Security Controls Are Not Requirements

April 24, 2019

Mark L. Spencer, CISSP
Mark L. Spencer
CISSP #5128 (Jan 1997)
VP and President ISSA-COS 14 years
ISSA Distinguished Fellow
ISSA Honor Roll
President Emeritus ISSA-COS
Over 24 years in cybersecurity
Target Audience

- Entry to mid-level cybersecurity personnel
  1. Have little experience in writing requirements
  2. Have no experience in writing requirements
Target Audience

Why not senior cybersecurity people?

1. Have experience in requirements and are good at writing them

2. Have experience in requirements and avoid them like the plague

3. Both 1 and 2
Why Run from Requirements?

- Too often the following occurs:
- “We need your security requirements by Friday for the new system.”
  - Hundreds of controls to consider
- Panic occurs
Controls are not requirements
For what are requirements used
Identifying requirements using controls
Writing good requirements
Controls

- OMB A-130 Circular defines a Security Control, as “a safeguard or countermeasure prescribed for an information system or an organization to protect the confidentiality, integrity, and availability of the system and its information.”

- Mitigations of previously identified risks

Requirement Types

- Interface, Environment, Training, Personnel
- Physical Characteristics, Operability
- Functional, Performance
- Design

We will use design to illustrate elicitation of requirements
Controls ≠ Requirements

- Controls are verifiable implementations of mitigations
- Requirements are verifiable implementations of design
- Requirements must be achieved to be able to meet controls
Requirement Identification

- Control: backup security audit records weekly
- What must be available allow this control to be met?
  1. Must have a backup capability
  2. Must have security audit records
  3. Must back the audit records up weekly
Design Requirements Rationale

- Needed to meet the control
  - Backup capability (key design requirement)
  - Audit records (not part of this design requirement, probably a configuration issue)
  - A process, manual or automated, to run weekly (not part of this design requirement, could be configuration or procedure)
- Verification of design requirement (not control)
  - Does a backup capability exist?
Control Validation

- Does a backup capability exist?
- Do you backup audit records?
- Do you backup audit records weekly?
Writing a Good Requirement

- One requirement at a time
  - The X system shall do this and that
  - Choose one or make two requirements
    - The X system shall do this
    - The X system shall do that

- Avoid conjunctions
  - and or

- Avoid exceptions
  - The X system shall allow all inputs, except bad ones.

- No negative requirements
  - The X system shall not allow ...
Writing a Good Requirement

- Simple, explicit sentences
  - Specify the “What,” **not** the “How”
  - Fewer words means fewer opportunities to misunderstand
  - Be very specific
  - Use precise measurements instead of general concepts
    - The X system shall be available most of the time.
    - The X system shall be available 99.9% of scheduled operational time.
Writing a Good Requirement

- Must be **achievable**
- Must be **testable** (verifiable)
Writing a Good Requirement

- Unique
- Derived requirements must be traceable
  - Levels of requirements
    - Level 1 – Very high level and general
    - Level 2 – 3 – greater specificity
    - Level 4 and on – more detail
- Define verifiable criteria with precision
  - How does it pass or fail
Exercise

- No one “right” answer
- Lots of “wrong” answers

- What are cybersecurity, high-level design requirements for a new IT system?
Examples of Cybersecurity Requirements

- Boundary layer protection
  - Capability to examine incoming data streams
  - Capability to examine outgoing data streams

- Network defenses
  - Capability to detect malware
  - Capability to eradicate malware
  - Capability to sense network attacks
  - Capability to stop network attacks
Examples of Cybersecurity Requirements

- **Backup system**
  - Capability to backup data to storage media
    - Define “storage media” in notes

- **End Point Protection**
  - Capability to detect cyber attacks directed toward the endpoint device
  - Capability to .....
Summary

- Controls are not requirements
- Design requirements must be met to meet controls
- Not that easy to do...
Security Controls Are Not Requirements

Questions?
References

- https://gracorp.com/write-clear-requirements-document/
- https://www.mpug.com/articles/writing-effective-project-requirements/
- https://gracorp.com/write-clear-requirements-document/
- https://www.whitehouse.gov/sites/whitehouse.gov/files/omb/circulars/A130/a130revised.pdf
Verification & Validation

- **Verification**
  - Did we build the system right?
    - Does it meet the design specifications and requirements?

- **Validation**
  - Did we build the right system?
    - Does it do what the customer expects?