Internal Control:
A Standard Setter’s Perspective
What Is Internal Control?

Formal Definition:
a process effected by an entity’s oversight body, management, and other personnel that provides reasonable assurance that the objectives of an entity will be achieved.
What Is Internal Control? (Cont.)

Informally:
a process to help entities achieve objectives.

Source: GAO. | GAO-14-704G
# Green Book: Components, Principles and Attributes

<table>
<thead>
<tr>
<th>5 Components</th>
<th>17 Principles</th>
<th>48 Attributes</th>
</tr>
</thead>
<tbody>
<tr>
<td>Control Environment</td>
<td>1. Demonstrate Commitment to Integrity and Ethical Values</td>
<td>Tone at the top: Standards of Conduct</td>
</tr>
<tr>
<td>Risk Assessment</td>
<td>2. Exercise Oversight Responsibility</td>
<td>Adherence to standards of conduct</td>
</tr>
<tr>
<td>Control Activities</td>
<td>3. Establish Structure, Responsibility, and Authority</td>
<td>Oversight Structure</td>
</tr>
<tr>
<td>Information &amp; Communication</td>
<td>4. Demonstrate Commitment to Competence</td>
<td>Oversight for the Internal Control System</td>
</tr>
<tr>
<td>Monitoring</td>
<td>5. Enforce Accountability</td>
<td>Input for Remediation of Deficiencies</td>
</tr>
<tr>
<td></td>
<td>6. Define Objectives and Risk Tolerances</td>
<td>Definition of Objectives</td>
</tr>
<tr>
<td></td>
<td>7. Identify, Analyze, and Respond to Risk</td>
<td>Definitions of Risk Tolerances</td>
</tr>
<tr>
<td></td>
<td>8. Assess Fraud Risk</td>
<td>Identification of Risks</td>
</tr>
<tr>
<td></td>
<td>9. Analyze and Respond to Change</td>
<td>Analysis of Risks</td>
</tr>
<tr>
<td></td>
<td>10. Design Control Activities</td>
<td>Response to Risks</td>
</tr>
<tr>
<td></td>
<td>11. Design Activities for the Information System</td>
<td>Types of Fraud</td>
</tr>
<tr>
<td></td>
<td>12. Implement Control Activities</td>
<td>Fraud Risk Factors</td>
</tr>
<tr>
<td></td>
<td>13. Use Quality Information</td>
<td>Response to Fraud Risks</td>
</tr>
<tr>
<td></td>
<td>14. Communicate Internally</td>
<td>Identification of Change</td>
</tr>
<tr>
<td></td>
<td>15. Communicate Externally</td>
<td>Analysis of and Response to Change</td>
</tr>
<tr>
<td></td>
<td>16. Perform Monitoring Activities</td>
<td>Response to Objectives and Risks</td>
</tr>
<tr>
<td></td>
<td>17. Remediate Deficiencies</td>
<td>Design of Appropriate Types of Control Activities</td>
</tr>
</tbody>
</table>

**Definitions and Descriptions:**

- **Control Environment:**
  - Tone at the top: Standards of Conduct
  - Adherence to standards of conduct
  - Oversight Structure
  - Oversight for the Internal Control System

- **Risk Assessment:**
  - Input for Remediation of Deficiencies
  - Definition of Objectives
  - Definitions of Risk Tolerances

- **Control Activities:**
  - Identification of Risks
  - Analysis of Risks
  - Response to Risks
  - Types of Fraud

- **Information & Communication:**
  - Fraud Risk Factors
  - Response to Fraud Risks
  - Identification of Change

- **Monitoring:**
  - Analysis of and Response to Change

**Additional Elements:**

- **Response to Objectives and Risks:**
  - Design of Appropriate Types of Control Activities
  - Design of Control Activities at Various Levels

- **Information & Communication:**
  - Communication throughout the Entity
  - Appropriate Methods of Communication
  - Communication with External Parties

- **Monitoring:**
  - Reporting of Issues
  - Corrective Actions

- **Establishing a Robust Internal Control System Monitoring:**
  - Evaluation of Risks
  - Reporting of Issues
  - Corrective Actions
Component, Principle, and Attributes Working Together

Control Environment

The oversight body and management should demonstrate a commitment to integrity and ethical values

Component

Principle

Attributes

Set the Tone at the Top

Establish standards of conduct

Evaluate adherence to standards of conduct
Example Objective From Daily Life

Having dinner as a family
Family Dinner

Different Factors = Success

Requirements:

• Everyone there at same time, ready to eat; need:
  o Communication
  o Planning
  o Consistency
  o Conduct expectations

• Food to eat; need:
  o Supplies/equipment
  o A plan
  o Competent cook

• Contingency plans
Prioritize Dinner

Leading by example

Leadership: demonstrates commitment by adhering to standards of conduct

5 Components
- Control Environment
- Risk Assessment
- Control Activities
- Information & Communication
- Monitoring

17 Principles
1. Demonstrate Commitment to Integrity and Ethical Values
2. Exercise Oversight Responsibility
3. Establish Structure, Responsibility, and Authority
4. Demonstrate Commitment to Competence
5. Enforce Accountability
6. Define Objectives and Risk Tolerances
7. Identify, Analyze, and Respond to Risk
8. Assess Fraud Risk
9. Analyze and Respond to Change
10. Design Control Activities
11. Design Activities for the Information System
12. Implement Control Activities
13. Use Quality Information
14. Communicate Internally
15. Communicate Externally
16. Perform Monitoring Activities
17. Remediate Deficiencies
Have a Competent Cook

Take cooking classes (if needed)

Knowledge and skills - critical to success

Obtained by:
• Experience
• Training
• Certification

5 Components

- Control Environment
- Risk Assessment
- Control Activities
- Information & Communication
- Monitoring

17 Principles

1. Demonstrate Commitment to Integrity and Ethical Values
2. Exercise Oversight Responsibility
3. Establish Structure, Responsibility, and Authority
4. Demonstrate Commitment to Competence
5. Enforce Accountability
6. Define Objectives and Risk Tolerances
7. Identify, Analyze, and Respond to Risk
8. Assess Fraud Risk
9. Analyze and Respond to Change
10. Design Control Activities
11. Design Activities for the Information System
12. Implement Control Activities
13. Use Quality Information
14. Communicate Internally
15. Communicate Externally
16. Perform Monitoring Activities
17. Remediate Deficiencies
Have a Backup Dinner Plan

Respond to unexpected changes

What if an ingredient is missing?
Is there a backup plan (other than fast food)?

<table>
<thead>
<tr>
<th>5 Components</th>
<th>17 Principles</th>
</tr>
</thead>
<tbody>
<tr>
<td>Control Environment</td>
<td>1. Demonstrate Commitment to Integrity and Ethical Values</td>
</tr>
<tr>
<td>Risk Assessment</td>
<td>2. Exercise Oversight Responsibility</td>
</tr>
<tr>
<td>Control Activities</td>
<td>3. Establish Structure, Responsibility, and Authority</td>
</tr>
<tr>
<td>Information &amp;</td>
<td>4. Demonstrate Commitment to Competence</td>
</tr>
<tr>
<td>Communication</td>
<td>5. Enforce Accountability</td>
</tr>
<tr>
<td>Monitoring</td>
<td>6. Define Objectives and Risk Tolerances</td>
</tr>
<tr>
<td></td>
<td>7. Identify, Analyze, and Respond to Risk</td>
</tr>
<tr>
<td></td>
<td>8. Assess Fraud Risk</td>
</tr>
<tr>
<td></td>
<td>9. Analyze and Respond to Change</td>
</tr>
<tr>
<td></td>
<td>10. Design Control Activities</td>
</tr>
<tr>
<td></td>
<td>11. Design Activities for the Information System</td>
</tr>
<tr>
<td></td>
<td>12. Implement Control Activities</td>
</tr>
<tr>
<td></td>
<td>13. Use Quality Information</td>
</tr>
<tr>
<td></td>
<td>14. Communicate Internally</td>
</tr>
<tr>
<td></td>
<td>15. Communicate Externally</td>
</tr>
<tr>
<td></td>
<td>16. Perform Monitoring Activities</td>
</tr>
<tr>
<td></td>
<td>17. Remediate Deficiencies</td>
</tr>
</tbody>
</table>
Ensure There are Supplies

Manage a slew of related activities

Weekly plan may consist of:
- Planning meals
- Taking inventory
- Getting supplies

May be done by more than one person

<table>
<thead>
<tr>
<th>5 Components</th>
<th>17 Principles</th>
</tr>
</thead>
<tbody>
<tr>
<td>Control Environment</td>
<td>1. Demonstrate Commitment to Integrity and Ethical</td>
</tr>
<tr>
<td></td>
<td>Values</td>
</tr>
<tr>
<td>Risk Assessment</td>
<td>2. Exercise Oversight Responsibility</td>
</tr>
<tr>
<td></td>
<td>3. Establish Structure, Responsibility, and Authority</td>
</tr>
<tr>
<td></td>
<td>4. Demonstrate Commitment to Competence</td>
</tr>
<tr>
<td>Control Activities</td>
<td>5. Enforce Accountability</td>
</tr>
<tr>
<td>Information &amp;</td>
<td>6. Define Objectives and Risk Tolerances</td>
</tr>
<tr>
<td>Communication</td>
<td>7. Identify, Analyze, and Respond to Risk</td>
</tr>
<tr>
<td>Monitoring</td>
<td>8. Assess Fraud Risk</td>
</tr>
<tr>
<td></td>
<td>9. Analyze and Respond to Change</td>
</tr>
<tr>
<td></td>
<td>10. Design Control Activities</td>
</tr>
<tr>
<td></td>
<td>11. Design Activities for the Information System</td>
</tr>
<tr>
<td></td>
<td>12. Implement Control Activities</td>
</tr>
<tr>
<td></td>
<td>13. Use Quality Information</td>
</tr>
<tr>
<td></td>
<td>14. Communicate Internally</td>
</tr>
<tr>
<td></td>
<td>15. Communicate Externally</td>
</tr>
<tr>
<td></td>
<td>16. Perform Monitoring Activities</td>
</tr>
<tr>
<td></td>
<td>17. Remediate Deficiencies</td>
</tr>
</tbody>
</table>
Communicate

Family Calendar

Does Susie have a recital?

Family calendar can help ensure plans succeed

---

### 5 Components

- **Control Environment**
- **Risk Assessment**
- **Control Activities**
- **Information & Communication**
- **Monitoring**

### 17 Principles

1. Demonstrate Commitment to Integrity and Ethical Values
2. Exercise Oversight Responsibility
3. Establish Structure, Responsibility, and Authority
4. Demonstrate Commitment to Competence
5. Enforce Accountability
6. Define Objectives and Risk Tolerances
7. Identify, Analyze, and Respond to Risk
8. Assess Fraud Risk
9. Analyze and Respond to Change
10. Design Control Activities
11. Design Activities for the Information System
12. Implement Control Activities
13. Use Quality Information
14. Communicate Internally
15. Communicate Externally
16. Perform Monitoring Activities
17. Remediate Deficiencies
Adapt Strategy if Dinner Doesn’t Happen
Change course if needed

Family dinner not happening?
Controls need to be improved

<table>
<thead>
<tr>
<th>5 Components</th>
<th>17 Principles</th>
</tr>
</thead>
<tbody>
<tr>
<td>Control Environment</td>
<td>1. Demonstrate Commitment to Integrity and Ethical Values</td>
</tr>
<tr>
<td>Risk Assessment</td>
<td>2. Exercise Oversight Responsibility</td>
</tr>
<tr>
<td>Control Activities</td>
<td>3. Establish Structure, Responsibility, and Authority</td>
</tr>
<tr>
<td>Information &amp; Communication</td>
<td>4. Demonstrate Commitment to Competence</td>
</tr>
<tr>
<td>Monitoring</td>
<td>5. Enforce Accountability</td>
</tr>
<tr>
<td></td>
<td>6. Define Objectives and Risk Tolerances</td>
</tr>
<tr>
<td></td>
<td>7. Identify, Analyze, and Respond to Risk</td>
</tr>
<tr>
<td></td>
<td>8. Assess Fraud Risk</td>
</tr>
<tr>
<td></td>
<td>9. Analyze and Respond to Change</td>
</tr>
<tr>
<td></td>
<td>10. Design Control Activities</td>
</tr>
<tr>
<td></td>
<td>11. Design Activities for the Information System</td>
</tr>
<tr>
<td></td>
<td>12. Implement Control Activities</td>
</tr>
<tr>
<td></td>
<td>13. Use Quality Information</td>
</tr>
<tr>
<td></td>
<td>14. Communicate Internally</td>
</tr>
<tr>
<td></td>
<td>15. Communicate Externally</td>
</tr>
<tr>
<td></td>
<td>16. Perform Monitoring Activities</td>
</tr>
<tr>
<td></td>
<td>17. Remediate Deficiencies</td>
</tr>
</tbody>
</table>
Internal Control Components

Components; not one dimensional.

May be different based on:
- Objectives
- Organizational structure
Example Objectives

Operations
- Protect US & Allies
- Use resources efficiently
- Safeguard tangible and intangible assets

Reporting
Relevant, reliable, and timely financial data for taxpayers

Compliance
Comply with laws and regulations
Example Organizational Structure

**Entity**
Department of Defense

**Division**
Military Services and ODOs

**Operating Unit**
Military Sealift Command (Navy)

**Function**
Operations and Maintenance Procurement
Audit Findings

Up Next – Selected Findings from the FY 2018 audits discussing:

- Challenges for financial reporting
- How internal control can help
- Overlap of reporting objectives and compliance objectives.
Internal Control in Practice

Information Technology
Information Technology Controls Need Improvement

FY 2018 Financial Statement Audit:

• DOD Inspector General listed IT as one of the 20 Material Weaknesses

• DOD management reported:
  “DOD financial and business management systems and processes do not provide reliable, timely, nor accurate information”
Information Technology Impact On Objectives

Operations:
- Information security
- Weapon system functioning
- Protecting intangible assets

Reporting:
- Material weakness

Compliance:
- FMFIA compliance
Green Book: IT Controls

5 Components

- Control Environment
- Risk Assessment
- Control Activities
- Information & Communication
- Monitoring

17 Principles

1. Demonstrate Commitment to Integrity and Ethical Values
2. Exercise Oversight Responsibility
3. Establish Structure, Responsibility, and Authority
4. Demonstrate Commitment to Competence
5. Enforce Accountability
6. Define Objectives and Risk Tolerances
7. Identify, Analyze, and Respond to Risk
8. Assess Fraud Risk
9. Analyze and Respond to Change
10. Design Control Activities
11. Design Activities for the Information System
12. Implement Control Activities
13. Use Quality Information
14. Communicate Internally
15. Communicate Externally
16. Perform Monitoring Activities
17. Remediate Deficiencies
Information Technology: Controls

DOD policy\(^1\) requires the use of security controls from NIST Special Publication 800-53

---

1. DOD instruction No. 8510.01, *Risk Management Framework for DOD Information Technology*
Information Technology: Management Objectives

DOD policy\textsuperscript{1} states:

\textit{DOD must have an enterprise-wide decision structure for cybersecurity risk management

This comprehensive framework must ensure the effectiveness of information security controls over information resources

1. DOD instruction No. 8510.01, Risk Management Framework for DOD Information Technology, which requires adherence to Chapter 35 of Title 44, United States Code}
Access Controls

Limit or detect unauthorized access to computer resources

- Data
- Equipment
- Facilities

Protecting from unauthorized modification, loss, and disclosure.
Access Controls
Reporting Example

Intrusion Detection

What Auditors Found

An entity did not have an intrusion detection system (IDS) placed behind firewalls in an accounting system.

There were no host intrusion prevention systems (HIPS) in place.
Access Controls
Reporting Example

Criteria

Allow only authorized accesses for users which are necessary to accomplish assigned tasks

Why it Happened

The accounting system resides on a legacy network that does not include IDS or HIPS.

1. NIST SP 800-53, AC-6
Access Controls
Reporting Example

Impact

• anomalous activities on the network could go undetected
• alerts may not be sent to the appropriate personnel
• malicious traffic may not be identified and mitigated in a timely manner
• decreases the reliability of information reported on the financial statements.
Application of the Green Book

11.11 Management designs control activities for security management of the entity’s information system for appropriate access by internal and external sources to protect the entity’s information system.

11.12 Security management includes the information processes and control activities related to access rights in an entity’s information technology, including who has the ability to execute transactions.

Principle 11 Attributes:
- Design of the Entity’s Information System
- Design of Appropriate Types of Control Activities
- Design of Information Technology Infrastructure
- Design of Security Management
- Design of IT Acquisition, Development, and Maintenance
Access Controls
Operations Example

What Auditors Found

Cybersecurity test reports that GAO reviewed showed that test teams were able to gain unauthorized access and take full or partial control of weapon systems in a short amount of time using relatively simple tools and techniques.
Access Controls
Operations Example

Criteria

The organization:

a. Establishes and documents usage restrictions, configuration/connection requirements, and implementation guidance for each type of remote access allowed; and

b. Authorizes remote access to the information system prior to allowing such connections

Why it Happened

Historically, DOD focused on the cybersecurity of its networks, but not weapon systems themselves.

1. NIST SP 800-53, AC-17
Impact

Cyber attacks can target any weapon subsystem that is dependent on software, potentially leading to an inability to complete military missions or even loss of life.

Weapon system functions susceptible to compromise:

- Powering a system on and off
- Targeting a missile
- Maintaining a pilot’s oxygen level
- Flying aircraft

Source: DOD | https://media.defense.gov
Changing conditions often prompt new risks or changes to existing risks that need to be assessed. As part of analyzing and responding to change, management performs a risk assessment to identify, analyze, and respond to any new risks prompted by the changes.
Segregation of Duties

Movie Theater Example

Counts the till, observes

Sells Ticket

Takes the Ticket
Segregation of Duties
Reporting Example

What Auditors Found

No controls were in place to prevent system administrators from giving themselves Contracting Officer capabilities.
Segregation of Duties Reporting Example

Criteria

The organization:

a. Separates duties of individuals,

b. Documents separation of duties of individuals; and

c. Defines information system access authorizations to support separation of duties.¹
Segregation of Duties

Reporting Example

Why it Happened

Management did not define which roles and functions are incompatible and would cause a segregation of duties conflict.

Impact

Increased risk that unauthorized access or inappropriate activity could occur without detection or management knowledge.

Could affect the accuracy, integrity, and availability of the system and data.
Management considers segregation of duties in designing control activity responsibilities so that incompatible duties are segregated and, where such segregation is not practical, designs alternative control activities to address the risk.

10.12 Management considers segregation of duties in designing control activity responsibilities so that incompatible duties are segregated and, where such segregation is not practical, designs alternative control activities to address the risk.
Configuration Management

- Centralized oversight of the entire network
- Using security policies to prevent application-level changes from happening without formal review
Configuration Management Reporting Example

What Auditors Found

For a human resources web application:

Management did not have a complete and accurate configuration inventory of

- Hardware
- Software
- Firmware
Configuration Management Reporting Example

Criteria

Baseline configuration:
“The organization develops, documents, and maintains under configuration control, a current baseline configuration of the information system.”

Why it Happened
Management is in the process of updating the inventory, however they are not finished yet.

1. NIST SP 800-53, CM-2
Impact

Management will be unable to accurately know the effect of application changes on the full enterprise.

If financial systems are not configured correctly, reported financial information may not be reliable.
Application of the Green Book

Principle 11 Attributes:
- Design of the Entity’s Information System
- Design of Appropriate Types of Control Activities
- Design of Information Technology Infrastructure
- Design of Security Management
- Design of IT Acquisition, Development, and Maintenance

11.07 Information system general controls … include security management, logical and physical access, configuration management, segregation of duties, and contingency planning.
IT Objectives are not Achieved

Auditor Findings = Symptoms

IT Controls = Cure
Internal Control in Practice

DOD Mission Critical Assets

Real Property

Source: Defense Imagery and Video Distribution System | www.dvidshub.net

Equipment

Source: U.S. Army | www.army.mil

Supplies

Source: Defense Imagery and Video Distribution System | www.dvidshub.net
Asset Accountability Impact On Objectives

Operations:
Location and condition of mission critical assets

Reporting:
• Existence
• Completeness
• Valuation
Mission Critical Assets – Key Information

• Assets DOD has
• Location
• Condition
• Cost
DOD Objectives for Real Property

Operations

Real property managed to promote most efficient and effective use.\(^1\)

Reporting

All PP&E acquired by DOD

- Must be recognized for accountability and financial reporting.
- Should have correct acquisition value.\(^2\)

1. DOD Directive 4165.06
2. DOD Financial Management Regulation, vol. 4, chapter 6
Real Property Example

Existence

What Auditors Found

Real property assets recorded did not exist

- Demolished assets not removed from property system.
- Demolished assets shown as active in another service’s property system.
Real Property Example: Existence

Operations Criteria

Real property that is no longer required should be disposed.\(^1\)

Reporting Criteria

Entries to record financial transactions must be supported by source documents, including all disposals or retirements.\(^2\)

\(^1\) DOD Directive 4165.06
\(^2\) DOD Financial Management Regulation, vol. 4, chapter 6, 060106
Real Property Example: Existence

Why it Happened

- Lack of control over transactions shown by deletions not in system.
- Process to obtain approval and subsequently demolish an asset
  - Has multiple steps
  - Extends over a long period of time
Real Property Example: Existence

Impact on Operations
DOD cannot accurately determine the sustainment needs and related costs for its real property.

Impact on Reporting
The reported dollar amount of DOD real property is inaccurate.
Application Of The Green Book

**Control Activities**

**10. Design Control Activities**

**11. Design Activities for the Information System**

**12. Implement Control Activities**

**Principle 10 Attributes:**
- **Response to Objectives and Risks**
- Design of Appropriate Types of Control Activities
- Design of Control Activities at Various Levels
- Segregation of Duties

**10.02** Management designs control activities to address objectives and risks

**10.03** Management clearly documents internal control and all transactions and other events
Real Property Example: Completeness

What Auditors Found

Real property assets exist, but not recorded in DOD records.
Real Property Example: Completeness

Operations Criteria

All PP&E acquisitions must be recognized for accountability purposes.¹

Reporting Criteria

Entries to record financial transactions must be supported by source documents reflecting all transactions affecting real property.²

1. DOD Financial Management Regulation, vol. 4, chapter 6, 060105
2. DOD Financial Management Regulation, vol. 4, chapter 6, 060106
Real Property Example: Completeness

Why it Happened

Real Property Accountable Officers (RPAOs) did not timely record assets in system.

Real property added to the site without the RPAOs knowledge.
Real Property Example: Completeness

Impact on Operations

Real property not included in records may not be most economically managed.

Impact on Reporting

The reported dollar amount of real property is inaccurate.
Application Of The Green Book

Principle 10 Attributes:
- Response to Objectives and Risks
- Design of Appropriate Types of Control Activities
- Design of Control Activities at Various Levels
- Segregation of Duties

10.03 Transactions are promptly recorded for relevance and value in controlling operations and making decisions.
DOD Objectives for Equipment

Operations

Financial management of accountable government property:
• Contributes to operational readiness
• Supports auditability.¹

Reporting

All PP&E acquired by DOD
• Must be recognized for accountability and financial reporting
• Should have correct acquisition value.²

¹ DOD Instruction 5000.64
² DOD Financial Management Regulation, vol. 4, chapter 6
Equipment Example

What Auditors Found

Equipment records had:

- Duplicate asset records
- Blank fields including:
  - serial numbers
  - locations
Equipment Example

Operations Criteria

*Internal controls support the efficient and effective material management of accountable government property.*\(^1\)

Reporting Criteria

*Accounting entries must enable periodic, independent verification by periodic physical inventories.*\(^2\)

1. DOD Instruction 5000.64
2. DOD Financial Management Regulation, vol. 4, chapter 6, 060106
Why it Happened

- The military service’s procedures to address blank, inaccurate data fields, and duplicate records are not operating effectively.

- These errors occur due to human error or systems issues.
Equipment Example

Operations Impact

Possible loss, damage, theft, or waste of equipment

Reporting Impact

General equipment could be materially misstated on financial statements and notes.
Control Activities

10. Design Control Activities
11. Design Activities for the Information System
12. Implement Control Activities

Principle 10 Attributes:
- Response to Objectives and Risks
- Design of Appropriate Types of Control Activities
- Design of Control Activities at Various Levels
- Segregation of Duties

10.06 Control activities can be implemented in either an automated or a manual manner. Automated control activities are either wholly or partially automated through the entity’s information technology.
Objectives For Supplies

Operations

• Effective/efficient management of supplies
• Avoiding spending on unneeded materials.

Reporting

• Compliance with Generally Accepted Accounting Principles (GAAP)
• DOD Components responsible for ensuring that supplies are accounted per GAAP.
Supplies Example #1

What Auditors Found

Missile motors at one base were found to be in working order, but were recorded as unusable.
Supplies Example #1

Operating Criteria

*Personnel with physical custody of assets keep records of*

- Quantity
- Condition.¹

Reporting Criteria

*Supplies are reported and valued differently based on condition.*²

---

1. DOD Manual 4140.01, Vol. 11, 3.3.c.(1)
2. SFFAS No. 3
Supplies Example #1

Why this Happened

- DOD guidance not followed on use of Supply Condition Code.
- Lack of clear policies on proper use of Logistic Supply Condition Codes.
- Lack of appropriate training for maintenance staff.
- Lack of effective internal control in place to prevent incorrect condition codes being updated to the property records.
Supplies Example #1

Operations Impact

Putting these useable motor missiles back in circulation allowed DOD to redirect needed resources to supporting mission.

Reporting Impact

Incorrect information provided for “OM&S Held for Repair” and “OM&S Held for Use.”
Application Of The Green Book

Control Activities
10. Design Control Activities
11. Design Activities for the Information System
12. Implement Control Activities

Principle 10 Attributes:
- Response to Objectives and Risks
- Design of Appropriate Types of Control Activities
- Design of Control Activities at Various Levels
- Segregation of Duties

10.10 Transaction control activities are actions built directly into operations to help the entity achieve objectives and address risks. Management may design transaction control activities for operations, including verifications.
Supplies Example #2

What Auditors Found

Inventory recorded as “repairable” was beyond repair.

- Nose tips and boom cones should have been $0.
Supplies Example #2

Operating Criteria

*Personnel with physical custody of assets will keep records of*

- Quantity
- Condition.¹

Reporting Criteria

"*Unserviceable inventory*" is damaged inventory that is more economical to dispose of than to repair.²

¹. DOD Manual 4140.01, Vol. 11, 3.3.c.1
². SFFAS No. 3, Paragraph 29-30
Supplies Example #2

Why this happened

No control for performing periodic reconciliations.

Lag time from classifying inventory as repairable to beyond repair.
Supplies Example #2

Operations Impact
Inaccurate data imperils mission readiness.

Reporting Impact
Financial statements could be materially misstated.
16.04 Management monitors the internal control system through ongoing monitoring and separate evaluations.

16.05 Management performs ongoing monitoring of the design and operating effectiveness of the internal control system as part of the normal operations.

Principle 16 Attributes:
- Establishment of a Baseline
- Internal Control System Monitoring
- Evaluation of Results
Questions?

• Practical Application of the Green Book
• Information Technology
• Mission Critical Assets
Where to Find Us

- The Green Book is available on GAO’s website at: www.gao.gov/greenbook

- For technical assistance, contact us at: greenbook@gao.gov or call (202) 512-9535

- The source for all photos is GAO, unless otherwise attributed