

Abu Dhabi Government Entities (ADGEs)

Information Security Planning, Risk Assessment and Risk Treatment Services

Presenter:

Nevenko Bartolinčić, Security Department Leader

Mohammad ShAms, Director, Middle East Operations

noitulo2

Our typical understanding of the ADGEs project

Our methodology

Project Management

Delivery team

Company introduction

Typical Project scope and environment

Coverage of first 3 phases of ADSIC's Information Security Programme

Objectives:

- identification, classification and categorization of information systems and services
- identification and valorization of vulnerabilities and threats, calculation of risk
- development of risk treatment plan

IT Services included

- overlapping supportive systems (facilities, ICT, HR, utilities, intangibles)

Preparation for upcoming DRP project

Typical Project roadmap



Risk management (continued)

Out of scope...

Information services identification, categorization and classification

Identification of services' supporting systems, their categorization and classification

Estimation: approx. man/days

Determination of services and systems boundary and scope

Identification of legal requirements

Creation of information security plans (ISPs) draft

- ISO/IEC 27005:2008 - Information security risk management
 - member of ISO 27000 information security standard series
 - developed from BS 7799-3:2006
 - utilized in RECRO-NET approach
- other:
 - NIST SP800-30 - Risk management guide for IT systems
 - Octave (Operationally Critical Threat, Asset, and Vulnerability Evaluation) information security risk evaluation
 - CRAMM (Central Computing and Telecommunications Agency Risk Analysis and Management Method)
 - and many more...

Risk management

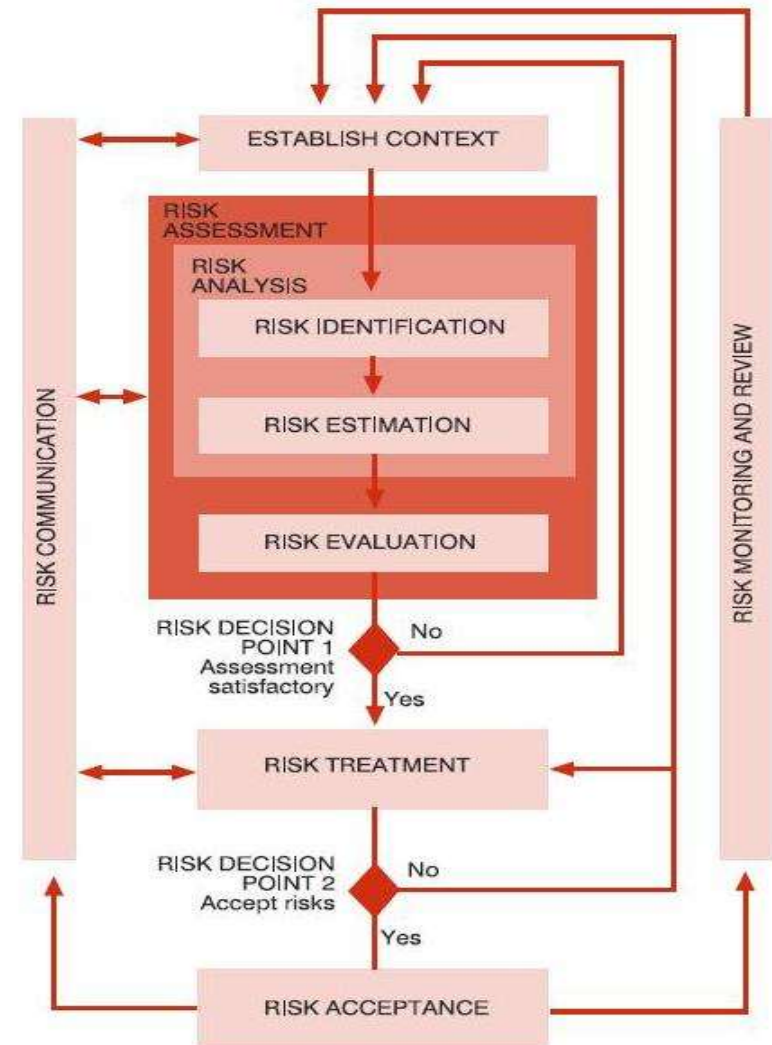
- coordinated activities to direct and control an organization with regard to risk
- includes risk assessment, risk treatment, risk acceptance, risk communication, risk monitoring and risk review

Risk assessment – overall process of:

- risk analysis – qualitative (subjective)
- risk evaluation – quantitative (calculation)

Risk treatment

- selection of mitigation strategy (cost-benefit)
- selection of security controls
- identify responsibility and deadlines



Basic criteria:

- unambiguity
- objectivity
- reliability
- repeatability
- → comparable and reproducible results

Suitable to organizational needs (size, business, level of effort...)

Coverage of all aspects of the complete information systems scope

Clear definition of roles and responsibilities involved in the process

Assessment techniques

- Documentation Review
- Interviews/Stakeholder Workshops
- Configuration Review
- Vulnerability assessment

Creation of information assets inventory

- definition of ownership
- impact classification (criteria of confidentiality, integrity, availability)

Recognition and rating of vulnerabilities (weaknesses)

- → using comprehensive (non-exhaustive) lists

Identification and rating of threats (potential hazards)

- → using comprehensive (non-exhaustive) lists

Estimation of probability (likelihood of occurrence)

Evaluation of risk

Risk treatment

Determination of safeguards

Analysis of existing mitigation measures

Considering risk management options:

- reducing the risk (likelihood and/or impact)
- accepting the risk
- transferring the risk (to a third party)
- avoiding the risk

Deciding on optimal solution

Evaluation of risk after solution implementation

Accepting the residual risk

Ongoing monitoring of effectiveness

- re-assessments

Training arrangement based on:

- ISO/IEC 27001/27002 standards, or
- ADSIC Information Security Programme

Duration

- 5 working days (recommended, depending on number of attendees and coverage depth)

Language

- provided in English language
- Arabic translator ensured

Deliverables



Entity services inventory workbooks



System security categorisation workbooks



Security scoping documents



Services/systems' risk assessment reports



Services/systems' risk treatment plans



Services' information security plans



Training materials



Executive summary

- senior management support and involvement
- establishment of focal points (resources: time & personnel, i.e. funds)
- usage of procedures & standardized tools
- involvement of business & technical experts
- provision of adequate training & support
- accountability of responsible participants
- determination of individual assessments scope
- documented & maintained results

- standardization establishes a consistent approach
 - provided direction for information security initiatives
 - documentation for audit provided
 - assurance of regulatory compliance
 - increased IT security awareness
- optimum solution (in terms of required expertise, time and funds)

Our Certified Resources

Consultant Name	Title	Years of experience	Client Handled	Education & Certification
Nevenko Bartolinčić	Security Dpt. Leader	20	Renault, OTP bank, T-Mobile Croatian Ministry of Environmental Protection, Physical Planning and Construction	CISSP, CISA ISMSLAC CCNP, CCNA, CCSI, CCAI ITILv3
Ivan Kleković	Information Security Consultant	7	DB Schenker , Jadransko Insurance Co. Croatian Ministry of Environmental Protection, Physical Planning and Construction	CISA Security+ ISMSLAC ITILv3
Davor Šerfez	Computer Security Expert	14	OTP bank, Bauhaus, T-Com T-Mobile	CISSP LPI1
Bojan Kornijenko	Computer Security Expert	8	European Union Police Mission in BIH Leasing financial institution BIH Largest BIH Pharmaceutical company Austrian Insurance Company BIH	CCIE, CCNA, CFWS, CCSI, CCSP MCSA GSEC, GCIA, GCIH
Anup Narayanan	Information security professional	10	Ericsson, Vodafone India, Bharti Airtel, Lakshmi Machine Works, J Kalachand and Co., Accel Transmatic, Cordiant Technologies Pvt. Ltd., DocuStream India Technologies Ltd.	CISA CISSP ISO 27001 Lead Implementer
Praveen Reddy	Information Security consultant	10	GLOPORE IM Services Pvt. Ltd., Emirates Airlines, Acs-India Pvt Ltd, Aptuit (Infopro Solutions Pvt Ltd)...	CISSP, CISA ITIL V3 Foundation CCNA, MCSE, CCA

- **RECRO Group is the leading Technology Services provider in EMEA with:**



- 2008. Revenue growth 23% to \$372m (Technology Services and Distributions)
- 10+ years of Excellence in Services and Solutions Delivery
- ISO9001 certification, ISO27001 in-progress
- HQ in Zagreb, Croatia
- Regional offices in Sarajevo and Dubai
- Channel Partners in all over EMEA
- Leader in Technology distributions in SEE
- 300+ employees in RECRO Group

Croatia



- +300 employees
- leading ICT group in Croatia
- 1200 customers and partners



BiH



UAE

- RECRO-NET range of delivery services and its strength in process and quality excellence ensuring the Service Quality Assurance to our customers in EMEA;
- The Infrastructure Services business and Security Services uses the BS, ISO standard as the base process framework for compliance and all processes are governed by ITIL;
- Successfully building the large corporate ICT infrastructure that helps the business quickly respond to emerging threats and collaborate with confidence.



RECRO-NET Portfolio & Services

ICT Infrastructure Lifecycle Services

- Data Center Solutions
- Networking & NMS
(GSR, 76xx, 65xx, MARS, Compuware, NetScout)
- Unified Communications
- NGN Solutions
(IP/MPLS, Metro Ethernet, QoS)

Business Solutions

- Enterprise Portal Solution
- CRM/ERP Solutions
- Business Continuity Mgmt. BS25999
- Professional Services
(ICT audit, consulting, PM, SM)

Security Solutions

- IPS/IDS, FW, mail & web security,
- PKI & smartcard solutions
- DDOS detection and mitigation
- ICT Security Auditing
ISMS ISO 27001

Multimedia Solutions

- Cisco DMS
(Integration with RFID)
- Video Conferencing
(Tandberg/Cisco)
- Cisco IP video surveillance (ATP)

Proven and Guaranteed ICT implementation & Local and regional Support

Optimum mix of onshore, near-shore and offshore resource

End to End Business Solution and Services

Manage Risks, costs \$\$\$ to enable Business

Emerging Technologies Implementation and Services

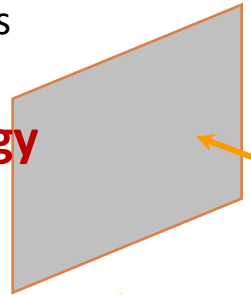
RECRO-NET Expertise

- ☐ Data Center modernization
- ☐ Carrier Management Services
- ☐ Technology Advisory and Audit
- ☐ Identity Management Services
- ☐ Unified Communications
- ☐ Project Management

IT Security and Compliance

- ☐ IT GRC Security
- ☐ ISO 17799/ 27001 gap Analysis
- ☐ Business Continuity and Disaster recovery
- ☐ Nextgen Digital Security (PKI)

Infrastructure strategy & Implementation



ERP Implementation

- ☐ Application development & Management
- ☐ CRM, SCM/SRM
- ☐ Enterprise portal
- ☐ ERP Integrations

NGN

- ☐ IP/MPLS Core & ROADM DWDM
- ☐ IP Backbone Architecture
- ☐ MPLS Traffic Engineering
- ☐ Edge Transport Network (IP/MPLS)
- ☐ L2 Security

RFID Middleware

- ☐ RFID Integration with DMS
- ☐ Asset Tracking Management

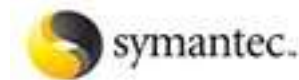
Network Mgmt.

- ☐ Networking Application Services
- ☐ Network Management
- ☐ Network Transformation Services
- ☐ Network Forensic Services

Certified engineers (CCIE/CISA/CISSP/CCNP/ITILv3)



- **Cisco Systems, Inc.** – Gold Certified Partner
- **Arbor Networks** – Certified Partner
- **TriGeo NS, Inc.** – Certified Partner
- **Netscout Systems, Inc.** – Certified Partner
- **IBM** – Certified Partner (IIS, Tivoli)
- **OpenTrust** – Certified Implementation Partner
- **Gemalto** – Certified Partner
- **ObserveIT** – Certified Partner
- **Symantec** – Certified Partner





مركز أبوظبي للأنظمة الإلكترونية والمعلومات
Abu Dhabi Systems & Information Centre

- on August 4th 2010
- RECRO-NET „has been put on a shortlist of service providers to Abu Dhabi Government Entities (ADGEs)”

Formal knowledge, verified by certificates (independent and vendor specific)

Professional experience in numerous information security projects

IT-oriented company in various domains provides broad know-how (recommendations for technical controls) and partnership benefits with leading global providers

RECRO-NET Middle East FZ-LLC

Business Central Twin Towers

Office: 2702A, Dubai Internet City,

PO. Box: 503012 Dubai, UAE

Phone: +971 4 434 7599 / 04-3754306

Mobile: +971 50 6406647

Fax: +971 4 438 0198

E-mail: middle-east@recro-net.com

Web: www.recro-net.com

