CERT-SA

Saudi Arabia Computer Emergency Response Team

Suliman A. Al Samhan

Information security Specialist

CERT-SA

Ssamhan (at) cert.gov.sa

Contents

- Vision & Mission
- Operation Strategy & Implementation Plan
- Service Delivery
- The CERT-SA Portal
- Information Security Handbook
- Incident Response
- CERT-SA Infrastructure
- Security Investigation Laboratory/Forensics lab
- Security Operation Center
- Conclusion

Phone: +966 1 263 9292 - Fax: +966 1 263 9291
Email: info@cert.gov.sa Website: http://www.cert.gov.sa

Vision

"To be the trusted authoritative reference for information security in the Kingdom of Saudi Arabia."

Phone: +966 1 263 9292 - Fax: +966 1 263 9291
Email: info@cert.gov.sa Website: http://www.cert.gov.sa

Objectives

- Improve information security awareness level
- Coordinate national/international efforts towards promoting IT Security best practices and creating trust among cyber community.
- Support early discovery and containment of information security attacks and incidents.
- Become an information security reference point for the Cyber Community.
- Information security skills and capacity building.
- Promoting and supporting a trusted e-transactions environment.

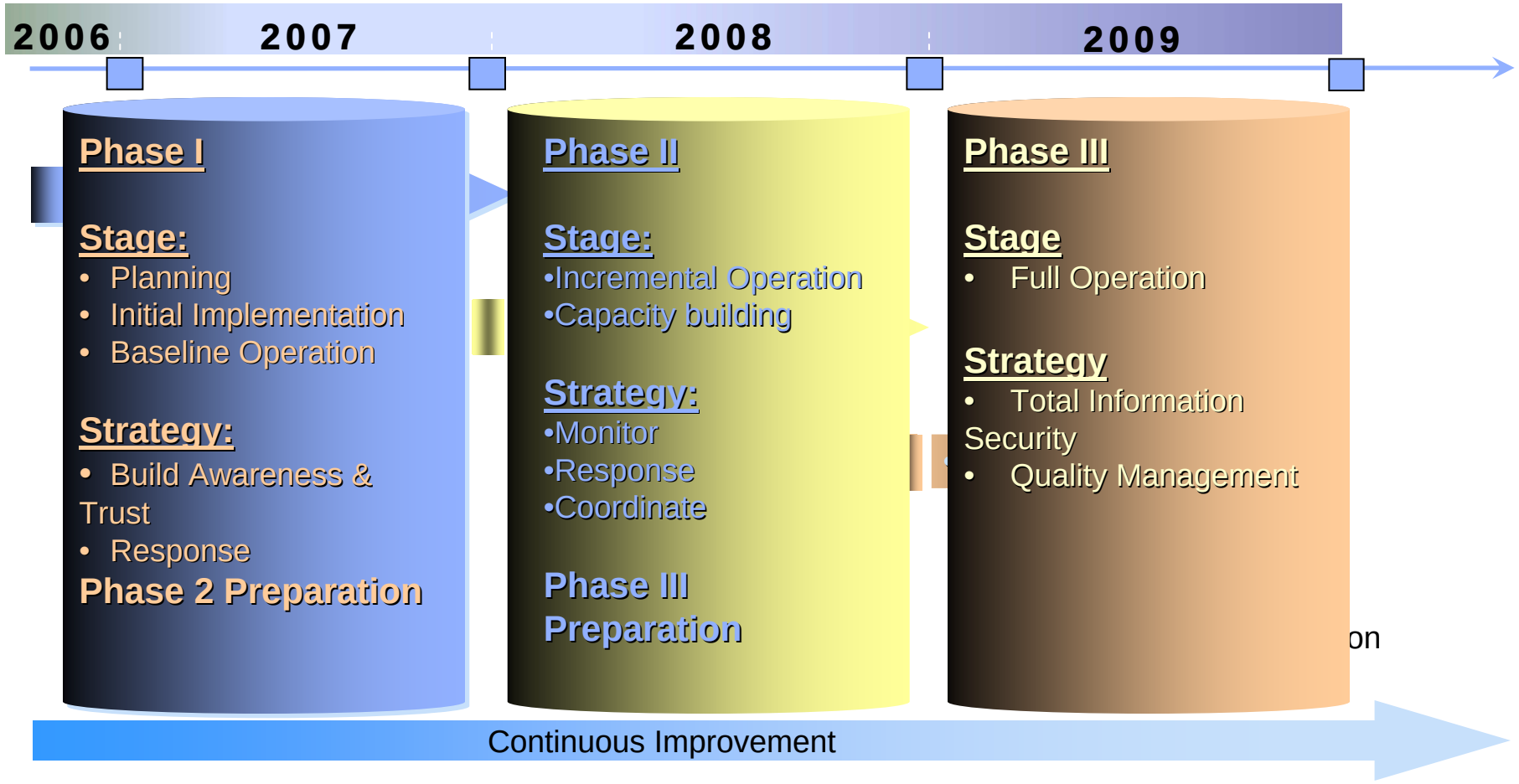
Phone: +966 1 263 9292 - Fax: +966 1 263 9291
Email: info@cert.gov.sa Website: http://www.cert.gov.sa

Operation Strategy and Implementation Plan

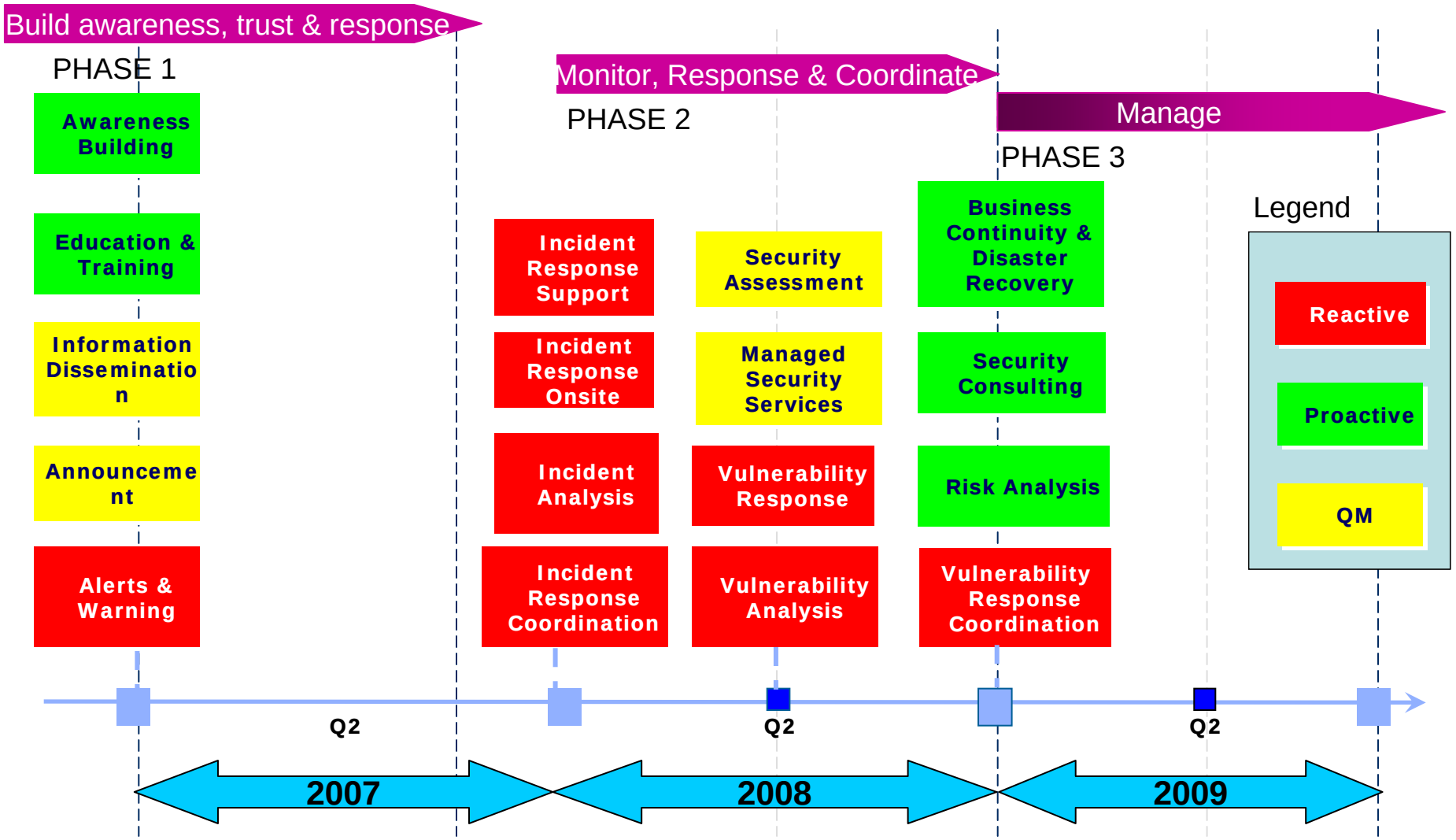
Phone: +966 1 263 9292 - Fax: +966 1 263 9291
Email: info@cert.gov.sa Website: http://www.cert.gov.sa

Operation Strategy

3 Phases of Implementation:



Service Implementation Plan



Phone: +966 1 263 9292 - Fax: +966 1 263 9291
Email: info@cert.gov.sa Website: http://www.cert.gov.sa

Service Delivery

Phone: +966 1 263 9292 - Fax: +966 1 263 9291
Email: info@cert.gov.sa Website: http://www.cert.gov.sa

CERT-SA Portal (Proactive)

http://www.cert.gov.sa

- **R1** Alerts & Warning
- **P1** Announcement
- **P3** Info. Dissemination
- **S1** Awareness Building
- **S2** Education & Training
- **R2, R3, R4** Incident Coordination

Phone: +966 1 263 9292 - Fax: +966 1 263 9291
Email: info@cert.gov.sa Website: http://www.cert.gov.sa

CERT-SA Portal

- Targeting both Arabic and English language speakers.
- Information security main reference point.

- Service delivery channel for:
  - Alerts & warning
  - Announcement
  - Information Dissemination
  - Awareness Building
  - Education & Training

Phone: +966 1 263 9292 - Fax: +966 1 263 9291
Email: info@cert.gov.sa Website: http://www.cert.gov.sa

CERT-SA Portal

R1 Alerts & Warnings

- Notify constituency regarding possible attacks, vulnerabilities, alerts, viruses, or hoax.
- Provide short-term recommendations for dealing with security problems.
- Provide guidance for protection and recovery.

Phone: +966 1 263 9292 - Fax: +966 1 263 9291
Email: info@cert.gov.sa Website: http://www.cert.gov.sa

CERT-SA Portal

P1 **Announcement**

- To notify intrusion alerts, vulnerability warnings, and security advisories
- To inform the constituency about new developments with medium to long-term impact, such as newly found vulnerabilities or intruder tools.
- To enable constituents to protect their systems before it can be exploited

Phone: +966 1 263 9292 - Fax: +966 1 263 9291
Email: info@cert.gov.sa Website: http://www.cert.gov.sa

CERT-SA Portal

P3 **Info. Dissemination**

- To disseminate various areas of information security related materials such as white paper, articles, product-based reviews etc..

Phone: +966 1 263 9292 - Fax: +966 1 263 9291
Email: info@cert.gov.sa Website: http://www.cert.gov.sa

S1 Awareness Building

- To raise awareness mainly for organization and general public.
- To increase security awareness of the constituents through developing articles, posters, newsletters, or other informational resources.
- To explain security best practices and provide advice and precautions.

Phone: +966 1 263 9292 - Fax: +966 1 263 9291
Email: info@cert.gov.sa Website: http://www.cert.gov.sa

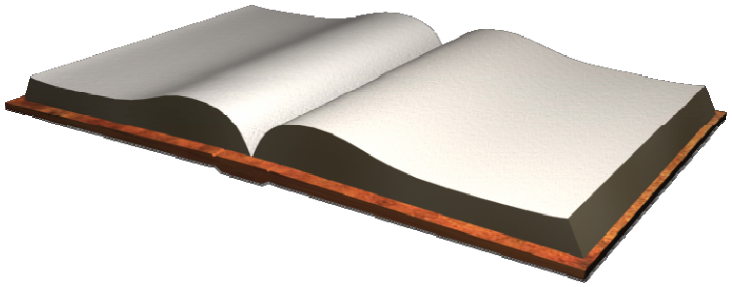
S2 Education & Training

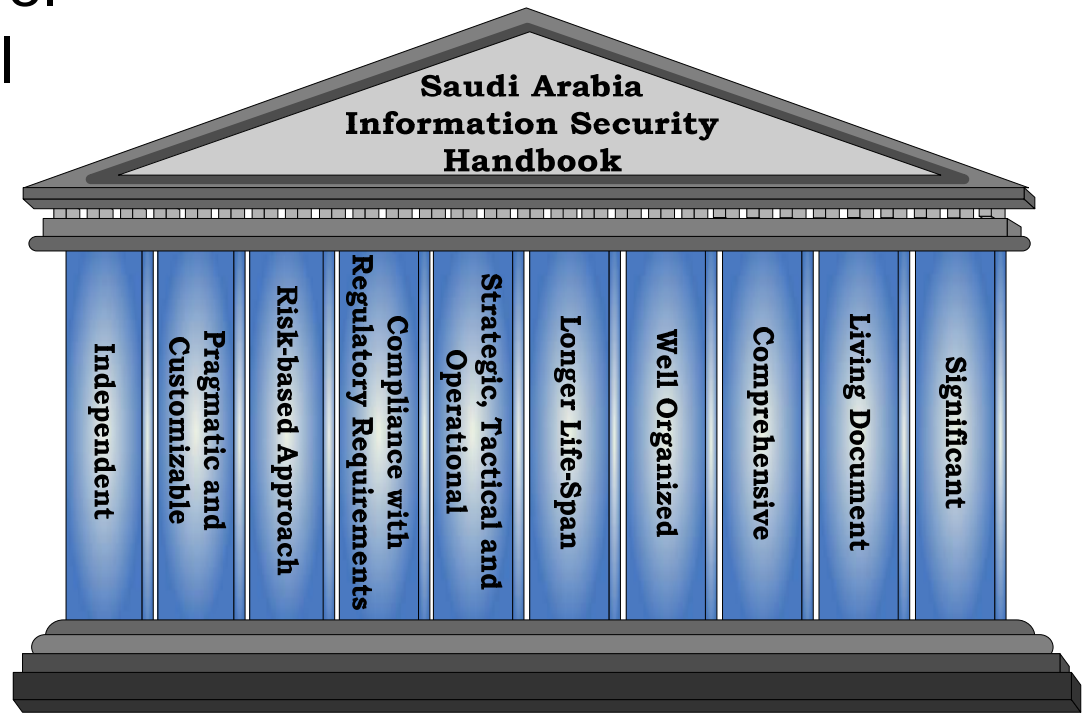
- Make available training/education material/information conducted by the CERT-SA or partners.

Phone: +966 1 263 9292 - Fax: +966 1 263 9291
Email: info@cert.gov.sa Website: http://www.cert.gov.sa

Information Security Handbook

- Is part of the Proactive Security Information Dissemination service
- Overall approach on information security:
  - Management control
  - Operational control
  - Technical control

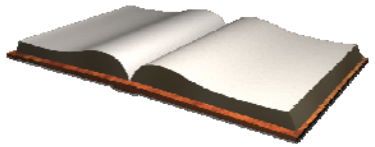




Phone: +966 1 263 9292 - Fax: +966 1 263 9291
Email: info@cert.gov.sa Website: http://www.cert.gov.sa

Information Security Handbook

- Will be available in both Arabic and English.
- In it's final reviews and to be released in early 2008.
- Will be available in both electronic and paper format.



Phone: +966 1 263 9292 - Fax: +966 1 263 9291
Email: info@cert.gov.sa Website: http://www.cert.gov.sa

Information Security handouts

- Developing security handouts in Arabic language
- Topics
  - Wireless security (Published)
  - Email security (Published)
  - Protecting home PC from internet threats (Published)
  - Privacy (under publishing)
  - SPAM (under publishing)
  - Phishing (under publishing)
  - Parental Guide towards Child safety on the internet (under publishing)

Phone: +966 1 263 9292 - Fax: +966 1 263 9291
Email: info@cert.gov.sa Website: http://www.cert.gov.sa

Incident Handling

- Incident handling consultancy services started in Q2, 2007 and gradually improving.
- Remote/onsite constituents' assistance in dealing with security incidents.
- Information on incident response best practices and how to report an incident to the CERT-SA is available on the portal and handouts.

Phone: +966 1 263 9292 - Fax: +966 1 263 9291
Email: info@cert.gov.sa Website: http://www.cert.gov.sa

Reactive Services:

- Incident Response:
  - Incident Analysis
    - Examination of all available information and supporting evidence or artifacts related to an incident or event.
    - Establishment of forensic lab
  - Incident Response Support
    - Assists and guides victim(s) of an attack in recovering from an incident via various range of delivery channels such as phone, email, fax.
  - Incident Response Onsite
    - On-site support to assist constituents in recovering from incidents.

Phone: +966 1 263 9292 - Fax: +966 1 263 9291
Email: info@cert.gov.sa Website: http://www.cert.gov.sa

CERT-SA Infrastructure

Phone: +966 1 263 9292 - Fax: +966 1 263 9291
Email: info@cert.gov.sa Website: http://www.cert.gov.sa

Security Investigation & analysis Lab

- To support CERT-SA with services, such as:
  - Feeding CERT-SA portal with threats and trends analysis.
  - Performing incident response investigation, mitigation and recovery.
  - Performing S/V A and penetration testing.

- Equipped with the necessary tools to deliver the proactive and reactive security services

Phone: +966 1 263 9292 - Fax: +966 1 263 9291
Email: info@cert.gov.sa Website: http://www.cert.gov.sa

Security Operation Center

- The need
  - National Information Security Status
  - Skills shortage.
  - Experts too busy.
  - Complexity of security solutions.
  - Attacks and vulnerabilities increased.
  - Keeping infrastructure up-to-date.
  - Need 24x7 monitoring operations.
  - Establish constituents trust.

- The Solution
  - Develop a solution to provide Security monitoring Service that is based on collecting and analyzing events from security devices (e.g. firewalls, intrusion detection/prevention, .., etc) to detect possible incidents.
  - SOC (Security Operation Center)
  - Team of experts
  - 24/7 operations
  - Service Level Agreements

Phone: +966 1 263 9292 - Fax: +966 1 263 9291
Email: info@cert.gov.sa Website: http://www.cert.gov.sa

Security Operation Center

- Under implementation to offer monitoring security services by Q1-2008 for certain constituents.
  - CERT-SA will work with the support of CITC to encourage the private sector in investing in MSSP.

- Two main functions
  - Internet Security Surveillance:
    - Monitor, detect, issue early warnings, and respond to any security threats.
  - Vulnerability Management:
    - Minimize cyber threats by detecting and identifying information system weaknesses.

Phone: +966 1 263 9292 - Fax: +966 1 263 9291
Email: info@cert.gov.sa Website: http://www.cert.gov.sa

Security Operation Center

- ISO27001:2005 Certification
  - Scope of certification
    - Certifying SOC services against ISO27001 standard
  - Objectives
    - Gaining constituents trust through applying international standards
    - Planning to expand the certification scope to include other CERT services.

Certificate of Registration

INFORMATION SECURITY MANAGEMENT SYSTEM - ISO/IEC 27001:2005

This is to certify that

Saudi Arabia Computer Emergency Response Team (CERT) / Communications and Information Technology Commission
P.O. Box 76606
Mursalat
Saudi Arabia

Holds Certificate No: IS 533720

and operates an Information Security Management System which complies with the requirements of ISO/IEC 27001:2005 for the following scope:

The Information Security Management System in relation to Communications and Information Technology Commission CERT SA Security Operation Centre Services. This is in accordance with the latest version of the Statement of Applicability

For and on behalf of BSI:

Managing Director, BSI Management Systems (EMEA)

Originally registered: 13/02/2008 Latest issue: 13/02/2008 Expiry Date: 13/04/2011

Page: 1 of 1

BSI Management Systems

Phone: +966 1 263 9292 - Fax: +966 1 263 9291
Email: info@cert.gov.sa Website: http://www.cert.gov.sa

Conclusion

Phone: +966 1 263 9292 - Fax: +966 1 263 9291
Email: info@cert.gov.sa Website: http://www.cert.gov.sa

Thank you for the time !

All centers start small and grow gradually.
International peers support is what makes CERTs unique.
Your cooperation and ideas are highly appreciated:

- Content to the CERT-SA portal
- Evaluation, additions, and improvements to the Information Security Handbook.
- Speakers to our activities.
- Sharing incidents information.
- Supporting CERT-SA activities in controlling attacks.
- Establishment of world recognition of CERT-SA.

Phone: +966 1 263 9292 - Fax: +966 1 263 9291
Email: info@cert.gov.sa Website: http://www.cert.gov.sa

Planned activities for 2007

Establishment of CERT-SA working group

Information Security Seminar

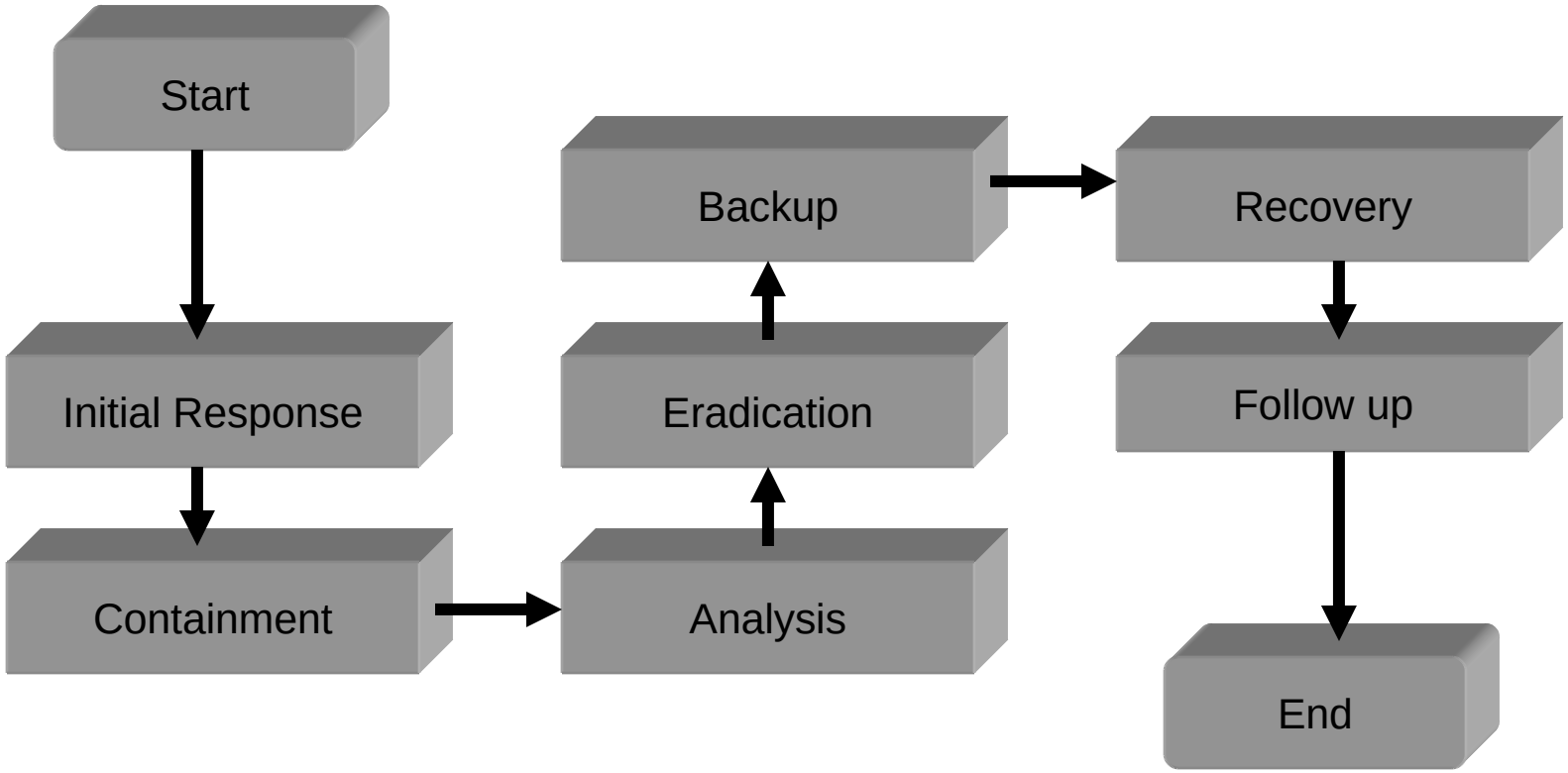
Quarterly knowledge sharing session

Month/Day of Information Security Awareness for the Kingdom

Phone: +966 1 263 9292 - Fax: +966 1 263 9291
Email: info@cert.gov.sa Website: http://www.cert.gov.sa

Incident Response

Generic incident response process



Phone: +966 1 263 9292 - Fax: +966 1 263 9291
Email: info@cert.gov.sa Website: http://www.cert.gov.sa

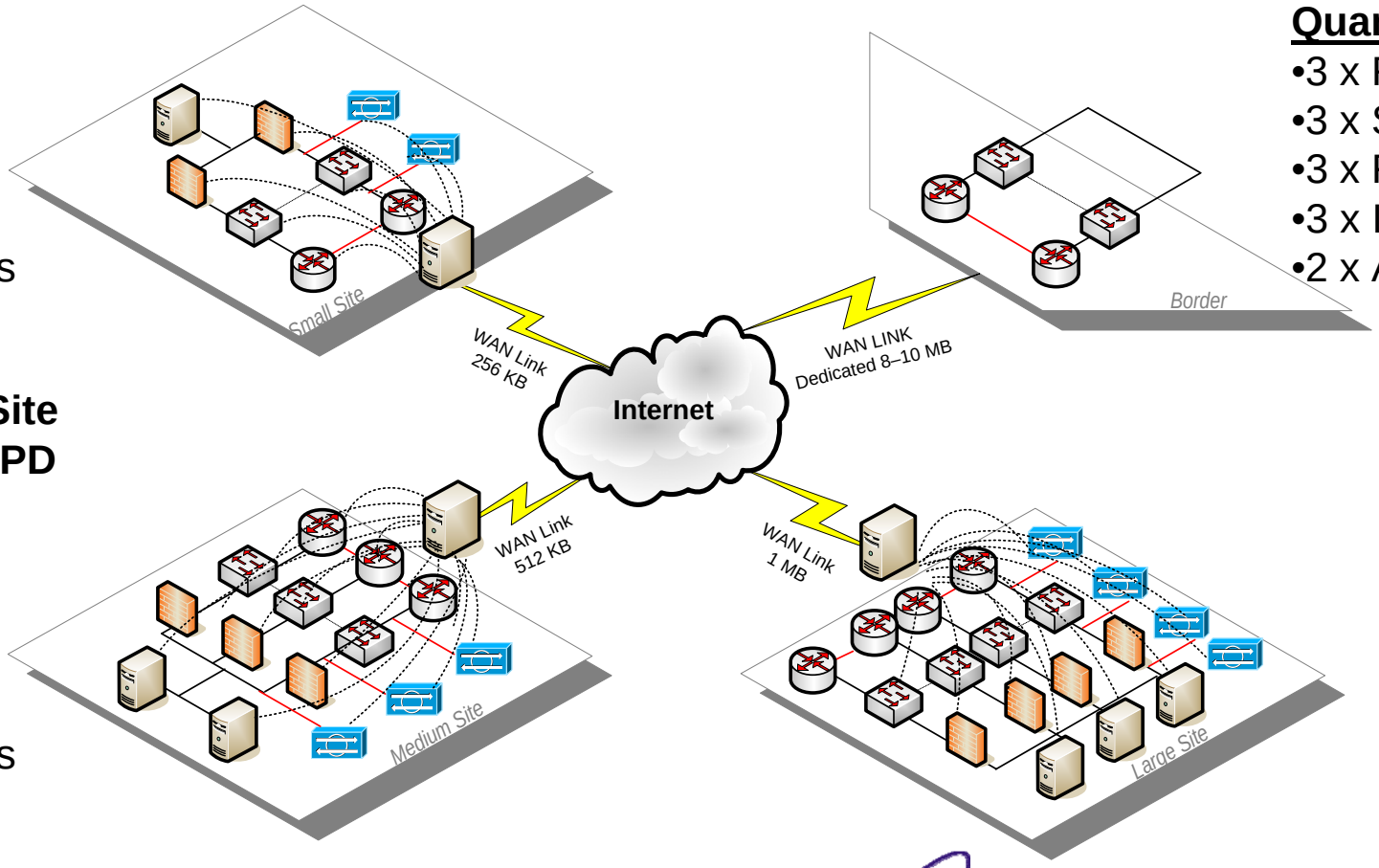
The Initial Architecture

10 X Small Site
Max 7M EPD

Quantity:
- 2 x Router
- 2 x Switch
- 2 x Firewall
- 2 x IDS
- 1 x Antivirus

3 X Large Site
Max 40M EPD

Quantity:
- 4 x Router
- 4 x Switch
- 4 x Firewall
- 4 x IDS
- 3 x Antivirus



7 X Medium Site
Max 18M EPD

Quantity:
- 3 x Router
- 3 x Switch
- 3 x Firewall
- 3 x IDS
- 2 x Antivirus

Phone: +966 1 263 9292 - Fax: +966 1 263 9291
Email: info@cert.gov.sa Website: http://www.cert.gov.sa

Information Security Handbook

Management Controls

- Information security program management
- Information security risk management
- Information security policy
- Security in application development
- Audit and assurance

Phone: +966 1 263 9292 - Fax: +966 1 263 9291
Email: info@cert.gov.sa Website: http://www.cert.gov.sa

Information Security Handbook

Operational Controls

- Human resource security
- Information security awareness, training and education
- Roles and responsibilities
- Security considerations in IT support and operations
- Physical and environmental issues
- Business continuity management
- Incident handling
- Asset management

Phone: +966 1 263 9292 - Fax: +966 1 263 9291
Email: info@cert.gov.sa Website: http://www.cert.gov.sa

Information Security Handbook

Technical Controls:

- Developing secure IT architecture
- Host-oriented security
- Network-oriented security

Phone: +966 1 263 9292 - Fax: +966 1 263 9291
Email: info@cert.gov.sa Website: http://www.cert.gov.sa

Information Security Handbook

I.S. is not all about security devices and solutions only!
I.S. is a habit, behavior, and attitude.

Overall approach on information security:

- Management control
- Operational control
- Technical control

Phone: +966 1 263 9292 - Fax: +966 1 263 9291
Email: info@cert.gov.sa Website: http://www.cert.gov.sa

Vision and Objectives

Phone: +966 1 263 9292 - Fax: +966 1 263 9291
Email: info@cert.gov.sa Website: http://www.cert.gov.sa