Cyber Defence East Africa 2013

Nashera Hotel, Morogoro, Tanzania

28th-30th August

Intensive three-day training on Critical Security Controls or Penetration testing for information security professionals, information systems auditors, IT risk professionals and IT enthusiasts. Showcase of state-of-art technologies.

INVITATION

NRD Norway Registers Development

ISACA
Trust in, and value from, information systems
Tanzania Chapter

Letter from organisers

Dear Participant,

On behalf of ISACA Tanzania Chapter and Norway Registers Development AS, we would like to invite you to attend the **Cyber Defence East Africa 2013** conference which will be taking place on the **28th-30th August in Morogoro, Tanzania.**

The importance of cyber security in Tanzania is increasing due to country's rapid development. More and more businesses and government institutions are conducting their activities online and, therefore, relying heavily on information technology. Smooth business activity often depends on a smooth functioning of IT infrastructure: inoperative applications, such as financial systems, e-mail or any other kind of database failure may cause many problems, lead to financial loss or even disrupt the activities of an organization. Rise in mobile money transactions, increasing importance of data and IT infrastructure's availability also heighten security concerns.

Furthermore, the scope, dynamics, and harm to organisations inflicted by cyber attacks have been intensively growing during the last years. The nature of the threats has changed significantly: before random attacks were dominant, now - targeted to certain persons or their groups, organisations. Cyber-crime is getting more industrialised, data leakage is becoming especially frequent.

As a consequence, international community is uniting and seeking for cooperation in order to stop cyber-crimes. European experience is very important for East Africa because manifestations of similar cyber threats are already present (data leakage, DDoS, resilience issues) while readiness to withstand them is still very low.

In order to assist organisations in creating a secure digital environment in Tanzania and whole East African region as well as maintaining trust of both citizens and foreign investors, ISACA Tanzania Chapter together with Norway Registers Development AS is organising intensive three-day **training** on **critical security controls** or **penetration testing** for information security professionals, information systems auditors, IT risk professionals and IT enthusiasts.

This event will help to get organizations up to speed in information security and prepare them to react appropriately and minimize the damage in case of a security incident. Motivating educational programmes are designed with a reference to the best security practices, standards of business ethics, legal regulations and principles of business continuity. Introductory security courses educate on the current cyber threats, the attack cycle, defence techniques, risk management, forensic challenges and incident response planning among many other things. Furthermore, during the event the biggest, industry leading cyber security vendors will showcase their state-of-art technologies. In addition, participants will have networking opportunities with colleagues from Tanzania, Kenya, Uganda and Zambia during unofficial meetings and the Gala Dinner. **Finally, participating in this event will also offer an opportunity to earn 24 CPE hours.**

We believe that your participation in this conference will bring many benefits both to you and to your respective organisations. **Therefore, we are really looking forward to seeing you there.**

Yours Sincerely,

CDEA'13 organising committee

P.S. In this package you will find full conference agenda, training descriptions, speaker profiles, registration details and all other relevant information.

AGENDA

Day 1. 28th August, 2013

Time	Day 1	
9:00 - 10:00	Arrival, registration and coffee	
10:00 - 10:30	Opening speech — Hon. January Y Makamba	
10:30 - 11:00	Keynote speech - Boniface Kanemba (ISACA)	
11:00 - 11:30	Second keynote speech— Gold sponsor	
11:30 - 12:00	Tea Break	
12:00 - 13:30	Track 1	Track 2
13:30 - 14:30	Lunch	
14:30 - 16:00	Track 1	Track 2
16:00 - 16:30	Lunch	
16:30 - 18:00	Track 1	Track 2

Day 2. 29th August, 2013

Time	Day 2	
9:00 - 10:00	SIEM Demo	APT Protection Demo
10:00 - 11:30	Device control and patch and remediation Demo/ GRC Demo	Kill abuse of unstructured data Demo
11:30 - 12:00	Tea Break	Tea Break
12:00 - 13:30	Track 1	Track 2
13:30 - 14:30	Lunch	Lunch
14:30 - 16:00	Track 1	Track 2
16:00 - 16:30	Lunch	Lunch
16:30 - 18:00	Track 1	Track 2
20:00 - 23:00	Gala Dinner	Gala Dinner

Day 3. 30th August, 2013

Time	Day3	
9:00 - 10:00	Forensics Demo	Vulnerability Management Demo
10:00 - 11:30	Universal Threat Management Demo	Privileged User Supervision Demo
11:30 - 12:00	Tea Break	Tea Break
12:00 - 13:30	Track 1	Track 2
13:30 - 14:30	Lunch	Lunch
14:30 - 16:00	Track 1	Track 2
16:00 - 16:30	Lunch	Lunch
16:30 - 18:00	Track 1	Track 2

Keynote speakers

We are delighted to present you two prominent personalities that will open our conference. They will look into the topic of cyber defence with a reference to their own specific fields of expertise.

Hon. January Y Makamba,
Tanzania MP & DM — CST.

Hon. January Yusuph Makamba is the Deputy Minister - Communication, Science & Technology at The Government of The United Republic of Tanzania, a Ministry which is responsible for policy making for Information Communication Technology, including cyber security matters.

Hon. Makamba is also a Member of Parliament (MP) for Bumbuli constituency in the Tanzanian National Assembly. He also serves as Politics & Foreign Relations Secretary at Chama Cha Mapinduzi (CCM). Prior to this post Honorable Makamba worked as Senior Aide to the President at The Presidency, United Republic of Tanzania.

Hon. Makamba holds Master of Science (M.Sc.), Conflict Analysis and Resolution and Bachelor's degree, Peace Studies and Conflict Resolution both from United States.

During the opening ceremony of the CDEA'13 Hon Makamba will deliver a speech on "Cyber Security in Tanzania – Government perspective".

Boniface Kanemba,
ISACA Tanzania
Chapter President.

Mr. Boniface Kanemba is a Senior Systems Auditor and the President of ISACA Tanzania Chapter, independent, non-profit, global association, actively involved in the development and implementation of consultative Tanzanian National Cyber security framework.

Mr. Kanemba derives his experience from implementation of ICT projects in the National Social Security Fund (NSSF), extensive trainings on Internet security and Cyber Laws (Singapore), IT Security Coordination and Computer Forensics (Germany) and multiple international conferences on the Information Security.

Mr. Kanemba holds Master of Science (M.Sc.) in Computer Security and Audit from Greenwich University (UK), Postgraduate Diploma in Information Security and Assurance and Postgraduate Diploma in Scientific Computing.

Mr. Kanemba will look at the cyber security from a perspective of a non-profit organisation. He will deliver a speech on "The role of ISACA in promoting Cyber Defence in Tanzania".

Trainer profiles

Sebastian Marondo,
Chief executive officer NRD EA, Information security expert.

Mr. Marondo is an information security expert and auditor with more than 6 years experience and achievement across the whole spectrum of technical aspects of Information Technology, Information Security, Business Continuity, Networking, Systems Integration and physical security in Information and Communications Technology (ICT).

In the past 5 years he has been in various industries include Banks (NMB, Akiba Commercial Bank), private sector (software development and consultancy), and Government (IFM, TRA and National Audit office). Also Sebastian worked on various projects include information system audit for United Nation organizations, UNFPA, UNON, UNEP, ICTR and UN-Habitat. ERP implementation for Zanzibar Telecommunication (ZANTEL), Zambia Telecommunication (ZAMTEL), Fraud investigation and Risk Assessment to various clients.

Sebastian Marondo holds MBA in International Business, Certified Information System Auditor (CISA), Certified Information Security Manager (CISM) both from ISACA.

Augustas Gutautas
experienced IT security and infrastructure professional, NRD

Mr. Gutautas is an experienced IT security and infrastructure professional with more than 10 years of experience in international projects including but not limited to Lithuania, Latvia, Norway, Denmark, United Kingdom, Belarus, France, Thailand, Tanzania and Burundi. Augustas has educational background of Complexity Management in area of ICT. His work experience ranges from high availability solutions, architecture design, disaster recovery solutions as well as design and implementation of critical IT infrastructures and security controls, cyber security solutions and security assessments, penetrations testing in banks, financial institutions, telecoms and government institutions.

Mr. Augustas Gutautas has been leading international projects and has been actively involved in international activities of the company acting as a team leader, consultant and project manager through various stages of engagements starting from proposal preparation to project delivery and support.

Augustas Gutautas has BSc Computing and Systems Practice from UK, has been lecturing in Bujumbura ISGI University, Burundi.

Trainer profiles

Dr. Vilius Benetis,
CISA, CRISC
Senior Cyber Security
Consultant, NRD

Dr. Vilius Benetis, CISA, CRISC is a senior consultant, focusing on cyber security, IT infrastructure audit and IT infrastructure architecture optimisation. He has been leading several projects on optimisation of IT infrastructure and data centres towards effectiveness, security (ISO 27001 based, as well as general security baselining) and Service management (ITIL).

Vilius Benetis specialises in Public Sector Information Security Consulting, IT Infrastructure Architecture, IT Audit Security Audits, Compliance Audits, Risk Assessment, IT security automatization (IAM, log and SIEM, encryption, security in depth, server security baselining, vulnerability management, patch and remediation, end point control, privileged user management, network segregation), Telecommunications Engineering and Compliance Management.

Dr. Benetis is one of the authors of the newly released ISACA publication “Transforming Cybersecurity: Using COBIT® 5“ and a subject matter expert reviewer of ISACA’s "Responding to targeted Cyber attacks".

Vilius has graduated from Kaunas Technical University, as well as from Danish Technical University in BSc in Computer Science, MSc and PhD in Teletraffic Engineering. Vilius has been on fellowship in Tsinghua University Hitachi Labs. He has as well extensive experience in corporate environment (Motorola, CA technologies, Dell), where he was supporting IT services and management project sales and implementations.

You are kindly invited to choose one of the tracks when registering:

Track 1: Critical Security Controls training

The 20 critical security controls are set of controls recommended and complied by consortium of more than 100 contributors from government agencies, commercial forensic experts and penetration testers. These controls are minimum recommendations for organizations to implement in order to block or mitigate known attacks. They are the baseline of high-priority information security measures and controls that can be applied across an organization in order to improve its cyber defence. The controls are designed so that primarily automated means can be used to implement, enforce and monitor them.

The security controls give no-nonsense, actionable recommendations for cyber security, written in a language that is easily understood by IT personnel. The goal of 20 critical security controls is to leverage cyber offense to inform cyber defence, focusing on high payoff areas, ensure that security investments are focused to counter highest threats, maximize use of automation to enforce security controls, thereby negating human errors, and use consensus process to collect best ideas.

It focuses on various technical measures and activities, with the primary goal of helping organizations to prioritise their efforts to defend against the current most common and the most damaging computer and network attacks. The 20 controls and supporting advice are dynamic in order that they recognize changing technology and methods of attack.

The strength of the Critical Controls is that they reflect the combined knowledge of actual attacks and effective defences of experts in the many organizations that have exclusive and deep knowledge about the current threats. These experts come from multiple agencies of the U.S. Department of Defense, Nuclear Laboratories of the U.S. Department of Energy, the U.S. Computer Emergency Readiness Team of the U.S. Department of Homeland Security, the United Kingdom's Centre for the Protection of Critical Infrastructure, the FBI and other law enforcement agencies, the Australian Defense Signals Directorate and government and civilian penetration testers and incident handlers.

Top experts from all these organizations have pooled their extensive first-hand knowledge of actual cyber attacks and developed a consensus list of the best defensive techniques to stop them. This has ensured that the Critical Controls are the most effective and specific set of technical measures available to detect, prevent, and mitigate damage from the most common and damaging of those attacks.

Objective of the training is to provide in depth understanding on all 20 critical security controls.

→ Introduction to 20 critical security controls;

→ Main concepts:

- Critical Control 1: Inventory of Authorized and Unauthorized Devices
- Critical Control 2: Inventory of Authorized and Unauthorized Software
- Critical Control 3: Secure Configurations for Hardware and Software on Mobile Devices, Laptops, Workstations, and Servers

- Critical Control 4: Continuous Vulnerability Assessment and Remediation
- Critical Control 5: Malware Defenses
- Critical Control 6: Application Software Security
- Critical Control 7: Wireless Device Control
- Critical Control 8: Data Recovery Capability
- Critical Control 9: Security Skills Assessment and Appropriate Training to Fill Gaps
- Critical Control 10: Secure Configurations for Network Devices such as Firewalls, Routers, and Switches
- Critical Control 11: Limitation and Control of Network Ports, Protocols, and Services
- Critical Control 12: Controlled Use of Administrative Privileges
- Critical Control 13: Boundary Defense
- Critical Control 14: Maintenance, Monitoring, and Analysis of Audit Logs
- Critical Control 15: Controlled Access Based on the Need to Know
- Critical Control 16: Account Monitoring and Control
- Critical Control 17: Data Loss Prevention
- Critical Control 18: Incident Response and Management
- Critical Control 19: Secure Network Engineering
- Critical Control 20: Penetration Tests and Red Team Exercises

→ Implementation and auditing of 20 critical controls.

Track 2: Penetration Testing training

As the world is advancing in use of cyber space with multi-tier network architectures, high speed connection, Web services, custom applications, and heterogeneous server platform environments, keeping data and information assets secure is more difficult than ever. This combination has formed complex systems that criminal organizations have organized their hacking efforts to break in; it is no longer just "script kiddies" trying to break into your network, but advanced technology is being used which includes supercomputing and distributed intelligent systems.

Although there are many ways to secure systems and applications, the only way to truly know how secure you are is to test yourself. By performing penetration tests against your environment, you can actually replicate the types of actions that a malicious attacker would take, giving you a more accurate representation of your security posture at any given time. Although most penetration testing methods have traditionally been somewhat ad-hoc, that has changed in the last several years. Robust, repeatable testing methodologies now exist, and high quality commercial tools can be implemented to ensure that both testing parameters and results are high-quality and trustworthy. Penetration testing provides an excellent view of the actual security state of an environment as well as organization's security state.

With penetration testing one can evaluate computer and network security by simulating an attack on a computer system or network from external and internal threats. This may include: attempt to gain access to resources without knowledge of usernames, passwords and other normal means of access. If the focus is on computer resources, then examples of a successful penetration would be obtaining or subverting confidential documents, pricelists, databases and other protected information. This process involves an active analysis of the system for any potential vulnerabilities that could result from poor or improper system configuration, both known and unknown hardware or software flaws, and operational weaknesses in the process or technical countermeasures. The main thing that separates a penetration tester from an attacker is permission. The penetration tester will have permission from the owner of the computing resources that are being tested and will be responsible to provide a report.

The ultimate goal of penetration testing is to seek improvement of the system and resources which are being tested.

Objective of the training is to provide in depth understanding on the following concepts:

- Penetration Testing;
- Security Assessments;
- Automated Testing;
- Manual Testing;
- Enumerating Devices;
- Denial of Service Emulation;
- Web Application testing;
- Tools for conducting tests.

To achieve these objectives, the following topics are to be covered:

- Penetration Testing Concepts;
- Types of Pen testing;
- Pen testing techniques;
- Pen testing phases;
- Penetration Testing Tools.

Technology demonstrations

When your organisation is designing a new information security infrastructure or when there is a need to update the old infrastructure with specific functions, renew or purchase software or hardware, you face a difficult challenge of having to choose the technology that best suits your needs.

In order to make this choice a more informed one, during the CDEA'13 we are going to introduce you to a set of proven, effective, state-of-art technologies and tools. After the demonstrations you will understand the purpose, benefits and operational features of these industry-standard and leading technology solutions.

Security information event management (SIEM) demo

Failure to effectively manage the massive amount of data generated in the event logs that network, security and other devices collect, perform the necessary analysis and respond to detected anomalous user behaviours and suspicious events can have a serious impact on the information security of the organisation.

In this demonstration, you will see how SIEM technology allows organisations to automate the process of effectively collecting, correlating and analysing events logged within your infrastructure and produced in multiple locations to spot trends and see patterns that are out of ordinary. You will see how this allows proactively identifying threats that could lead to a data breach and reducing the time from incident detection to containment and remediation. In addition, SIEM is one of the mandatory tools to ensure management of IT security of organisation, integrating under one umbrella all other activities, including incident response, security monitoring, reporting, analysis, and compliance.

Advanced Persistent Threat (APT) Protection Demo

The challenge in defending against advanced persistent threats comes from their complex and sophisticated nature (low-volume, professional, highly customized, well-funded, combining multiple methodologies) and their ability to threaten even the most protected information systems, especially if they rely on traditional, signature-based security techniques such as content-scanning, sender verification, reputation and creation of safe/unsafe lists.

During this demonstration you will see how a new-generation protection systems fill in the gaps left by traditional security techniques (firewalls, IPS, AV, and Web gateways) and deal with zero-day and targeted APT attacks.

Kill abuse of unstructured data Demo

A large share of the critical business data (e.g. finance, HR and marketing documents, spreadsheets, presentations, media files) is unstructured or semi-structured, i.e. it is not in a database or a part of an application data store. Protecting this data is particularly challenging because the amount of such data is too vast to manually identify which of it is sensitive and exposed to risk, who owns it, who should and who should not be able to access it, who uses it and who abuses it and manage the access rights accordingly. This means that far too often vulnerable information is exposed to risk and abuse.

In this demonstration you will learn about the newest technology solutions for managing unstructured data, identifying sensitive information and stale data, aligning critical business assets with their proper owners and allowing access intelligently to reduce risks, abuse and comply with the strictest regulatory requirements.

Technology demonstrations

Device Control and patch and remediation Demo

Outdated endpoint software patch management creates an easy path for cyber criminals. By eliminating vulnerabilities in third party applications and heterogeneous operating systems, IT risk can be effectively reduced, while endpoint operations can be improved. However, it is time consuming, costly and difficult to manually keep up and apply security or software changes across the entire organization.

Therefore, during this patch and remediation demonstration you will be introduced to a centralised management hub that automates discovery, assessment and remediation for heterogeneous endpoint environments and rapidly and accurately alerts your IT personnel when they need to take proactive actions on key issues.

This allows standardizing endpoint configurations and automating patch management to keep networks and devices up to date, secure and efficient at all times across the entire endpoint environment. In addition, this solution reduces complexity in your IT environment, reduces maintenance resources and IT operational friction.

Risk and compliance management Demo

Organisations often lack the ability to identify, measure, manage, monitor, review and report on IT risks and compliance gaps. They address these threats insufficiently because of inadequate efforts to handle multiple overlapping compliancy requirements and best-practice frameworks in each department separately and use inefficient, spreadsheet-based compliance reporting methods. In addition, they tend to overspend on manual audits and disparate data gathering. However, failure to monitor organisation's security state, track IT security metrics and map this information with business risk might cause business disruption, loss of important data and non-compliance with both internal policies and external regulations.

During this session you will witness how centralised, streamlined, automated technology for compliance and IT risk management helps to harmonise your controls, prioritise, assign and track your remediation efforts and responsibility while also saving time and reducing compliance costs. You will see how it allows establishing organization-wide consistency, optimising your IT resources and aligning them with your business strategy, minimising regulatory problems and streamlining audit workflows.

Forensics Demo

Even if your organisation is effectively protecting all of the weakest parts and all of the main resources, it is still vulnerable because there is no way to know the time, tools, direction and goals of a possible cyber-attack. Therefore, it is important that in case of fraud, intellectual property theft, industrial espionage, network compromises, employee misuse or malware you have the right knowledge and tools to properly handle a forensics investigation.

During this forensics demonstration you will see how a professional forensics tool allows handling of massive data sets and utilization of a distributed workforce in order to quickly and effectively extract and analyse relevant evidence and get a full picture of what happened and who was involved while also preserving data integrity. For non-forensics experts, this demonstration will help to understand the basics of obtaining complete and accurate information for security forensic investigations and compliance reports.

Technology demonstrations

Universal Threat Management (UTM) Demo

Even though organisations increasingly face advanced cyber security threats, it is important to remember that the Internet is still full of less sophisticated threats of all shapes, sizes, and severities that could also cause you some serious issues ranging from data leakage to interrupted business operations. However, managing many separate single-purpose security devices and software is difficult, ineffective and prone to errors.

Universal treat management devices allow simplifying security management, reducing costs and protecting your organisation from a variety of threats. During this technology demonstration, you will be introduced to a multi-service platform that delivers a total security package that protects against attacks, viruses, Trojans, spyware, malware, spam, phishing and other malicious threats.

Vulnerability Management Demo

Most of the cyber attacks exploit known security flaws for which remediation are available because organisations fail to manage and patch these vulnerabilities effectively.

Vulnerability Management software, that is going to be demonstrated, helps to maintain control over your network security by automatically identifying security vulnerabilities with external and internal scans, prioritising them according to the severity levels and impact on business, providing extensive, centralised reports (for both executive level and technical personnel) and verified remedies.

During this session you will see how this technology solution helps you to fix the vulnerabilities continuously, proactively and efficiently and in this way protect your business information while also significantly reducing your security managers' time researching, scanning and fixing network exposures.

Privileged User supervision Demo

The human factor is a common cause of security breaches. Privileged users' accounts are especially vulnerable because these users are able to directly access and manipulate sensitive information. Therefore, mismanagement of privileged identities puts your company at tremendous risk. However, at the same time, privileged accounts are especially difficult to manage and trace.

During this demonstration, you will see how privileged user supervision software addresses these problems. You will be able to observe how introduction of an independent auditor layer helps to monitor the work of your privileged users, controls their access and establish patterns of each user activity. You will learn about the alerts that you get when anomalous behaviour occurs, certain applications/systems are accessed, or unusual volumes of data are sent or received and how that allows you to address insider threats, improve control, protect access to enterprise resources and reduce risk.

Venue and accomodation

The event will take place at the **Nashera Hotel**, a four-star hotel, located just over 3km from the centre of Morogoro and defined by the panoramic views of the Uluguru Moutain.

Room reservations for the conference participants are offered at corporate rates.

	B&B	Half Board
Deluxe	$115	$135
Twin	$145	$165
Executive suit	$250	$270

After the trainings you will have an opportunity to continue discussions with other participants in a more relaxed and informal environment or enjoy one of many other attractions that the Nashera hotel and Morogoro have to offer.

On site attractions:

→ Volleyball court
→ Pool
→ Zumba - lessons available (5,000 tsh/pp)
→ Souvenir shop
→ Outdoor BBQ area
→ Morning/evening walks up road at foot of mountain
→ Hike/Trek from hotel through beautiful Uluguru Mountains (4hrs to peak)
→ Travel Counter for Safari Arrangements
→ Massage Service

Gala Dinner

The conference programme also includes a Gala Dinner on the 29th August. This event will provide an opportunity for networking with your trainers and around 100 other information systems auditors, IT risk professionals and IT enthusiasts from the most successful, innovative and influential companies with East African presence.

Nashera Hotel

Boma Road, LITI Area, P.O. Box 237
Morogoro, Tanzania
Phone: +255 716 678233
Email: info@nasherahotels.com

Off site attractions:

→ Morogoro Golf Club - a 9 Hole Golf Course facility within 5 minutes of Nashera (no driving range, vintage sand greens, approx. $10 for 9 holes, private rental sets may be available upon request)
→ Masai Market visit (Friday's 9am-4pm)
→ Local shops
→ Nearby Mikumi
→ Sustainable Tourism Opportunities through Chilunga Cultural Tourism Program (http://www.chilunga.or.tz/)
    → Where one can visit old German settlements
    → Visit Traditional Healers
    → Can see what the local nature offers such as waterfalls and bird watching.
    → A number of restaurants serving a range of local and international cuisine can also be found within 5 min. drive of the property.

Registration and tickets

You are kindly invited to register for the conference by sending an email to registration@nrd.no. Please write your name, organisation, title and which training track (Track 1/Track2) you are choosing.

Deadline for booking: 15th August 2013.
On-site registration will not be available. Please book in advance.

Included in your ticket:

⇒ Three-days conference pass;
⇒ Training materials;
⇒ Tea and lunch on all days;
⇒ Gala Dinner;
⇒ Attendee bag.

Registration fees can be paid by bank transfer to the following account:

Account Name: Norway Registers Development East Africa limited
Account number: 10100686207
Swift code: AKCOTZTZ
Akiba commercial Bank. Bank code: 12
Branch code: 0001
Do not forget to mention your **full name, organization and CDEA 2013** on the bank transfer slip. All bank fees must be paid by the participant.

Prices are indicated in the table below:

Registration fee	Till the 27th of July	After the 27th of July
ISACA members	US$350/Tsh 550,000	US$400/Tsh 650,000
Other	US$450/Tsh 750,000	US$500/Tsh 830,000

Important! If you register as an Early Bird, the fee should reach the account no later than 27th May, 2013.

Confirmation of Registration

The registration will be confirmed by email after we receive the payment. Those who do not receive a confirmation notice before the conference are strongly recommended to contact us at registration@nrd.no.

Cancelation and Refund Policy

⇒ Before 27th July, 2013: 50 % will be refunded from the payment.
⇒ After 27th July, 2013: No payment will be refunded.

Refunds will be issued after the conference. Bank charges will be deducted from the refund. For refunds please state your full bank account.

About Norway Registers Development in East Africa

NRD has been actively engaged in cyber security initiatives in the East African region for a while now: multiple seminars on cyber security, MoU with ISACA Tanzania Chapter on cooperation in the development and implementation of consultative Tanzanian National Cyber security framework, as well as recently signed two-year Cooperation and Services Agreement with local agent – SimbaNET. The main objective of these initiatives is to create a secure digital environment for East African states, governments, corporations and citizens.

In March 2013, in order to be closer to its clients, NRD AS has decided to invest in one of its partners. Newly acquired Norway Registers Development East Africa Ltd. (NRD EA) provides on-site delivery of the NRD services and is responsible for cyber-defence strategy design and implementation services for Government and corporate institutions. NRD EA supports Tanzanian companies in the delivery of information security technologies as a value added distributor. At the same time the new entity is actively involved in the improvement of the Business Climate in the East African Community.

Furthermore, with this acquisition, NRD is now fully equipped to assist other organisations investing in East Africa in the creation, development, maintenance and security of their information technology infrastructure.

Norway Registers Development AS has during the last 18 years been specializing in helping governments and institutions in all continents to build vital economy facilitating infrastructure together implementing necessary legal and organizational changes, particularly in the area of business registers.

The NRD services and experiences cover consultancy, legal research and drafting, institutional capabilities building and training, system designing and implementation as well as operation services as integrated solutions for effective operation of the required services. The NRD AS fields of experience cover the complete range of activities from the raising of awareness and political commitment to project designing and preparations, implementation support and execution, operation and maintenance.

Having been particularly specialized in complex registration reforms, NRD has accumulated a wide experience in designing, implementation and management of register projects. This experience gave NRD perfect ground to expand services to other fields where complex data management requirements come together with a necessity for legal and organizational reforms.

About ISACA Tanzania Chapter

ISACA is an independent, non-profit, global association, engaging in the development, adoption and use of globally accepted, industry-leading knowledge and practices for information systems. ISACA provides practical guidance, benchmarks and other effective tools for all enterprises that use information systems. Through its comprehensive guidance and services, ISACA defines the roles of information systems governance, security, audit and assurance professionals worldwide.