5: POLICY STANDARDS

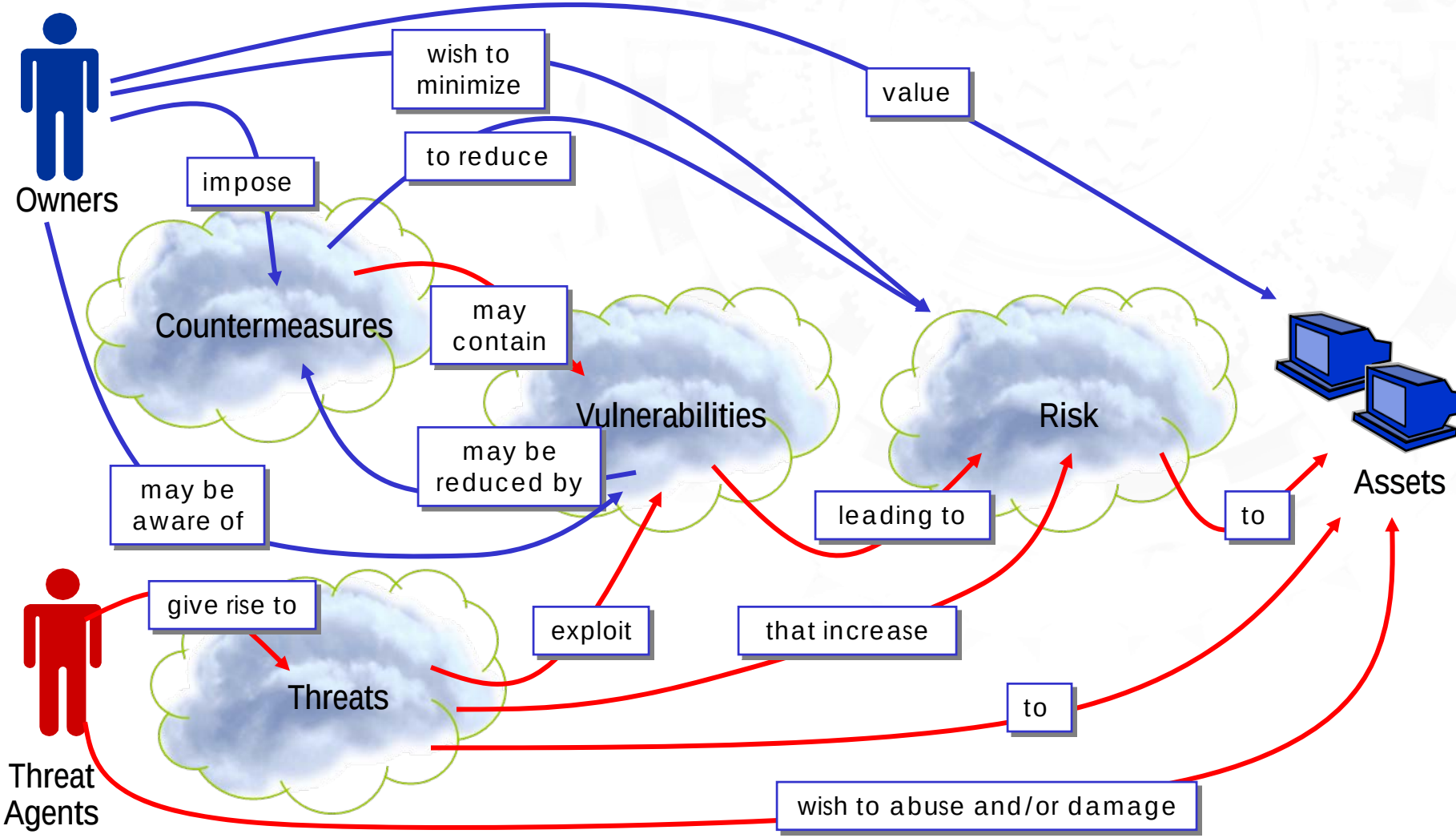
OBJECTIVES

1. Define and explain major information security standards relevant to policy.
2. Identify sources of information to help guide policy and standard development.

Examples of Standards

- ISO/IEC 27001 and 27002 (ISO 17799)
- Common Criteria
- NIST 800 Series of Special Publications
- NIST Federal Information Processing Standards (FIPS)

COMMON CRITERIA: RELATIONSHIPS



NIST 800 SERIES

General security practices:

- 800-14 (Securing IT systems)
- 800-16 (Security training)
- 800-18 (Security plans)
- 800-30 (Risk management)
- 800-34 (Contingency planning)
- 800-37 (Certification & Accreditation)
- 800-53A (Security assessment)
- 800-64 (Security in the SDLC)
- 800-100 (Information Security Handbook)
- 800-115 (Security testing)

NIST 800 SERIES

Focused security practices:

- 800-3 (Incident response)
- 800-9 (E-commerce)
- 800-21 (Implementing cryptography)
- 800-23 (Security assurance & acquisition)
- 800-40 (Patch handling)
- 800-44 (Securing public web servers)
- 800-88 (Media sanitization)
- 800-92 (Security log management)
- 800-95 (Secure web services)
- 800-97 (Wireless security)

NIST 800 SERIES

- Security technology guidelines:
  - 800-25 (Digital signatures)
  - 800-31 (IDS)
  - 800-32 (Federal PKI)
  - 800-41 (Firewalls)
  - 800-45 (Email security)
  - 800-48 (Wireless network security)
  - 800-77 (IPSec VPNs)
  - 800-94 (IDS and IPS systems)
  - 800-113 (SSL VPNs)
  - 800-123 (Server security)

FEDERAL INFORMATION PROCESSING STANDARDS (FIPS)

- Mandatory Security Standards:
  - FIPS 140 (Cryptographic modules)
  - FIPS 186 (Digital signature standard)
  - FIPS 191 (Local area network (LAN) security)
  - FIPS 197 (Advanced encryption standard (AES))
  - FIPS 199 (Security categorization)
  - FIPS 200 (Minimum security requirements)
  - FIPS 201 (Personal identity verification)