11.2 NIST Standards

The U.S. National Institute of Standards and Technology establishes standards for a wide range of things. Some of the standards that are most important towards network security are discussed within this section.

11.2.1 NIST SP 800-14

Special Publication 800-14, Generally Accepted Principles and Practices for Securing Information Technology Systems, describes common security principles that should be addressed within security policies. The purpose of this document is to describe 8 principles and 14 practices that can be used to develop security policies. This standard is based on 8 principles, which are:

1. Computer security supports the mission of the organisation.

2. Computer security is an integral element of sound management.

3. Computer security should be cost-effective.

4. System owners have security responsibilities outside their own organisations.

5. Computer security responsibilities and accountability should be made explicit.

6. Computer security requires a comprehensive and integrated approach.

7. Computer security should be periodically reassessed.

8. Computer is security is constrained by societal factors.

11.2.2 NIST SP 800-35

NIST SP 800-35, Guide to Information Technology Security Services, is an overview of information security. In this standard six phases of the IT security life cycle are defined:

- **Phase 1: Initiation.** At this point the organisation is looking to implement a IT security service, device, or process.
- **Phase 2: Assessment.** This phase involves determining and describing the organisation’s current security posture. It is recommended that this phase uses quantifiable metrics.

- **Phase 3: Solution.** This is where various solutions are evaluated and one or more are selected.
- **Phase 4: Implementation.** In this phase the IT security service, device, or process is implemented.
- **Phase 5: Operations.** Phase 5 is the ongoing operation and maintenance of the security service, device, or process that was implemented in phase 4.
- **Phase 6: Closeout.** At some point, whatever was implemented in phase 4 will be concluded. This often occurs when a system is replaced by a newer and better system.

11.2.3 NIST SP 800-30 Rev. 1

NIST SP 800-30 Rev. 1, Guide for Conducting Risk Assessments, is a standard for conducting risk assessments. Risk assessments were discussed in one of the previous chapters. This standard provides guidance on how to conduct such an assessment. There are nine steps in the process:

STEP 1. System Characterization

STEP 2. Threat Identification

STEP 3. Vulnerability Identification

STEP 4. Control Analysis

STEP 5. Likelihood Determination

STEP 6. Impact Analysis

STEP 7. Risk Determination

STEP 8. Control Recommendations

STEP 9. Results documentation