

Conducting an Information Security Assessment

NARUC SSIS
February 2005



Why Do This?

- Rampant attacks – they are happening
- IT opening itself to the world
- Responsibility for information
- Dependence on IT growing
- Constant vigilance required



Primary Objectives

- Assess the Security Infrastructure and Program
- Document Findings
- Recommend Actions



What to look at?

- Security program management
- Application and data security
- Installation security
- Security awareness and training
- Incident response
- Products/practices/services



Security Program Management

- Infrastructure framework – policy, compliance, risks, protection
- End-user strategies
- SDLC
- Network
- Disaster Recovery
- Compliance
- Physical security



Application/Data Security

- Overall structure – critical systems/data
- Policies and procedures
- Contingency plans
- Backup, restore & off-site procedures
- Audit trails and logs
- Change and patch control
- Access authorization and control
- Interfaces



Installation Security

- Risk analysis – threats and vulnerabilities
- Include deliberate and accidental
- Deliberate – willful damage, misuse, and theft
- Accidental – acts of nature, human errors, malfunctions
- Physical security



Security Awareness/Training

- All employees – awareness training
- IT Staff – training and/or development program for all staff, extent depends upon responsibilities



Incident Response

- Identify response team
- Define duties and responsibilities
- Incident handling guidelines
- Response tools and services



Evaluations

- Practices
- Technologies
- Services



Deliverables

- Assessment work plan
- Current status report
- Policies, procedures and standards report
- Recommended security strategies for applications/data, end-users, network, staff, installation, incidents
- Disaster recovery report
- Overall assessment summary and recommendations

