to plan and make logistical arrangements for the delivery of the seven training workshops.

Each training workshop required logistical preparations and support: identifying a suitable location, ensuring availability of teachers, advertising the course and selecting the trainees, arranging financial support to trainees if needed, and arranging accommodation.

Room hire and meals for workshop participants were paid by the TRANSITS project, as well as travel and subsistence costs of the teachers. Trainees were charged a (symbolic) fee of 100 euro, and they had to cover their own travel and hotel costs. However, to enable participation by staff of CSIRTs from non-profit organisations in economically less developed countries, the TRANSITS project had a fund to cover part of the costs of such participants.

The workshops were publicised as widely as possible so as to reach potential trainees from a variety of CSIRTs. Course materials were made available in printed form and on CD-ROM, and were distributed at the start of each workshop.

WP3 (Course delivery) was led by UKERNA. Its objective was to deliver seven training workshops for CSIRT staff.

The training workshops took place in October/November 2002, May 2003, October 2003, May 2004, November 2004, February 2005 and April 2005. Each workshop was rounded off with a report on the workshop, its preparations, its contents and the experiences of the presenters and the trainees.

Each course was presented by a minimum of four (usually five) experts from the European CSIRT community. Each training workshop consisted of presentations by the lecturers and hands-on exercises for the students with individual assistance by the teachers. For each workshop a team of lecturers was invited by Andrew Cormack, who also co-ordinated the actual course delivery. Tutors from the European CSIRT community were highly motivated, seeing the benefit to their own everyday work of enlarging the community. Without any problem, their employers gave them permission to lecture at the TRANSITS workshops during working days.

Support was provided by TERENA staff. The provision of good Internet connectivity at the workshop became an increasingly important requirement during the lifetime of the project and required much attention.

1.3. Milestones and Deliverables

The first edition of the course material was the first milestone of the TRANSITS project. Another important milestone was the second edition of that material, based on a thorough review and revision of the contents. Other milestones were the seven TRANSITS workshops.

Towards the end of the project's lifetime, much attention was given to creating a suitable permanent framework for the continued delivery of CSIRT training courses after the end of the TRANSITS project. This resulted in a Memorandum of Understanding between TERENA and FIRST.

20 June 2002	TRANSITS project contract signed by the European Commission
1 July 2002	Project start date
30 September 2002	First edition of course materials completed and submitted
31 October – 1 November 2002	1 st TRANSITS training workshop in Oegstgeest, the Netherlands
27-28 May 2003	2 nd TRANSITS training workshop in Warsaw, Poland
30-31 October 2003	3 rd TRANSITS training workshop in San Gaudenzio, Italy
15 December 2003	Project review meeting, Brussels

30 March 2004	Second edition of course materials completed and submitted
25-26 May 2004	4 th TRANSITS training workshop in Hamburg, Germany
16 June 2004	Agreement between TRANSITS and FIRST on the organisation of training courses in Latin-America and the Asia-Pacific region
11-12 November 2004	5 th TRANSITS training workshop in Průhonice, Czech Republic
15 December 2004	Project review meeting, Brussels
17-18 February 2005	6 th TRANSITS training workshop in Chantilly, France
24 February 2005	First contract amendment approved by the European Commission
28-29 April 2005	7 th TRANSITS training workshop in Carcavelos, Portugal
12 July 2005	Memorandum of Understanding signed between TERENA and FIRST.Org, Inc. on the continued provision of CSIRT training
1 August 2005	Second contract amendment approved by the European Commission
14 September 2005	Project review meeting, Brussels
30 September 2005	Project end date

The TRANSITS project contract³ foresees twelve project deliverables:

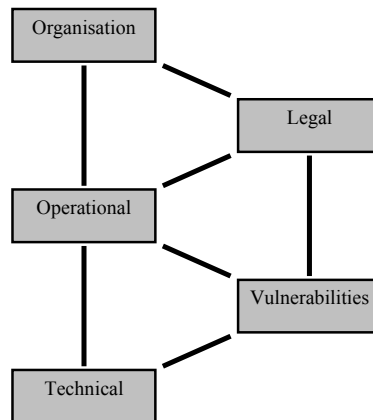
no.	deliverable	contractual date	actual date
D1	First edition of course material	September 2002	30 September 2002
D2	Report on 1 st training workshop	November 2002	19 November 2002
D3	Report on 2 nd training workshop	May 2003	21 June 2003
D4	First progress report and cost statement	July 2003	6 October 2003
D5	Report on 3 rd training workshop	November 2003	6 November 2003
D6	Second edition of course material	March 2004	30 March 2004
D7	Report on 4 th training workshop	May 2004	16 June 2004
D8	Second progress report and cost statement	July 2004	22 September 2004
D9	Report on 5 th training workshop	November 2004	24 November 2004
D10	Report on 6 th training workshop	February 2005	18 March 2005
D11	Report on 7 th training workshop	May 2005	27 May 2005
D12	Final report and cost statement	September 2005	25 October 2005

³ The TRANSITS project contract was amended twice, in February 2005 and in August 2005. Throughout this Final Report, reference is made only to the latest version of the contract.

2. TRANSITS COURSE MATERIALS

The training course materials give trainees an overview of the tasks involved in the operation of a CSIRT. They present the skills that are needed by a member of a computer and network security team. They present tools and techniques that are needed in incident response. And finally, the course gives an outline of important external relations that a CSIRT may want to or may need to maintain, such as with law enforcement and with legislative bodies.

The TRANSITS course material is highly modular. This makes it possible, also after the end of the TRANSITS project, to have each module developed and maintained by the most competent people for the particular topic in the CSIRT community. It also keeps the course as a whole easily maintainable.



The material consists of five modules:

Organisation

The module covers the organisation of CSIRTs: how they relate to their host organisation, their customers and the wider community. Topics include: 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. Students discuss their own organisation and how their team fits into it.

Operations

The module discusses the CSIRT staff, and systems and procedures that they need in order to carry out their chosen function. Topics include 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, students discuss and develop incident response plans for their own teams.

Technical

The technical module provides technical understanding of how Internet attacks and other security incidents are performed, detected and prevented. Topics include: 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 are used to show how these appear in practice.

Vulnerabilities

The module discusses how to deal with software and system vulnerabilities. Topics include: 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.

Legal

The module discusses legal issues affecting CSIRTs and their customers. Topics include: 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.

The modules were originally developed by the most knowledgeable experts in the European CSIRT community as a voluntary effort in the context of TF-CSIRT. At the start of the TRANSITS project, the materials were updated and restructured. This led to the first edition of the TRANSITS course materials, which was completed in September 2002.

Throughout the lifetime of the TRANSITS project the course materials have been continuously updated, based on the feedback from lecturers and trainees in the TRANSITS workshops and other training courses, and from the wider CSIRT community. At each TRANSITS training workshop the most recent version of the materials has been used. Also for other training courses using the TRANSITS materials the most recent version has been made available to the presenters.

A major milestone was a general overhaul of the materials that was carried out in early 2004, leading to the second edition of the TRANSITS course materials. In this revision, the legal module was rewritten in order to make it more practical, the division of material between the operational and organisational modules was reorganised, parts of the technical module were condensed, a vendor section was added to the module on vulnerabilities, the bibliography was checked and updated, and new versions of external handbooks were added. Updates from speakers, requests from students and suggestions from the CSIRT community were sources of information that was added to the material. In the legal module, new cases on liability and jurisdiction were added, as well as a discussion on how to improve the law. The operational module was extended with a discussion of forensic investigations and incident tracking tools. Incident surveys were a topic added to the organisational module, and in the technical module attention was paid to infrastructure attacks. In the module on vulnerabilities, the vendor process was discussed, as well as new projects and standards.

3. TRANSITS WORKSHOPS

3.1. Organisation of the Workshops

Seven training workshops were organised during the lifetime of the project. Each workshop required careful preparations. TERENA staff took responsibility for identifying a suitable location, arranging accommodation and arranging financial support to trainees if needed. UKERNA's Andrew Cormack was in charge of ensuring the availability of teachers and preparing the workshop materials. The courses were advertised jointly by TERENA and UKERNA, and Andrew Cormack and TERENA's 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 workshop materials produced. TERENA staff also took care of local support and logistics. Good Internet connectivity soon became an important requirement for the TRANSITS workshops, and was often not easy to realise.

Care was taken to spread the workshop locations over various regions in Europe. Criteria for the selection of the venues included:

- A location at a reasonable travel distance from a major international airport. Many of the workshop participants had very 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 was important to make intensive use of the 50 hours that trainees and lecturers were together.
- Moderately priced accommodation. While room hire, meals for workshop participants and travel and subsistence costs of the lecturers were paid by the TRANSITS project, trainees were expected to cover their own travel and hotel costs. Some of their employers were not-for-profit organisations with limited means.

In the course of the project it became clear that it was very important to maintain an ample time schedule for the announcements of the workshops. Workshops should be announced some 12 weeks before the event, with a deadline for applications more than a month later. Applicants should be notified one month before the workshop whether a place has been reserved for them or not, and they should be asked to pay the accommodation costs and registration fee no later than two weeks before the event. This arrangement not only simplified financial administration, but it also reduced the risk of no-shows.

The total costs of a training workshop (including workshop materials, meeting room hire, hotel rooms for participants and travel costs of lecturers) was typically between 15,000 and 20,000 euro. With on average 20 trainees, this would result in a price of 750-1000 euro. Thanks to the financial contributions from the TRANSITS budget provided by the European Commission, the payments could be limited to 225-400 euro per student.

Within the TRANSITS budget, TERENA managed funds to cover part of the participation costs of training workshop participants from economically less developed countries in Europe. This financial support covered always only part of the total costs of these participants, and was limited to trainees from non-commercial, non-profit organisations. Twenty of the 153 participants in the seven workshops applied for reimbursement of part of their costs from these funds.

The workshops were presented using the latest version of the TRANSITS materials. Participants received a workshop pack containing printed copies of the slides, exercises and supporting documentation. Digital copies of these materials were provided on a CD-ROM, which also included the CSIRT Handbook (with thanks to the copyright holders, Carnegie Mellon University) and a paper on Incident Response made freely available by the US National Institute for Standards and Technology (NIST). At the earlier workshops, the participant pack also included a Guidance Note on writing advisories published by UKERNA and a copy of the book *Incident Response* by Kenneth R. Van Wyk and Richard Forno (published by O'Reilly & Associates, Inc.). At the time of the later workshops this book was out of print, and no suitable replacement could be identified.

The presentation of the five modules took about 12-14 hours over the two workshop days. In addition there were exercises about incident analysis, drafting an organisation plan and an incident response plan. In the later workshops, the programme was extended with additional sessions in the evenings of the two days. One of these was a PGP key signing session. In other sessions, various "work in progress" topics were discussed. In the closing session on the final evening, students were encouraged to work through incident response scenarios in small groups, in order to identify issues from each of the modules that might arise in these scenarios.

Every trainee was asked to fill in a feedback form during the workshop 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, and for usefulness, organisation, visuals and delivery. Marks were also requested for workshop announcements, application and selection process, pre-workshop information, meeting rooms, Internet connectivity, hotel rooms, meals and support staff.

First workshop

Dates: 31 October – 1 November 2002
Venue: Oud-Poelgeest Conference Hotel, Oegstgeest, the Netherlands
Trainees: 21, from 14 countries
Lecturers: Andrew Cormack (UKERNA), Klaus Möller (DFN-CERT), Gareth Price (BT-SBS), Jacques Schuurman (CERT-NL) and Don Stikvoort (Stelvio)

Second workshop

Dates: 27-28 May 2003
Venue: NASK offices, Warsaw, Poland
Trainees: 20, from 13 countries
Lecturers: Andrew Cormack (UKERNA), Jan Meijer (CERT-NL), Klaus Möller (DFN-CERT), Gareth Price (BT-SBS) and Jacques Schuurman (CERT-NL)

Third workshop

Dates: 30-31 October 2003
Venue: Castello di San Gaudenzio, San Gaudenzio near Voghera, Italy
Trainees: 22, from 14 countries
Lecturers: Andrew Cormack (UKERNA), Klaus Möller (DFN-CERT), David Parker (UNIRAS), Jacques Schuurman (SURFnet CERT) and Don Stikvoort (Stelvio)

Fourth workshop

Dates: 25-26 May 2004
Venue: Mellingburger Schleuse Hotel, Hamburg, Germany
Trainees: 15, from 10 countries
Lecturers: Andrew Cormack (UKERNA), Stelios Maistros (GRNET-CERT), Klaus Möller (DFN-CERT), Claudia Natanson (BT) and Jacques Schuurman (SURFnet CERT)

Fifth workshop

Dates: 11-12 November 2004
Venue: Parkhotel, Průhonice, Czech Republic
Trainees: 23, from 13 countries
Lecturers: Andrew Cormack (UKERNA), Klaus Möller (DFN-CERT), Claudia Natanson (Diageo), David Parker (UNIRAS) and Jacques Schuurman (SURFnet CERT)

Sixth workshop

Dates: 17-18 February 2005
Venue: Chateau de la Tour, Gouvieux near Chantilly, France
Trainees: 22, from 13 countries
Lecturers: Andrew Cormack (UKERNA), Klaus Möller (DFN-CERT), Claudia Natanson (Diageo), David Parker (UNIRAS) and Jacques Schuurman (SURFnet CERT)

Seventh workshop

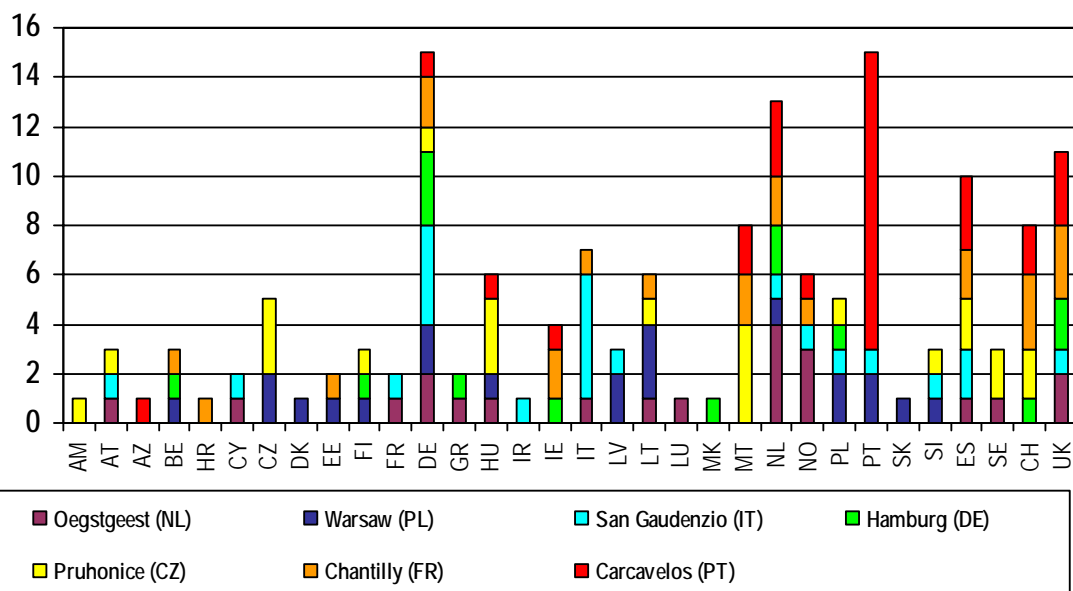
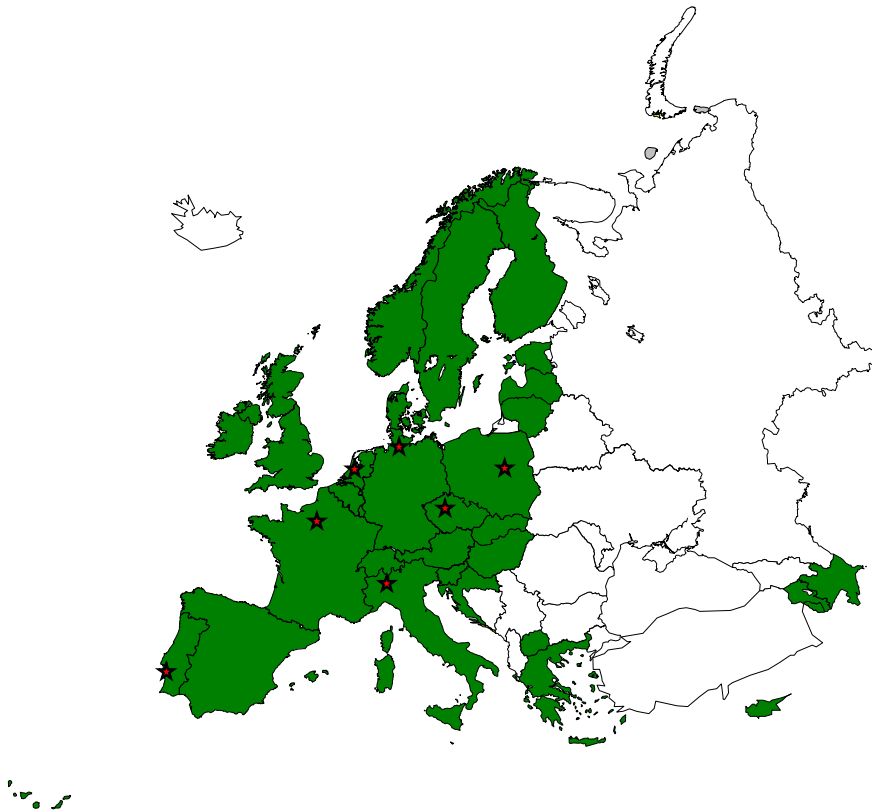
Dates: 28-29 April 2005

Venue: Hotel Riviera, Carcavelos, Portugal

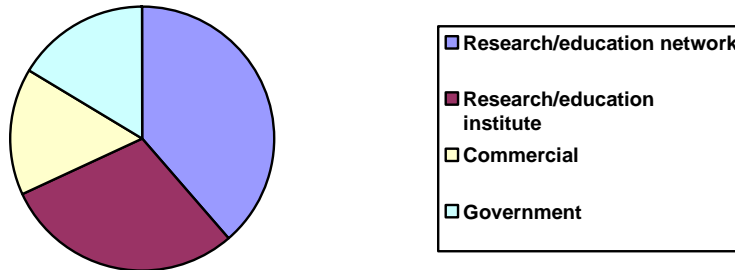
Trainees: 30, from 11 countries

Lecturers: Andrew Cormack (UKERNA), Jan Meijer (SURFnet CERT), Klaus Möller (DFN-CERT) and Don Stikvoort (S-CURE)

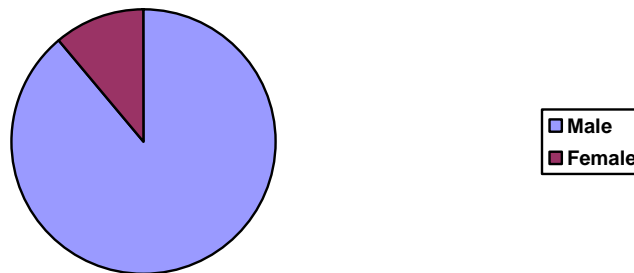
The countries represented at the various workshops can be seen from the map and the graph below:



The constituencies of the CSIRTs of the 153 trainees can be categorised by sector as follows:



By gender, the composition was as follows:



This seems to reflect the proportion of female staff members in CSIRTs in Europe in general. It should be noted that at the managerial level the percentage of women in the CSIRT community appears to be somewhat higher.

3.2. Feedback

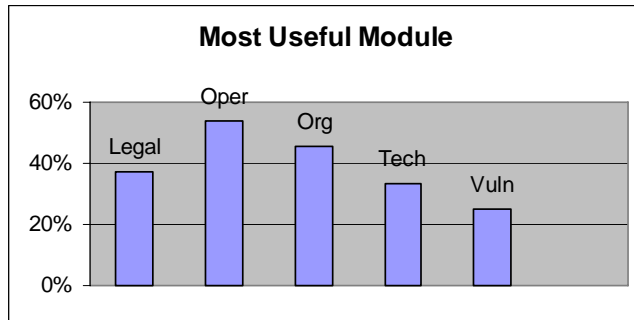
Starting in the summer of 2004, a questionnaire was sent to past students of TRANSITS workshops, to obtain further feedback from them some time after attending the course. This questionnaire aimed to determine the longer-term effectiveness of the training workshops, in particular:

- Whether the content of the course had been useful to trainees in their subsequent work for CSIRTs.
- Whether the course materials (printed slides, handouts, bibliography, course book) had been useful and whether the students could suggest improvements based on their subsequent experience.
- Whether trainees (and their teams) had continued to participate in the CSIRT community.
- What future demand for TRANSITS workshops would be likely.

The questions and responses from participants in the first five workshops (held between October 2002 and November 2004) are summarised below, with comments on changes that could be, or have already been, made as a result. The questionnaire was sent to 101 former trainees, and 24 responses were received.

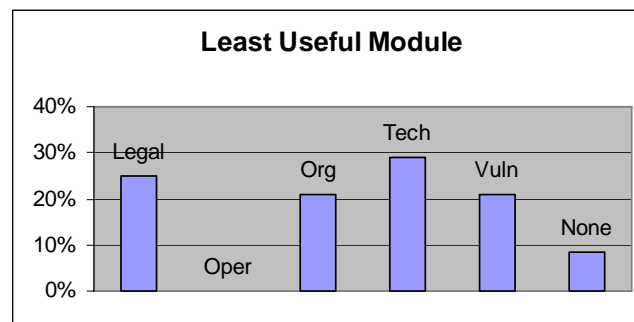
Which module of the course has been of most use?

Some respondents mentioned more than one module as the most useful. The graph shows the percentage of responses that mentioned each of the modules; it appears to indicate no serious problems of lack of relevance. Staff members of well-established CSIRTs are less likely to have an urgent need for the organisational module; operational issues are clearly significant for most CSIRTs; legal, technical and vulnerabilities are likely to be of interest to different team members.



Which module of the course has been of least use?

As might be expected, this graph is roughly the inverse of the one above. However, it is pleasing to see that no one considered that operational issues were irrelevant. Vulnerabilities was mentioned less often than might have been expected from the previous graph, perhaps indicating that it is a field of interest to many CSIRTs but not yet seen as a vital issue.

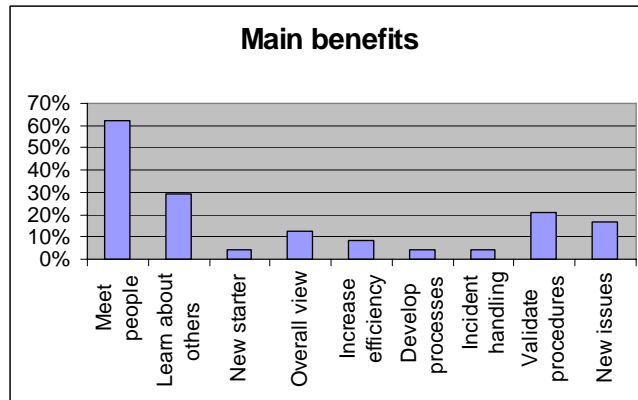


Are there other things you would have liked to have discussed in the workshop?

A wide range of topics was mentioned in responses to this question. However, a third of respondents said there were no other topics, and no response listed more than two issues. Three responses asked for information on forensics and presenting evidence in court and two for more discussion of technical issues. Other topics mentioned were regional/global co-operation, incident handling procedures and tools, PGP, the Incident Response Team (IRT) object in the RIPE database, the Trusted Introducer process for accrediting CSIRTs, handling different types of incidents, secure communication, issues relevant to academic networks, and application security. A number of these were addressed in the major review of the materials half-way through the project; the greatest remaining challenge is probably information about the very specialised area of computer forensics.

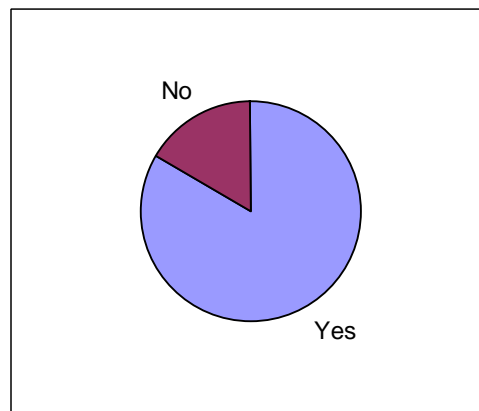
What were the main benefits to you from attending the workshop?

The responses to this open question indicate that the course is achieving its aims of developing the incident response community in Europe and enhancing incident response work. More than half of the responses said that meeting staff of other CSIRTs was a major benefit, the next two most common responses were learning about other teams and gaining a broader view of CSIRT work; a small number specifically said that attending the course had helped subsequent incident co-ordination activities. Other responses indicated that students had indeed applied what they had learned in their own CSIRTs: by validating existing procedures, developing new procedures or even learning about new areas of work.



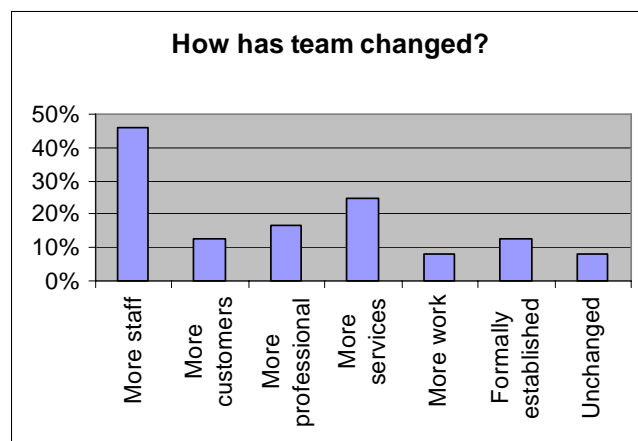
Have you used things you learned on the course to explain issues to others?

The majority of students have spread what they learned from the course to their colleagues. Specific examples quoted included designing systems for incident tracking and handling advisory notices, or developing team policies. One student said that the course materials had helped him to convince his management to set up a national CSIRT framework; two said that the materials had helped them in discussions with Internet Service Providers; and one reported a long discussion in the office on the legal issues affecting CSIRTs.



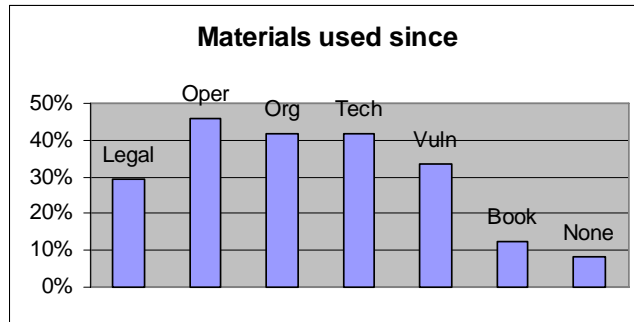
How has your CSIRT developed since the course (new tasks, staff size, funding, etc.)?

Answers to this question show clearly that CSIRTs are growing. Only few teams were unchanged, while half the respondents had had additional staff join their team. Others reported an increase in their customer base or the services offered to them; a significant number felt that their CSIRT had become more professional in its work. Some CSIRTs have been formally established since their staff attended the workshop.



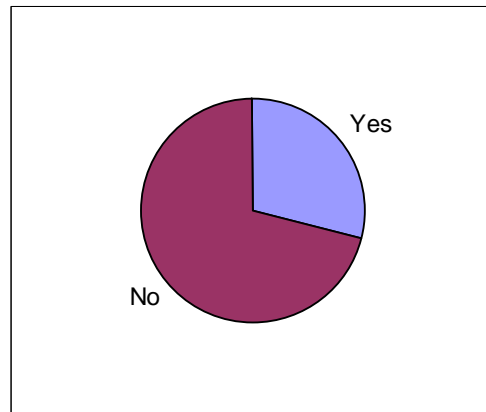
Which parts of the course materials have you looked at since the course?

The vast majority of students had looked at some or all of the course materials since attending. The technical and operational modules contain the most practical detailed information and are therefore likely to be the most frequently used as reference material. It is good to see that the other modules are also consulted by a significant number of trainees.



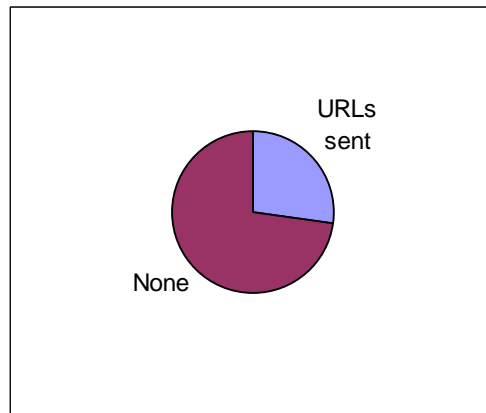
Are there other documents we could have included that would be useful now?

The majority of students seemed to find the materials and bibliography sufficient. Five other documents were suggested: a description of the process of creating an IRT object, more detail on the RFC2350 form for describing an incident response team, a collection of papers on secure programming, examples of workflows and the EISPP format for advisories. All of these have since been added to the slides and bibliography.



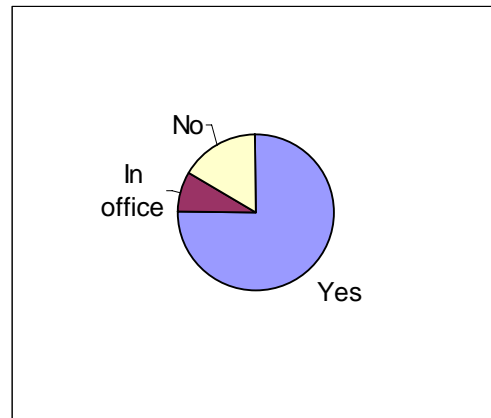
Which websites would you recommend adding to the bibliography?

Again, most students were satisfied with the existing bibliography, but a number sent their own particular favourite references on secure programming, tracing incidents and reporting channels. These will be added to the bibliography where appropriate. Another respondent requested information on government and national CSIRTs: this information is currently being collected by the European Network and Information Security Agency (ENISA).



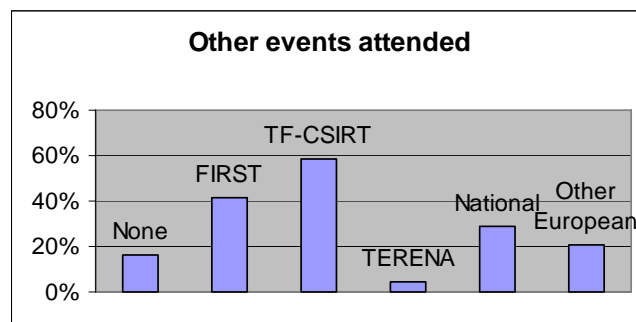
Have you given the materials to other colleagues to read or consult?

Most students had passed the course materials to their colleagues, in some cases they had become part of the office library. Some had used the materials in preparing their own presentations for internal and national presentations on CSIRTs. Two CSIRTs observed that since all their staff had been on the course everyone had their own set.



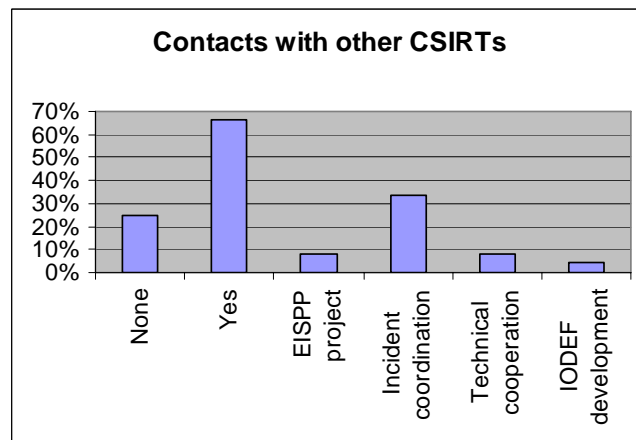
Have you attended any subsequent CSIRT events (e.g. national, TF-CSIRT, FIRST)? If so, which ones?

Almost all the respondents had attended other CSIRT community events, with the majority having attended international conferences or workshops. Particular events mentioned were TF-CSIRT meetings, the TERENA conferences, technical colloquia run by FIRST, the European Government CERTs meeting, the GOVCERT.NL international conference and the European Abuse Forum.



Have you had subsequent contacts with other members of the CSIRT community? If so, please give some examples?

Almost all students have had subsequent contacts with members of the CSIRT community. Not surprisingly the majority of these contacts were in the context of responding to security incidents, but co-ordination of vulnerability announcements and work on data exchange projects were also mentioned. Some students mentioned specifically that they had been in touch with fellow students or tutors whom they had met at the TRANSITS workshop.



Have you recommended the course to colleagues/others?

The only student to answer no to this question explained that all his colleagues were more experienced than he was. This confirms that there is a very high level of satisfaction with the TRANSITS courses.

Do you know of other individuals or organisations who would benefit from the course?

Almost all students felt that there were individuals or organisations who would benefit from TRANSITS training. Specific groups mentioned were ISP abuse teams, CSIRTs, security teams in companies and government institutions.

How many other people from your organisation/country would you expect to be interested in a TRANSITS course in the next year?

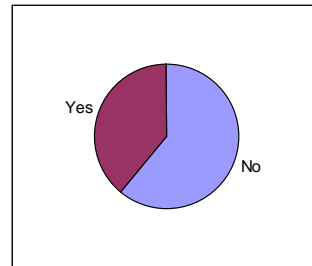
Most of those who answered these questions said that other factors made the number hard to estimate, but it appears that most organisations have at least one person who would be a candidate for TRANSITS training. Only three people were willing to speculate on national demand: these suggested about 10 additional students per country.

Would the TRANSITS materials be useful to educate people in your organisation, country or region?

All replies to this were positive. One commented that translation into local language would be helpful (an offer to do this was received but progress has apparently been slow), another that a workshop with experienced tutors was needed to get the greatest benefit from the materials.

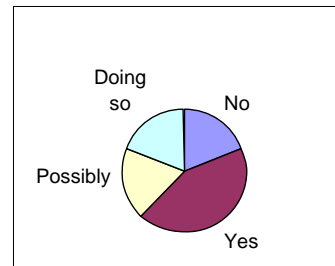
Have you used them in this way?

A significant and welcome minority of students appear to be already using the TRANSITS material in their own training.



Could you help to promote/arrange future courses in your country/region?

The majority of students were willing to help arrange courses, indeed a number were already doing so.



Additional suggestions were that there should be more material on the initial investigation of a suspect computer, and that the technical content might usefully be separated from a workshop purely on creating and managing a CSIRT. Finally, one student suggested a session simulating one or two incident response scenarios; this was added to the last three workshops and was extremely successful.

3.3. Experiences and Lessons Learned

Many useful lessons were learned in organising and presenting the seven training workshops in the TRANSITS project. The experiences gained in arranging and presenting these courses are presented here for the benefit of others who may arrange similar courses in future.

What is CSIRT training?

Since the establishment of the first CSIRT in 1988, incident response teams have succeeded in reducing the impact of security incidents on computers and networks by applying organised incident response processes and techniques. There are now nearly 180 incident response teams that are members of FIRST and probably at least as many other, smaller teams within organisations and networks. In Europe, roughly half the known CSIRTs are members of FIRST. These teams are extremely varied – in size, structure, skills, role, authority and many other factors – indicating that there is no single "right way" to run a CSIRT. Each CSIRT will be run in the way that best serves its parent organisation and constituency. Therefore, a training course on CSIRTs cannot seek to teach a single approach, but must present a variety of principles, experiences and tools to help the students to identify the most suitable approaches for their own situation.

CSIRTs have also found that they must work together, both to resolve incidents that are often international (and usually cross organisational boundaries) and to develop new tools and approaches. Since the work of CSIRTs often involves sharing sensitive information relating to compromises of particular software, systems or organisations, this work needs to be based on a foundation of trust that information shared will not be misused. A certain amount of trust can be achieved through formal or informal agreements between organisations (such as those provided by the FIRST membership process or the European Trusted Introducer framework), but successful CSIRT operations often rely on trust relations between individuals. A second purpose of the TRANSITS training workshops was therefore to introduce students to each other and to well-known members of the European CSIRT community in order to bring them into the existing network of trust relationships within that community.

These two requirements – to present experiences rather than a single, known, approach and to develop trust relations – require a particular approach to training. In the TRANSITS project it was found that these requirements guided choices of presentation methods, tutors, students, class sizes and even the locations chosen to deliver the training. One of the first decisions was that the training needed to be delivered face-to-face, rather than by any form of distance learning, to provide the right environment both for students to develop ideas for their own circumstances and to get to know each other and the lecturers. This provides the basis for subsequent on-line discussions and support.

Training methods

The TRANSITS courses presented a great deal of material in two days. If possible, the course might be better presented over a longer period, but the more intense schedule was chosen to reduce the time that students and the volunteer trainers needed to spend away from their offices.

To help trainees (and trainers) maintain their concentration, the course schedule was deliberately planned to include a variety of styles of learning: formal presentations and exercises where students worked in pairs or small groups, as well as informal discussions over coffee, meals and in the evenings. The exercises and informal discussions were particularly valuable to help students develop their own skills and explore how the ideas presented might be best applied in their own organisations. For example, in the operational exercise students were encouraged to work on an Incident Response Plan for their own organisation: a specific document that could be taken home, developed and used after the course. In the technical module, trainees were invited to analyse various network and system logs to develop their own skills at determining what had happened and how serious the consequences of the activity might be for the organisation.

During the lifetime of the TRANSITS project, additional sessions were added at the request of students and lecturers where these helped to address the overall aims of the training. Tutors were encouraged to present and discuss their own current projects in short informal sessions. These ranged from incident tracking tools and applying incident response techniques via Grid computing to working on a real incident, and aimed to involve students in the variety of work that incident response staff really do, as well as to provide useful discussion and feedback to the tutors. The aim of developing the network of trust was supported by a PGP key-signing event, where students' identities were checked and certified by digital signatures that the students can use in future to prove their identities when working across the Internet with other members of the CSIRT community. A session that students found particularly valuable was an informal workshop on the final evening, where by role-playing various incident response scenarios (adapted from the National Institute of Standards and Technologies "Computer Security Incident Handling Guide") the students could apply what they had learned in the course to the context of a particular type of incident. The scenarios used were chosen to raise issues from all five of the course topics: highlighting the need to think broadly about an incident rather than concentrating on a single aspect.

Since the aim of the course is to encourage students to think about what they have learned it is also important to offer them continuing support after the course. Students and lecturers were encouraged to exchange e-mail addresses and it is known that a number of discussions have taken place between tutors and trainees after the courses, both by e-mail and at other events. A mailing list was created for each course to which the teachers and students subscribed.

Tutor requirements

The nature of the training places particular requirements on the lecturers. These are certainly not subjects that can be taught by reading the slides and speaker notes. Indeed, it is not clear that "teaching" is the right approach in any case: the aim should be to help students develop their own ideas, rather than to impart any particular package of knowledge.

Tutors must have experience of working in CSIRTs, both to be able to guide the students and because illustrating the materials with real-life experiences makes the training much more effective. It is helpful if tutors can present a range of experiences of different CSIRTs and types of CSIRTs – in the TRANSITS training workshop there were lecturers from educational, commercial and government teams. This reminds students that every CSIRT is different and provides them with a range of solutions to assess and learn from.

Tutors need to be flexible: able and willing to assess ideas from students and help the students develop them. Newcomers to the CSIRT world may often be the best placed to see novel and effective approaches and the course should provide a safe and helpful environment to propose and discuss these. Lecturers should be willing to learn from trainees, as well as the other way around.

Presentation skills are important, especially in international groups where tutors and students may not be speaking their native language⁴. Some CSIRT staff are already experienced presenters, and these skills can be developed through courses or just experience and constructive feedback. Before using a lecturer whose experience of presenting is limited or unknown, the course organiser should check that the individual is able to present the material effectively and, where necessary, offer help in developing the necessary skills. For TRANSITS courses, the tutors also need to be able to encourage each student to contribute as much as possible: in some cases this may require sensitivity to different cultures and styles of learning.

Student requirements

The TRANSITS materials concentrate on those topics that are specifically relevant to CSIRT work, and therefore assume a significant amount of knowledge as a prerequisite. In particular, students need to have an awareness of the security issues involved in connecting computers to the Internet and the possible impact of a security breach. For the technical parts of the course, familiarity with normal operation of TCP/IP networks, addresses, port numbers and protocols are assumed. Typical students will have experience as system, network or IT managers, although staff from other backgrounds who had reasonable technical awareness have also been able to follow the course. Above all, students must be committed to using their skills to improve the security of computers and networks. Within the TRANSITS project it did not prove necessary to have a formal list of the assumed prior knowledge; instead each student was asked to provide a short curriculum vitae with their application, and the suitability of their prior knowledge was assessed from this. On the rare occasions when students were considered unsuitable and had to be turned down for the courses it was considered important to offer them alternative assistance.

Students also need to be prepared to think outside their own area of expertise. In dealing with computer security incidents it is rare to be able to separate technical and organisational issues; this can be challenging for individuals who spend their working life in one or other mode. Technical staff may be resistant to the idea of developing and following set incident response procedures, even though these provide a way to remove the drudgery of routine actions. They may also be surprised to learn that many incidents have non-technical causes and solutions: a Web server defacement resulting from a poor choice of administrator password cannot be prevented by technical means, nor will the problem go away when the server has been restored to a technically secure state. Those with a management mindset may well be disappointed to learn that security incidents are rarely "solved" – very often it will be impossible to even identify the intruders, let alone punish them, and the best that can be achieved is for the organisation to learn and resolve to do better next time.

⁴ An interesting observation from a number of TRANSITS feedback forms was that presenters who were not native English-speakers could be easier to understand than those who were presenting in their own first language.

Students need to be prepared to discuss their ideas, and ideally to talk about how these fit into their own organisations. The course will be most effective if it allows students to try out ideas for their own organisations and obtain constructive comments on them. As this may involve revealing sensitive information about individuals or organisations, it is best to agree on the standard confidentiality rules early in the course. Two existing standards may be helpful, depending on the members of the group: the rules of FIRST allow information to be shared within FIRST member teams, but no further; the "Chatham House Rule" allows information to be shared so long as it is not attributed, either explicitly or implicitly, to a particular individual, organisation or country. In a few cases it may be necessary to agree that information will not be repeated at all outside the group of workshop participants. Whatever rule is agreed should be the standard: if a tutor or student wishes a different rule to apply to a particular piece of information, they should state this in advance. Sharing of information or experiences can often be helped if the tutors take a lead: demonstrating that it is safe to discuss incidents and mistakes can be very encouraging to others.

Class size and structure

The choice of class size and groups can have a significant impact on how a training course will progress. This has been the topic of much discussion during the TRANSITS project. The use of TRANSITS materials in other continents has also brought home how much these issues depend on local culture. The points below are based on the European experience.

The size of group greatly affects the styles of learning that are possible:

- Intense interaction, where all the members of a group work together on a problem, is only likely to be possible in small groups. With more than about six members, a group is likely either to split or else to develop its own internal structure, both of which are likely to change the way the group works. The exercises in the operational and organisational modules of the TRANSITS course are designed for small groups; the exercises in the technical module, where students are looking in detail at logfiles or other evidence gathered from computers, are suited to groups of two or three, where students can share the same printout and point out significant features to one another. For group exercises it is best if the students can sit in a circle, around or across a small table.
- Discussion facilitated by the tutor can take place in larger groups, up to about twelve to fifteen people. In this size of group it should be possible for everyone to contribute, but a leader is likely to be needed to guide the discussion and ensure that all students are able to make their points. In the TRANSITS workshops, all materials were presented in two parallel groups to ensure that both groups were no larger than this. For discussion it is important that students can see one another, so seating around a U-shaped table was the most effective.
- Once a group contains more than about twenty students, it is likely that a presentation will become a lecture, with the tutor providing most of the input and students asking occasional questions. For reasons of space, the only practical seating arrangement is likely to be rows of seats facing the front, which means it is hard for students to interact with one another. If this style of presentation is used, the organisers should ensure that there are other opportunities for students to discuss issues either with the tutors or with each other.

It may be possible to move between these styles of learning in a single session. For example, the informal scenario exercise was done with the full group of up to 30 students together, but seated in sub-groups of about eight people around individual tables. This allowed the scenario to be explained to the whole group, but discussion to take place in smaller groups.

The allocation of students to groups can also affect the type of discussion and learning. In the TRANSITS project the choice was to make all courses and groups as diverse as possible. Students from the same organisation were split between groups so that the organisation received ideas from as many sides as possible. People with the same nationality or first language were also divided over different groups to prevent a small set of people discussing in their own language and excluding others.

Choice of venue

The TRANSITS workshops were planned to provide intense training, with the maximum possible learning fitted into the time available. Since informal discussions were felt to be important, the chosen venues had to ensure that students and tutors met together outside the formal schedule as well as during the timetabled hours. Where possible, therefore, venues were chosen that could provide all requirements for 50 hours in a single location. This meant that teaching, sleeping, eating and meeting areas should be close together, ideally with few other distractions to tempt the group to split up. Good food and drink help to create a productive environment. Small hotels or conference centres with their own grounds were found to be the best way to meet these requirements.

The TRANSITS workshops required venues with at least two training rooms: one capable of seating the whole group and one smaller one for the parallel sessions. As discussed above, it was helpful to vary the seating arrangements for different sessions. The acoustics of training rooms vary considerably, so it is important to check periodically that all students can hear the presenters clearly, especially when they are not speaking or listening in their first language.

Internet connectivity can be a mixed blessing. It can be very useful to access on-line resources relevant to the course material or to students' questions, and also helps tutors and students to keep in touch with their offices. However, the availability of Internet connectivity can also become a distraction. It appears there are still considerable differences between the connectivity that can be expected in hotels in different countries and regions in Europe. At each of the seven TRANSITS workshops, wireless access to the Internet was set up by the organisers, but the bandwidth available varied from ISDN to Ethernet speeds and on some occasions it required considerable technical expertise and ingenuity to set up the connectivity.

It was also important that students and tutors are able to travel to and from the workshop venues relatively easily using public transport. Locations were therefore chosen near major airports but outside city centres to avoid distractions.

Preparation and schedule

Travel arrangements were one of a number of areas where good preparation and information helped students to get the best out of the course. Detailed instructions were provided in advance on how to get from local airports or train stations to the venue, and a phone number was provided in case unexpected problems would occur. All practical information was sent by e-mail to students about a fortnight before the course, along with the operational and organisational exercises.

TRANSITS workshops were originally scheduled to take the least possible time to deliver the materials. This meant that the participants arrived at the venue on the evening before the first day and left at the end of the second day. A number of students commented that this meant they had to leave just as their discussions were becoming productive, so the last three workshops were extended to include a review session, in the form of a group exercise based on incident response scenarios, on the evening of the second day, with the students leaving the next morning. This change was very successful, with the final session being rated one of the most useful on nearly all feedback forms. This change to the schedule also removed the pressure to finish the afternoon sessions on the second day by a particular time.

Conclusions

The aim of the TRANSITS workshops was to train new staff for existing and new CSIRTs, both by developing their knowledge and skills of CSIRT work and by introducing them into the international CSIRT community. The small-group style of learning that was adopted was successful in both aims: many of the students are now active members of incident response teams and participate in national and international working groups. The mixture of technical and management topics appears to have broadened the outlook of many – as one student commented on his way home: "I'm a techie, but this management stuff looks interesting".

4. OTHER DELIVERIES OF THE COURSE MATERIALS

The TRANSITS project has encouraged the use of the course materials in other training events besides the workshops organised by the project itself. The TRANSITS slides, handouts and other materials are copyright TERENA⁵. The whole, or parts of these materials may be used, unaltered, for non-commercial training courses provided their origin is acknowledged and permission is obtained from TERENA. These arrangements promote the widespread use of the material while avoiding monopolisation of the information, misuse or commercial exploitation.

Organisations or individuals who apply for permission to use the course materials are requested to provide the following information:

- A statement that the training course for which the TRANSITS materials will be used will be non-commercial, i.e. that the income from the event will not be higher than is necessary to recover the direct costs of the organisers and the presenters of the course.
- The names and affiliations of the presenters of the training course; at least one of them needs to have very recent experience as a member of a professional CSIRT.
- The dates and location of the training course.
- The expected number of trainees in the course and the type of organisations that they are working for.

TERENA gives permission for the use of the training materials under the following conditions:

- The presenters will only use the most recent versions of the TRANSITS materials and will enquire shortly before the training event about any latest updates.
- Within three weeks after the training course the organisers will submit a report to TERENA. This report should include: the dates and location of the training course, the names and affiliations of the presenters, if possible the names and affiliations of the trainees (and in any case their number, the nature of their functions and the organisation(s) that they are working for), and feedback from the presenters and from the trainees on the TRANSITS materials.

4.1. Other Training Workshops

During the lifetime of the TRANSITS project, the TRANSITS materials were used a number of times at training workshops and other events, after permission had been obtained from TERENA following the procedure described above. The list of events is as follows:

Dates: 24-25 July 2002
Venue: Aston University, Birmingham, United Kingdom
Trainees: 18 staff members of higher education, further education and research sites connected to the JANET network
Lecturers: Andrew Cormack and Garaidh Cochrane (UKERNA)
Presentation of the full course

Dates: 15-16 January 2003
Venue: Thistle Hotel, London, United Kingdom
Trainees: 20 staff members of higher education, further education and research sites connected to the JANET network
Lecturers: Andrew Cormack (UKERNA)
Presentation of the full course

⁵ Individual authors and their employers may also hold copyright in individual items.

Dates: 8-9 April 2003
Venue: Amsterdam Medical Centre, Amsterdam, the Netherlands
Trainees: 12 staff members from (higher) education sites connected to the SURFnet network
Lecturers: Andrew Cormack (UKERNA), Jan Meijer (SURFnet), Klaus Möller (DFN-CERT) and Jacques Schuurman (SURFnet)
Presentation of the full course

Dates: 24 June 2003
Venue: Westin Hotel, Ottawa, Canada
Andrew Cormack (UKERNA) presented the vulnerabilities module to about 100 delegates at the FIRST Incident Handling Conference 2003.

Dates: 15-16 July 2003
Venue: IoD Hub, Bristol, United Kingdom
Trainees: 17 staff members of higher and further education organisations connected to the JANET network
Lecturers: Andrew Cormack and Tom Meyer (UKERNA)
Presentation of the full course

Dates: 16 January 2004
Venue: Montpellier, France
Trainees: 19 staff members from research and education networking organisations in the Mediterranean region (Algeria, Cyprus, Israel, Malta, Morocco, Syria and Tunisia)
Lecturers: Stelios Maistros and Nikos Fouteris (GRNET)
The TRANSITS materials were used in a one-day session on network security and CSIRTs as part of a workshop organised by the EUMEDCONNECT project.

Dates: 24-26 August 2005
Venue: Tblisi, Georgia
Trainees: 7 staff members from national research and education networking organisations in Azerbaijan, Georgia and Armenia
Lecturers: Przemyslaw Jaroszewski (CERT Polska), Mirosław Maj (CERT Polska) and Jacques Schuurman (SURFnet)
The full course was presented in a three-day workshop. The module-specific exercises were replaced by a single "Grand Exercise", designed as a role play for all participants.

Dates: 31 August – 1 September 2005
Venue: Brussels, Belgium
Trainees: 6 staff members from organisations connected to the BELNET network
Lecturer: Lionel Ferette (BELNET)
Presentation of the full course

Dates: 29-30 September 2005
Venue: Brussels, Belgium
Trainees: 8 staff members from organisations connected to the BELNET network
Lecturer: Lionel Ferette and Koen Van Impe (BELNET)
Presentation of the full course

4.2. Training Workshops in Other Continents – Collaboration with FIRST

FIRST⁶, the Forum of Incident Response and Security Teams, is the principal international organisation representing CSIRTs worldwide. FIRST was formed in 1991 and has grown to over 170 member organisations from national, governmental, educational and commercial organisations in countries all around the world. FIRST is overseen by a Steering Committee whose members are elected by the FIRST membership; administrative duties are performed under contract by the FIRST Secretariat.

FIRST seeks to encourage and support the development of new CSIRTs in all regions and sectors, and has identified the lack of affordable training as a significant hindrance to the development of security teams. This applies particularly in Latin America and the Asia-Pacific region, where governments and other organisations are willing to set up CSIRTs⁷, but do not have ready access to training and expertise to assist them. FIRST has therefore contacted the TRANSITS project, to discuss collaboration.

As a result of the talks between FIRST and TRANSITS in May-June 2004, an agreement was reached whereby FIRST has received permission to use the TRANSITS materials under the same conditions as described above. Conversely, FIRST committed to hold at least one training course per year in Latin America and at least one course per year in the Asia-Pacific region, and to build regional and specialist modules around the core curriculum of the TRANSITS modules.

In order to create a pool of lecturers for these training workshops outside Europe, "Train the Trainers" workshops were organised at the annual FIRST conferences in Budapest in June 2004 and in Singapore in June 2005. The first regional training workshops organised under the auspices of FIRST took place in Rio de Janeiro in November 2004, in Guilin (China) in March 2005, and in Seoul in August-September 2005. In addition, graduates from the "Train the Trainers" courses delivered the materials at events in Mozambique in April 2005 and in Mexico in May 2005.

First "Train the Trainers" workshop

Dates: 18-19 June 2004
Venue: Budapest, Hungary
Trainees: 12 staff members of CSIRTs in Latin America and the Asia-Pacific region. These participants had been selected by FIRST as regional trainers.
Lecturers: Andrew Cormack (UKERNA), Jaap van Ginkel (University of Amsterdam), Klaus Möller (DFN-CERT) and Don Stikvoort (S-CURE)

Second "Train the Trainers" workshop

Dates: 25-26 June 2005
Venue: Singapore
Trainees: 17, from Australia, Canada, China, Hong Kong, Japan, Korea, Malaysia, the Netherlands and Japan
Lecturers: Andrew Cormack (UKERNA), Ulrich Kiermayr (ACOnet CERT), Klaus Möller (DFN-CERT) and Don Stikvoort (S-CURE), with assistance from Georgia Kilcreece and Robin Ruefle (CERT-CC)

⁶ For more information about FIRST, see www.first.org/

⁷ For example, the ten members of ASEAN (the Association of Southeast Asian Nations) aim to set up a national CSIRT for each country by 2005.

First regional training workshop for Latin America, under the auspices of FIRST

Dates: 26-27 November 2004
Venue: Rio de Janeiro, Brazil
Trainees: 18, from Argentina, Bolivia, Brazil, Chile, Costa Rica, Ecuador, El Salvador, Guatemala, Mexico, Nicaragua, Panama, Peru, Spain and the United Kingdom. Most of the trainees were management and technical staff from national research and education networks who have created their own CSIRT or are intending to do so.
Lecturers: Juan Carlos Guel Lopez (UNAM-CERT), Jacomo Boca Piccolini (CAIS/RNP) and Liliana Velásquez Solha (CAIS/RNP)

First regional training workshop for the Asia-Pacific region, under the auspices of FIRST

Dates: 22-23 March 2005
Venue: Guilin, China
Trainees: 91, mostly from China with small numbers of participants from Australia, Brunei, Cambodia, Korea, Laos, Myanmar and Singapore
Lecturers: David Crochemore (CERTA), Mark McPherson (AusCERT), Don Stikvoort (S-CURE) and Arnold Yoon (KrCERT/CC)

Second regional training workshop for the Asia-Pacific region, under the auspices of FIRST

Dates: 29 August – 2 September 2005
Venue: Seoul, Korea
Trainees: 27, from Cambodia, China, Indonesia, Laos, Malaysia, Myanmar, the Philippines, Taiwan and Thailand
Lecturers: Jinhyun Cho (KrCERT/CC), Yuejin Du (CNCERT/CC), Jamie Gillespie (AusCERT), Robert Lowe (AusCERT) and Arnold Yoon (KrCERT/CC)

The full course was presented as part of a five-day workshop, which also included introductions to relevant organisations in Korea and site visits.

Other course deliveries:

Date: 24 April 2005
Venue: Maputo, Mozambique
Trainees: 9, from Angola, Mozambique and Kenya
Liliana Velásquez Solha (CAIS/RNP) used the TRANSITS operational and organisational modules as the basis for a half-day tutorial at an AFNOG (African Network Operators Group) workshop.

Date: 25 May 2005
Venue: Mexico City, Mexico
Juan Carlos Guel Lopez (UNAM-CERT), Jacomo Boca Piccolini (CAIS/RNP), Francisco Monserrat Coll (IRIS-CERT) and Liliana Velásquez Solha (CAIS/RNP) presented the organisational, operational and technical modules to about 60 delegates at a computer security conference organised by the National Autonomous University of Mexico (UNAM).

5. FOLLOW-UP OF THE TRANSITS PROJECT

As part of the TRANSITS project, project partners TERENA and UKERNA have taken on the obligation to create a suitable permanent framework for the further maintenance and updating of the course materials after the completion of the project, and the continued delivery of training courses in Europe. These arrangements have been the topics of discussions with FIRST, which have taken the larger part of the first half of the year 2005.

An agreement was reached towards the end of June, which has been laid down in a Memorandum of Understanding between TERENA and FIRST.Org, Inc. In the Memorandum of Understanding, FIRST.Org, Inc. commits to make additional funding available to the FIRST Secretariat, so that it can take on new tasks related to CSIRT training.

The FIRST Secretariat, a function provided by S-CURE B.V. in the Netherlands, will enlist the assistance of volunteer experts from the international CSIRT community who will regularly provide updates of the TRANSITS course materials. The FIRST Secretariat will act as the final editor of the updates of the course materials, integrating the contributions from the volunteer experts and guarding the completeness and consistency of the materials as a whole.

FIRST.Org, Inc. takes responsibility for organising at least three training workshops per year outside Europe, which will cover all five core subjects of the TRANSITS materials: technical issues, legal issues, vulnerabilities, organisational issues and operational issues. At least one of these training workshops will be held in Central or South America, and at least one of them will be held in the Asia-Pacific region. The organisation of these workshops will be handled either by the FIRST Secretariat or by volunteers from the FIRST membership with assistance from the FIRST Secretariat.

TERENA and FIRST.Org, Inc. jointly take responsibility for organising at least two training workshops per year in Europe. The logistic organisation of these events – including the selection of venue and the financial arrangements – will be handled by the TERENA Secretariat, while the FIRST Secretariat will take care of the programme of the workshops, including the invitation of the lecturers.

CTR (05) 00

TSao(05)04rev1

MEMORANDUM OF UNDERSTANDING

between

TERENA and FIRST.Org, Inc.

**on the provision of training to CSIRT staff members
using the TRANSITS materials**

Whereas TERENA (the Trans-European Research and Education Networking Association) is the Co-ordinator of the TRANSITS (Training of Network Security Incident Teams Staff) project in the 5th Framework Programme for Research and Technical Development of the European Union;

Whereas TERENA has taken responsibility for creating a suitable permanent framework and identifying a suitable organisation for delivering further training courses and regularly updating the course materials after the end of the TRANSITS project;

Whereas FIRST.Org, Inc. (FIRST) as the representative of the global Forum of Incident Response and Security Teams is committed to organise training for Computer Security Incident Response Team (CSIRT) staff members worldwide;

TERENA and FIRST have agreed as follows:

1. FIRST takes responsibility for the maintenance and updating of the TRANSITS course materials after the end of the TRANSITS project (30 September 2005):
 - The FIRST Secretariat, advised by TERENA, will enlist the assistance of volunteer experts (at least two per TRANSITS course module) from the international CSIRT community who will regularly provide updates of the TRANSITS course materials to the FIRST Secretariat.
 - The FIRST Secretariat will act as the final editor of the updates of the TRANSITS course materials, integrating the contributions from the volunteer experts and guarding the completeness and consistency of the materials as a whole.
 - The FIRST Secretariat will make the latest updated version of the TRANSITS course materials available to organisations or individuals who have received permission from TERENA to use the TRANSITS materials for training courses on the basis of the procedures described in the Annex to this Memorandum of Understanding.
 - FIRST will provide the FIRST Secretariat with sufficient funding to cover the costs of its work for the maintenance and updating of the TRANSITS course materials, estimated at 15 man-days per year.
2. FIRST takes responsibility for organising at least three training courses per year outside Europe, covering all five core subjects (technical issues, legal issues, vulnerabilities, organisational issues and operational issues) of the TRANSITS training course. At least one of these three training courses will be held in Central or South America, and at least one of these three training courses will be held in the Asia-Pacific region.
 - The FIRST Secretariat will maintain a schedule of past and planned training courses organised under the auspices of FIRST, including dates, locations, organizers and lecturers.
 - The organisation of the training courses - including logistic arrangements, invitation of lecturers, selection of participants - may be handled either by the FIRST Secretariat or by volunteers from the FIRST membership with assistance from the FIRST Secretariat. In the latter case, the FIRST Secretariat will monitor the organisation of the training course to ensure that FIRST's commitments are met.
 - For each training course, the organiser will request permission from TERENA to use the TRANSITS materials for the training course, following the procedure described in the Annex to this Memorandum of Understanding.

j.d.

L.P.
UK

The copyright of the TRANSITS course materials will remain with TERENA. Organisations or individuals may obtain permission from TERENA to use the TRANSITS course materials, provided that the materials will be used only for non-commercial training purposes. Another condition is that TERENA will receive a report on the course delivery with feedback from the presenters and the trainees; this will be of great use for keeping the course materials relevant and up to date.

The agreement between TERENA and FIRST.Org, Inc. is initially for a period ending on 31 October 2006. In September 2006, the two organisations will evaluate the agreement, and depending on the result of the evaluation they will seek to conclude a new, longer-term agreement, which is expected to enter into force on or before 1 November 2006.

These new arrangements will officially be implemented starting immediately after the completion of the TRANSITS project, i.e. from 1 October 2005. However, TERENA and the FIRST Secretariat have already been working together during the last months of the TRANSITS project lifetime to prepare for the future form of collaboration. This includes setting up the organisational framework for the collaboration between the staff of the two organisations and for the organisation of training workshops in Latin America and the Asia-Pacific region, as well as the preparations for the first "after-TRANSITS" training workshop in Europe. That workshop is planned to be organised in Vienna in November 2005, with financial sponsorship from the Austrian ISP association ISPA.

- The training courses will be non-commercial, i.e., the income from the event will not be higher than is necessary to recover the direct costs of the organisers and the presenters of the course (including the costs of the work by the FIRST Secretariat for the organisation of the event).
 - Persons who have successfully completed a training course organised under the auspices of FIRST will receive a certificate, which will be produced by the FIRST Secretariat.
 - FIRST will provide the FIRST Secretariat with sufficient funding to cover the costs of its work for the organisation of training courses outside Europe, estimated at 18 man-days per year.
3. TERENA and FIRST jointly take responsibility for organising at least two training courses per year in Europe, covering all five core subjects (technical issues, legal issues, vulnerabilities, organisational issues and operational issues) of the TRANSITS training course.
- The dates of the training courses will be agreed between TERENA and the FIRST Secretariat, the logistic organisation of the training courses - including selection of venue and financial arrangements - will be handled by TERENA, the organisation of the programme of the training courses - including the invitation of lecturers - will be handled by the FIRST Secretariat, and the selection of participants will be done jointly by TERENA and the FIRST Secretariat.
 - The training courses will be non-commercial, i.e., the income from the event will not be higher than is necessary to recover the direct costs of the organisers and the presenters of the course (including the costs of the work by TERENA and by the FIRST Secretariat for the organisation of the event).
 - Persons who have successfully completed a training course organised by TERENA and the FIRST Secretariat will receive a certificate, which will be produced by the FIRST Secretariat.
 - FIRST will provide the FIRST Secretariat with sufficient funding to cover the costs of its work for the organisation of training courses in Europe, estimated at 12 man-days per year.
4. The copyright of the TRANSITS course materials will remain with TERENA. Organisations or individuals may request permission from TERENA to use the TRANSITS course materials, following the procedure described in the Annex to this Memorandum of Understanding.
5. This Memorandum of Understanding is initially for a period ending on 31 October 2006. TERENA and FIRST share the vision that, depending on the results of this initial trial period, they will want to enter subsequently into a long-term arrangement, which will be governed by the following principles:
- The goal of the partnership will be for FIRST to deliver training courses based on the TRANSITS materials throughout the world, with deliveries in European being co-supported by TERENA, and to continue to ensure the quality of the TRANSITS materials.
 - While TERENA retains the copyright of the TRANSITS materials, FIRST will be given a non-exclusive, non-commercial, unlimited, non-transferable right to use these materials.
 - To ensure continuity and quality of service, FIRST will handle the TRANSITS activities as a regular task of its Secretariat.
- This Memorandum of Understanding will be evaluated by TERENA and FIRST in September 2006. Taking into account the results of this evaluation, TERENA and FIRST will seek to conclude a new longer-term agreement, which will enter into force on or before 1 November 2006.

Signed:

on behalf of TERENA,
at Amsterdam
on 12 July 2005


Karin Vieschi,
Secretary General



on behalf of FIRST.Org, Inc.,
at Singapore
on Thursday, 30 June 2005


Klaus-Peter Kosakowski,
President

21