Planning vs Testing for Security in T&E Software Development

Kathy Reid
March - 2012

DISTRIBUTION A. Approved for public release; distribution unlimited.

Outline

- Organization
- Standard Process
- Problem
- Tailored Process
- Analysis
- Real World Example

DISTRIBUTION A. Approved for public release; distribution unlimited.

Organization – Mission

- **46 Range Control Squadron (46 RNCS) Mission**
  - Provide mathematical, engineering and software development for test data from aircraft, weapons and Command and Control Systems
  - Provide analysis, control and range safety of test and training missions on the Eglin range
  - Provide modeling and simulation analysis expertise for surface to air threat systems
  - Serve as the Air Force lead for target drone control software development

DISTRIBUTION A. Approved for public release; distribution unlimited.

Organization – Objective

Provide a quality product to a satisfied customer on time and within cost, as promised

Challenge: Potential vulnerabilities/security threats exist and continually impact our ability to deliver a quality product on time

Solution: Integrate security requirements into the system to allow for continuous threat monitoring

Organization – Approach

Rated as a Capability Maturity Model Integration (CMMI) Maturity Level 3 organization, which means we have established a

- Proven performance record
- Documented software development and systems engineering processes
- Instantiated common assets available to all software development teams across the organization

DISTRIBUTION A. Approved for public release; distribution unlimited.

Organization – CMMI Model

- **Process areas that specifically address testing**
  - **Verification**
    - Conduct preparation tasks for verification
    - Perform peer reviews on selected work products
    - Verify selected work products against their specified requirements
  - **Validation**
    - Conduct preparation tasks for validation
    - Validate product to ensure suitability for use in its intended environment

Organization – CMMI Model

- **Process areas that support testing**
  - **Configuration Management**
    - Place testing work products under configuration management
  - **Process and Product Quality Assurance**
    - Review testing work products for quality and adherence to standards

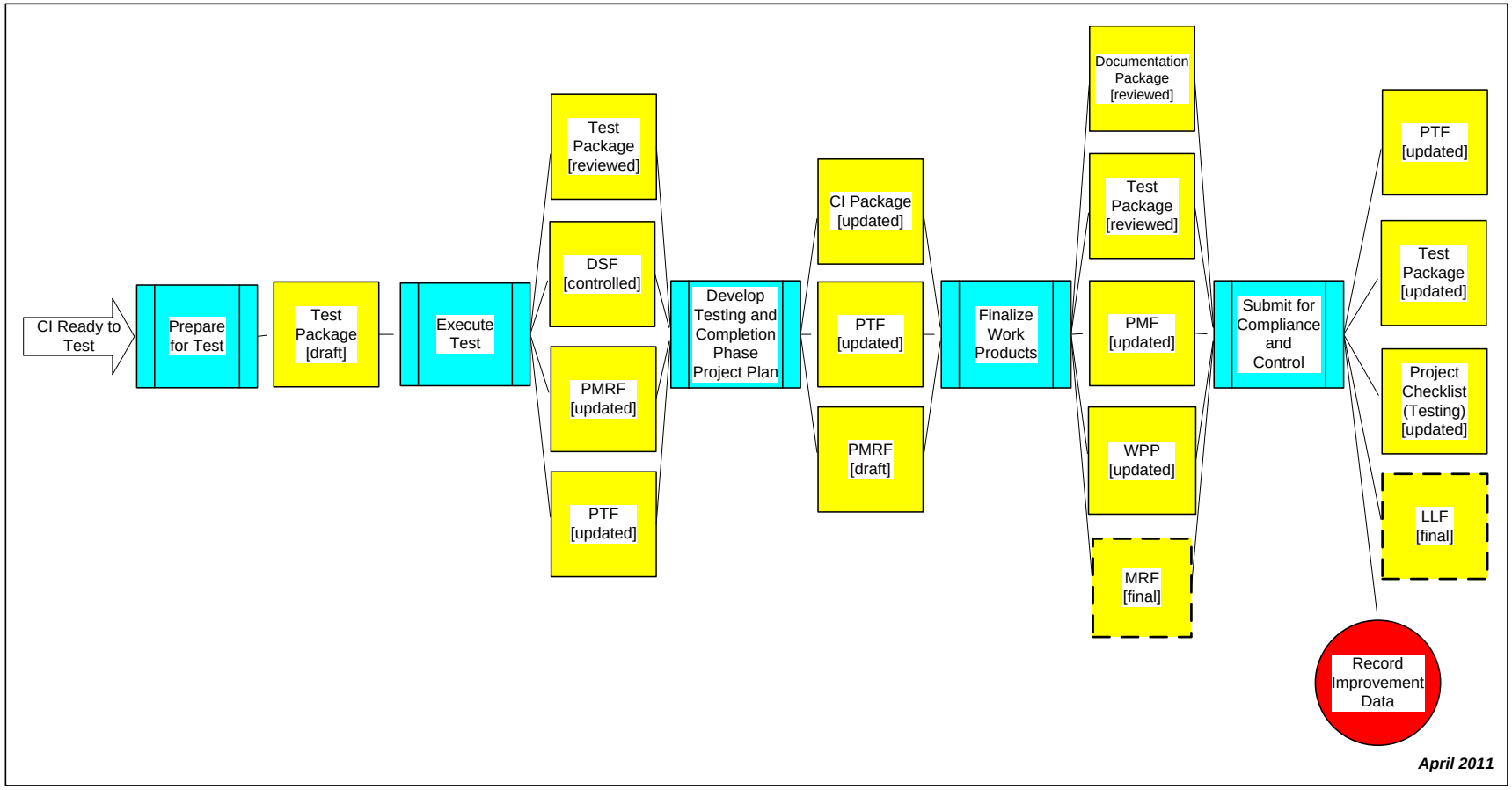
Standard Process…

- **Enable variation in Perspectives**
  - **Expertise (novice, expert)**
  - **Discipline (software, system, service)**
- **Contain detailed procedures**
  - **Visually**
  - **Textually**
- **Provide easy access to required artifacts**
  - **Templates to set content expectations**
  - **Plans, test cases, data, scripts and schedules**

DISTRIBUTION A. Approved for public release; distribution unlimited.

Standard Process – Graphical Expert View

Testing [Process Overview]



Standard Process – Textual Novice View

Step	Action	Artifact	Responsible
Verify Entry Criteria			
1	Verify the CI is ready for testing	E-mail	PL
2	Review Testing as well as Compliance and Control Process LLFs and best practices	Process Overview	PL
3	Collect required project testing artifacts collectively referred to as the Test Package • STP - record the scenarios and/or detailed test cases for each applicable level of testing (integration, system, acceptance) • Approved Section Product for the test document or database stored on the SKP • DSF - record process type, phase, participants, products, and findings for testing	STP SKP (Section Templates) DSF	PL
4	Record the Testing Phase adjusted completion date in the PTF by referencing the delta between the estimated start date and the actual start date and making the appropriate changes to the adjusted completion date	PTF (Breakdown)	PL
Prepare for Test			
5	Update the Test Package to document the verification test cases/drivers, criteria to ensure the requirements are met, and the environment to include equipment, software and resources	Test Package	PL
6	Update the Test Package to document the validation test cases/drivers, criteria to ensure the product fulfills its intended use	Test Package	PL
7	Setup environment to support verification and validation activities and confirm that each component is identified, functions correctly and complies with interface descriptions as defined in the Test Package	Test Package	PL
8	Submit an electronic message with the testing instructions to the Testers defining how to record testing issues, defect saves and lessons learned	E-mail	PL

Standard Process – Textual Novice View

Step	Action	Artifact	Responsible
Execute Test			
9	If the Test Package is complex, Testers/Verifiers do not have domain knowledge, or have questions about the Test Package and/or the product being tested, execute a preview meeting following the **Meeting Process** at least one working day after the test message is distributed. Preview meeting must review goals of the test, and have Implementor or PL present to discuss the product being tested and address questions	Calendar, E-mail	PL, Tester, Verifier
10	Execute verification and validation activities as defined by the test cases in the Test Package using Approved Section-specific checklists, templates and standards stored on the SKP (note: if a specified level of testing is not performed an explanation is required in the PTF)	SKP (Section Checklists) SKP (Section Templates) SKP (Section Policies, Procedures and Standards) PTF (Tailoring)	Tester
11	Analyze the verification and validation results to confirm the components were assembled according to the defined integration sequence, to verify/validate interfaces performed correctly, and to determine if the test case passed or failed based on defined criteria	Test Package DSF	Tester
12	Record test indicator, severity, injection and type and time spent on verification and validation activities, as requested by the PL (note: issues are not required to have severity, injection and type defined - "None chosen" can be selected for these fields)	DSF	Recorder
13	Record causal analysis on all major testing defect saves by identifying the root cause of the defect save, recording probable cause, and identifying improvements to eliminate future defect saves in the DSF (note: improvements must be documented using SERTS to submit a change request	DSF SERTS	PL

Standard Process – Textual Novice View

Step	Action	Artifact	Responsible
14	Execute rework, record rework effort and enter Section required testing information in the comments fields of the DSF then notify the Verifier when the product is ready for verification. Rework includes updates to any of the following items: • Requirements Package - SRS/RTM, SRSF or an Approved Section Product • Design Package - SDD or an Approved Section Product • Technical Data Package - implementation artifacts created to accomplish the defined requirements • Documentation Package - artifacts created to understand the functionality • Test Package - STP or an Approved Section Product	SRS/RTM, SRSF, SDD, Technical Data Package, STP, Documentation, Approved Section Product PTF (Tailoring) DSF	PL
15	Verify test defect saves were corrected, record verification effort and enter Section required testing information in the comments field of the DSF then notify the PL when the verification is complete	DSF E-mail	Verifier
16	Execute steps 10-15 with PL and Tester until all failed test cases are corrected and verified and notify the PL the testing verification is complete	DSF E-mail	Verifier
17	Review validation results and correct items listed as non-compliant	PTF (Testing)	PL
18	Record the pass/fail test results in the Requirements Testing documentation (e.g., SRS/RTM, SRSF, DSF or via an Approved Section-specific document) as defined by Section-specific testing procedures • If the SRSF or RTM is used, a row must be added to the requirements testing section for each time the requirement failed testing with the last entry of a failed requirement showing that the requirement passed • If the DSF or Approved Section product is used, the requirement identifier must be referenced to provide a mechanism to cross-reference requirements and testing)	SRS/RTM, SRSF, Approved Section Product DSF	PL

Standard Process – Textual Novice View

Step	Action	Artifact	Responsible
19	Record/update testing techniques and Test Package storage location for integration, system and acceptance testing, as applicable, in the PTF	PTF (Tailoring)	PL
20	When acceptance testing is completed: • Record customer acceptance of the product via electronic message or PMRF • Coordinate with the Section Security Representative to verify the proper markings are placed on the classified documents associated with the project • Deliver the product as defined by the Section CMF	E-mail PMRF (Testing)	PL
Develop Testing and Completion Phase Project Plan			
21	Update the Requirements Package, PTO Package, Design Package, Technical Data Package, and Documentation Package based on the Test Package and verify the packages are accurately cross-referenced	SRS/RTM or SRSF, SDD, Technical Data Package, STP, Documentation, PTO Package, Approved Section Product PTF (Tailoring)	PL
22	Define the key tasks required to accomplish the next Testing Phase (if more than one phase of testing is performed) or the Completion Phase, when the last phase of testing is performed and assess the impact of the following factors: • Number of planned key tasks • Availability of assigned resources (i.e., leave, training courses, etc.) • Project productivity to date recorded in the PMF • Peer review trends (estimated vs actual review and rework effort) captured in AMET • Probability of completing the project within the defined quality goals (key tasks, requirement priority, etc.)	PMF (Metrics) PTF (Breakdown) SKP (Section Templates) AMET	PL
23	Record the key tasks derived from the detailed planning activities and for any changes to dates, effort and scope acquire team commitment to applicable test phase or the completion phase project plan via the PMRF, e-mails controlled as data management items, or if more than eight team members, using the **Meeting Process**	PMRF (Testing) E-mails	PL

Standard Process – Textual Novice View

Step	Action	Artifact	Responsible
Finalize Work Products			
24	Execute **Peer Review Process** to verify work products created/updated for consistency, accuracy, completeness and adherence to standards	Test Package, Documentation Package, Work Products	PL
25	Update the PMF in order to auto-populate the peer review and testing data	PMF	PL
26	If testing phase is identified as a critical milestone, execute the Testing Milestone Review using the MRF	MRF	PL
Submit for Compliance and Control			
27	Review validation results and correct items listed as non-compliant	PTF (Testing)	PL
28	Complete Project checklist and submit any project work products updated since the last compliance review and not contained in PDB to the QA Manager for the testing lifecycle review	Project Checklist (Testing) Test Package E-mail	PL
Record Improvement Data			
29	Record Testing as well as Compliance and Control Process lessons learned by selecting the Organizational, Section or applicable project based on the lesson learned	LLF	PL, Tester, Verifier
30	Verify/record actual hours in SERTS under the Integration, System and Acceptance Test lifecycle activity, as applicable and record the phase completion date in the PTF	SERTS PTF (Breakdown)	PL, Tester, Verifier

Problem

- **Building complex systems in an environment where we are experiencing increased vulnerabilities to attack given the explosion of information accessibility and connectivity**

- **Vulnerabilities being discovered at a rate faster than we can test**
  - **Systems may be required to adhere to multiple versions of the Security Technical Implementation Guide (STIG) and the Application Security and Development Checklist in a single release**

DISTRIBUTION A. Approved for public release; distribution unlimited.

Problem – Certification & Accreditation

C&A Renewal of Authority To Operate (ATO) due March 2012

- **Initial: Feb 2010 established estimated effort 300 hours and estimated completion date (ECD) Oct 2010**
- **Change #1: Jul 2010 increased estimated effort to 660 hours and extended ECD to Feb 2011**
- **Change #2: Mar 2011 increased estimated effort to 900 hours and extended ECD to Nov 2011**
- **Change #3: Jan 2012 increased estimated effort to 1200 hours and extended ECD to Mar 2012**

DISTRIBUTION A. Approved for public release; distribution unlimited.

Problem – Approach

- **Reviewed STIG and Application Security and Development Checklist**
- **157 items identified in checklist, review showed**
  - **53 items were not applicable (no classified data, non-CAC authentication, etc.)**
  - **94 items already compliant due to existing engineering practices**
  - **10 items that showed non compliance (7 CAT II and 3 CAT III)**

Attended lots of meetings to identify security expertise with respect to software security – trend has been to focus on network/system security

Software is significantly more challenging

Problem – Approach

- **Moderate priority to monitoring Not Applicable items**
  - **Updated coding standard to add considerations section to address items possibly applicable in future applications**

As much as possible, applicable items from the DISA Application Security and Development Checklist have a corresponding item in these standards so that compliance with these standards helps ensure compliance with the DISA checklist. However, certain technologies and techniques covered by the DISA checklist are not used within this office and do not have corresponding standards items. If any of these technologies or techniques are used during the course of an assignment, the PL must be careful to ensure that their application is compliant with the DISA checklist and that this document gets updated with the appropriate items. As of this writing, the following are not covered by this document:

- Accessing a Universal Description, Discovery, and Integration (UDDI) repository
- Applications that store classified or privacy act information
- Authentication through means other than Common Access Card (CAC)
- Externally accessible applications or web sites
- Passing commands to an operating system command shell
- Mobile code, defined by the DISA checklist as "software obtained from remote systems, transferred across a network, and then downloaded and executed on a local system without explicit installation or execution by the recipient."
- Use of non-standard ports/protocols (e.g. HTTP on port 80 or HTTPS on port 443)
- Use of third-party libraries without access to the source code or some form of warranty
- Web Services

Problem – Approach

- **Routine priority to monitoring compliant items**
  - **Added STIG mapping identifiers to coding standards**
- **High priority to correcting non-compliant items**
  - **Initiated change request to correct process assets based on non-compliance issues**
  - **Assigned tasks to correct deficiencies**

DISTRIBUTION A. Approved for public release; distribution unlimited.

Problem – Solution

- **Establish a centralized knowledge base that continuously assesses the changes and provides feedback to the projects on critical areas that must be addressed**

- **Integrate security into the system during the development cycle to improve the capacity to address the continuous vulnerability threats**

DISTRIBUTION A. Approved for public release; distribution unlimited.

Tailored Process – Initiation

- **Establish security requirements at project startup**

Step	Action	Artifact	Responsible
5	Record the Project Details	PTF (Initiation)	FLS

Extracted from
Project Tracking Form (PTF)

Security:

This project is an Unclassified Project and is part of the Organization Software Process Environment Certification and Accreditation package. Software security is critical to the overall success of any project. It is better to be proactive and build security into a program upfront instead of being reactive and constantly fixing bugs after the software has been deployed. Therefore, in order to reduce/eliminate the number of software vulnerabilities, the current Defense Information Systems Agency (DISA) Application Security and Development Security Technical Implementation Guide (STIG) will be used as a guideline. The Application STIG is located on the IASE website.

Tailored Process – Requirements

- **Based on First Level Supervisor guidance defined in the PTF, each Project Leader must ensure security requirements are understood and clearly documented**

Step	Action	Artifact	Responsible
5	Review Project Details to identify project specific requirements noted by the FLS	PTF (Initiation)	PL

Depending on severity and probability of the vulnerability/threat, security requirements may be documented in the Standard Requirements Specification Form (SRSF) or the security requirement may be addressed by updating project assets such as checklists, test cases, and/or procedures.

Tailored Process – Requirements

- **If the security requirement is addressed using an SRSF, the following information is documented**

Requirement Information			
Identifier:	**1.0 [Enter Requirement Name]**	**Type:**	
Priority			
Description:			
Scenarios:			
Inputs:			
Processing:			
Outputs:			
Design:			
Implementation:			

Requirement Testing						
SERF/Tracking #	**Test Type**	**V&V Method**	**Test Plan Name/Section**	**Test Case(s)**	**Date Tested**	**Test Status**

Requirement Tracking					
SERF/Tracking #	**Req Status**	**Status Date**	**Req Description Change**	**Revision Description**	**Production Date**

Tailored Process – Requirements

- **Project Leaders must also understand vulnerability management defined in the Organization's Configuration Management Form (CMF)**

Step	Action	Artifact	Responsible
22	Review the Section CMF to verify the project is following the Section configuration management procedures for naming conventions, storage policies, and required data management items	SKP (Section CM)	PL

Tailored Process – Requirements

- **Organization CMF addresses**

Vulnerability Management:	Strong configuration management is a foundation requirement for successful vulnerability management, and the two functions shall be highly coordinated. As potential threats and vulnerabilities are identified, they must be prioritized, tracked and mitigated. The organization shall track compliance with DoD directives and taskings to mitigate vulnerabilities or respond to threats in a coordinated manner. Additionally, The organization shall provide the capability to systematically identify and assess vulnerabilities and to direct and track coordinated mitigations. To the extent that system capabilities permit, mitigations shall be independently validated. Compliance with DoD-directed solutions, such Information Assurance Vulnerability Alerts (IAVAs), and Information Operation Conditions (INFOCONs) shall be a management review item. These items are reviewed and tracked via the Web Database TWG Meeting Minutes. Web-Database TWG status is reviewed monthly at Senior Management meetings and as driven by events at the Executive Steering Committee (ESC) meetings. Permissions for the SKP and SVN areas are managed by Architectural Engineering (AE). These permissions are checked by the steps defined in the AE AD Management Procedures contained within the Architectural Engineering CMF.

Tailored Process – Requirements

- **Organization CMF addresses**

Incident Response:	An incident response plan is documented in the Organizational Software Process Enterprise (OSPE) Contingency and Business Continuity Plan (CBCP) Artifact. The CBCP identifies the incident responders in accordance with DoD Instruction O-8530.2 and CJCS Instruction 6510.01D, defines reportable incidents, outlines a standard operating procedure for incident response to include INFOCON, provides for user training, and establishes an incident response team. The plan is exercised at least annually during HURCON Exercises and Unit Contingency Inspections (UCIs). Users are trained in incident recognition and initial notification through annual Information Protection Training. The Organizational Training Manager tracks all organization personnel having been trained and manages annual refresher training in January of every year.
Mobile Code:	Mobile Code as defined by DoDI 8552.01 is not allowed in deployed software. Mobile Code is defined as *software modules obtained from remote systems, transferred across a network, and then downloaded and executed on a local system WITHOUT explicit installation or execution by the recipient.*

Tailored Process – Requirements

Organization CMF addresses

Ports, Protocols and Services:	Only required ports, protocols and services are activated. Servers are protected by an I-NOSC controlled firewall to provide boundary defense mechanisms and ensure adherence to DoD Ports and Protocols guidance. The Defense Information System Agency (DISA) standards are applied to setup the Windows Server operating system and Internet Information Services in accordance with the applicable consensus DISA standard. The standards are developed with Information Technology (IT) security as well as operational impact in mind. Operational impact includes required security settings, which will disable or cause loss of functionality of the information system or application. Operational impact cannot override security; the operational impact must be weighed against the risk of not implementing a security control. The standard is the establishment of a minimum-security baseline applied to DoD systems. The standard provides a high level of assurance that the functionality of the information system or application will not be adversely impacted as a result of implementing standard settings. The standard also provides the capability for the detection, remediation and reporting of vulnerabilities on Windows-based systems and applications. All servers are scanned periodically and the ports, protocols and services are required to stay in compliance with DoD standards. • All Web Servers shall comply with DoD ports, protocols, and services guidance. Guidance is found in DoDI 8551.1, Ports, Protocols, and Services Management (PPSM), 13 August 2004 - http://iase.disa.mil/ports/index.html. • A port, protocol, or service that does not explicitly support a business function shall be disabled or removed. • A list of ports, protocols, and services shall be documented and regularly updated and maintained through the Web-Database TWG/AE CCB. • Project Leaders shall identify the network ports, protocols, and services they plan to use within software applications, outsourced IT-based processes and platform IT as early in the life cycle as possible and notify the Web-Database TWG. • Organization shall monitor emerging threats and vulnerabilities to the ports, protocols, and services they use.

Tailored Process – Requirements

- **Peer Reviews are a critical asset used to review requirements to ensure the system functions properly and meets the needs of the user**

Step	Action	Artifact	Responsible
40	Execute **Peer Review Process** to verify work products created/updated for consistency, accuracy, completeness and adherence to standards	Requirements Package, PTO Package, Work Products	PL

Established a database tool to support centralized data collection and automation of data analysis associated with testing defects identified. We categorize defects to be able to identify, predict and improve trends. Security would be a category for the defect save.

Tailored Process – Requirements

- **Defect Save Forms (DSFs) capture general defect**

Defect Save Form
General Information
Project Name: Data Processing Application
Title: Requirements Review
Phase: Requirements
Compliance Status: Compliant

Tracking Number: PS-2011-00365
Process Type: Peer Review
Completion Date: 12/16/2011
ID: 1

Participants

Name	Role	Effort (hrs)	Date
John Smith	Implementor	12.00	12/16/2011
Jane Doe	Reviewer	8.50	11/17/2011
Jim Bob	Recorder	1.00	12/16/2011
Jane Doe	Verifier	3.25	12/14/2011
Jim Bob	Moderator	0.50	12/14/2011

Products

Name	Version	Size	Unit Name
Data Processing SRSF	6.8	55	Pages

Tailored Process – Requirements

- **DSF captures data specific to each defect**

Defect Saves/Issues Log
Indicator: Defect Save
Severity: Minor

ID: 1
Injection: Requirements
Type: Security

Location:
Requirement 1.6 in Data Processing Application Standard Requirements Specification Form

Description:
Requirement states application must be compatible with all major browsers; however all browsers do not support CAC authentication, which is a security requirement.

Causal Analysis:
N/A

Tailored Process – Requirements Phase Checklist

Project Checklist - Requirements Phase					
ID	**Level**	**Artifact**	**Question**	**Response**	**Comments**
Requirements					
1	Standards	Req Pkg	Are the external and internal interfaces (how the software/system interacts with people, system hardware, other hardware or other software defined?		
2	Standards	Req Pkg	Is the performance defined by speed, availability, response time, recovery time, etc.?		
3	Standards	Req Pkg	Are operational scenarios defined?		
4	Standards	Req Pkg	Is a description of how the system is intended to be used in the operational environment defined?		
5	Organization	PTF, PMRF	Have previous requirements lessons learned been reviewed?		
6	Organization	Req Pkg	Are the attributes defined in terms of portability, correctness, maintainability, security, etc.?		
7	Organization	Req Pkg	Are the design constraints imposed on implementation defined such as standards for programming languages, policies for database integrity, resource limits, operating environment, etc.?		

Tailored Process – Requirements Peer Review Helper Checklist

General	
1.	Is the item consistent with its associated requirements and design documentation? This includes checking for missing, incorrect, or additional functionality.
2.	Are terms used within the application and its interface consistent with other artifacts and applications that refer to the same item (i.e. is the field called the same thing on the entry form, the report, the documentation, the OSP, etc.)?
3.	Are data value restrictions consistent across application levels (e.g. form, data access class, DB)?
4.	Do all files contain appropriate headers including modification comments?
5.	Has all dead/debug code been removed (excluding debug items that are conditionally compiled)? [APP3050]
6.	Are all exceptions, error conditions, and warnings recorded (e.g. log file, email to support team) with appropriate level of detail?
7.	Is any functionality that could be re-used in other development efforts adequately modularized and generic (i.e. can be re-used without copy/paste)?
8.	Does the code use existing APIs where possible instead of re-inventing the wheel?
9.	Are all unmanaged resources (e.g. database connections, file handles) correctly released?
10.	Is the database correctly normalized (at least 3rd normal form)?
11.	Is terminology used in a manner consistent with related applications and documentation?
12.	Are global variables only used when other means of storing the information (e.g. local variable, parameter) would not work? [APP3630]
13.	If using any of the techniques/technologies listed in section 1.8, were the applicable DISA checklist items verified and have the appropriate updates to this document been made/requested?

This checklist is used for peer reviews in all phases

Tailored Process – Requirements Traceability

- **Traceability provides the mechanism to track requirements through design, implementation and testing**
  - **Requirements – Acceptance Testing pass/fail criteria**
  - **Design – System Testing functional criteria**
  - **Implementation – Integration Testing interface criteria**
  - **Test – Regression Testing verification**

DISTRIBUTION A. Approved for public release; distribution unlimited.

Tailored Process – Design

- **Project Management technique of roll wave planning is used to plan the detailed execution of implementation activities**

13	Update the Requirements Package (specifically the SRS/RTM, SRSF or an Approved Section Product), PTO Package, Design Package, Documentation Package and Test Package (specifically the STP or an Approved Section Product) based on the Design Package and verify the packages are accurately cross-referenced	SRS/RTM or SRSF, SDD, STP, Documentation, PTO Package, Approved Section Product *PTF (Tailoring)*	PL

We would ensure the requirements, code, testing and user documentation is updated for consistency and assess the security risk associated with the changes

Tailored Process – Design

- **Peer Reviews are a critical asset used to review design to ensure the system functions properly and meets the needs of the user**

16	Execute **Peer Review Process** to verify Work Products created/updated since the last peer review for consistency, accuracy, completeness and adherence to standards	Design Package, Work Products	PL

Tailored Process – Design Phase Checklist

Project Checklist - Design Phase					
ID	**Level**	**Artifact**	**Question**	**Response**	**Comments**
1	Standards	Design Pkg	Does the design artifact document possible solutions considered?		
2	Standards	Design Pkg	If more than one solution considered, are criteria documented for the solution chosen (e.g., cost, performance, complexity, risk, operational use, maintainability, environmental constraints, future enhancements, technology limitations)?		
3	Standards	Design Pkg	Does the design artifact clearly document products/components to be developed?		
4	Standards	Design Pkg	Does the design artifact clearly document the criteria to use when evaluating the design (e.g., modularity, simplicity, maintainability, verifiability, portability, reliability, testability, security, scalability, usability, and clarity)?		
5	Standards	Design Pkg	Does the design artifact document interfaces between the products/components, with external systems/applications and between the product/component and lifecycle processes?		

Tailored Process – Implementation

- **Integration sequence defines the order components are compiled to build the application/system**

10	Document the integration sequence of the product components in the CI Package	CI Package	PL

Security must be considered when establishing the integration sequence to ensure vulnerabilities are minimized, especially when connecting/testing with external systems. How isolated is the development system from the production system?

Tailored Process – Implementation

- **Roll wave planning is used to plan the detailed execution of testing activities**

11	Update the Requirements Package (specifically the SRS/RTM, SRSF or an Approved Section Product), PTO Package, Design Package (specifically the SDD or an Approved Section Product), Documentation Package and Test Package (specifically the STP or an Approved Section Product) based on the Technical Data Package and verify the packages are accurately cross-referenced	SRS/RTM or SRSF, SDD, STP, Documentation, PTO Package, Approved Section Product *PTF (Tailoring)*	PL

We would ensure the requirements, code, testing and user documentation is updated for consistency and assess the security risk associated with the changes

Tailored Process – Implementation

- **Peer Reviews are a critical asset used to review source code to ensure the system functions properly and meets the needs of the user**

14	Execute **Peer Review Process** to verify Work Products created/updated for consistency, accuracy, completeness and adherence to standards	Technical Data Package, Work Products	PL

We would ensure the code reviews assess the security risk associated with the implemented solution

Tailored Process – Implementation Phase Checklist

Project Checklist - Implementation Phase					
ID	**Level**	**Artifact**	**Question**	**Response**	**Comments**
1	Standards	Technical Data Pkg	Does the Technical Data Package adhere to defined Section coding or system configuration standards?		
2	Organization	Technical Data Pkg	Were the artifacts required by the OSP Implementation Process produced?		
3	Organization	Technical Data Pkg	Do the artifacts in the defined Technical Data Package adhere to the approved templates?		
4	Organization	Technical Data Pkg	Are the documented requirements, design and implementation components cross-referenced to provide bi-directional traceability?		
5	Organization	Technical Data Pkg	Are the documented integration test for each defined interface, the Test Package and the Requirement Package components cross-referenced to provide bi-directional traceability?		
6	Standards	Technical Data Pkg	Is the integration sequence for the implemented components documented?		
7	Organization	Technical Data Pkg, PMRF	Are unit testing activities documented?		
8	Organization	DSF	Has the Moderator verified reviewer consensus was reached on the validity, severity and source of each defect save/issue?		
9	Organization	DSF	Is the effort for the review team recorded correctly?		
10	Organization	DSF	Were reviewers independent of management and implementation tasks?		
11	Organization	DSF	Were standards/references used?		
12	Organization	PSF, MRF	If this phase was identified as a critical milestone, have the appropriate milestone review activities been performed and recorded?		

Tailored Process – Testing Levels

- **Integration Testing**
  - **Focuses on debugging component interfaces and systematically testing the software**
- **System Testing**
  - **Focuses on verifying "the product is built right" by evaluating functionality**
- **Acceptance Testing**
  - **Focuses on validating "the right product is built" by evaluating the system's intended use in its intended environment**
- **Regression Testing**
  - **Focuses on testing components to verify the functionality was not affected by the modifications**

DISTRIBUTION A. Approved for public release; distribution unlimited.

Tailored Process – Testing

- **Levels of testing required to verify functional and validate operational use must be defined**

10	Execute verification and validation activities as defined by the test cases in the Test Package using Approved Section-specific checklists, templates and standards stored on the SKP (note: if a specified level of testing is not performed an explanation is required in the PTF)	*SKP (Section Checklists)* *SKP (Section Templates)* *SKP (Section Policies, Procedures and Standards)* *PTF (Tailoring)*	Tester

Security must be considered when defining the levels of testing and specifically what system components are required and what security issues must be addressed to minimize vulnerabilities that could be introduced during the test phase.

Tailored Process – Testing

- **Results of testing must be documented, analyzed against the integration sequence and verified to ensure pass/fail criteria was met**

11	Analyze the verification and validation results to confirm the components were assembled according to the defined integration sequence, to verify/validate interfaces performed correctly, and to determine if the test case passed or failed based on defined criteria	Test Package *DSF*	Tester

If security testing defect saves are identified, the appropriate security representatives must be involved in the corrective action to ensure it meets the intent of the Security Technical Implementation Guide (STIG) and the Application Security and Development Checklist

Tailored Process – Testing

- **Roll wave planning is used to plan the detailed execution of testing activities**

21	Update the Requirements Package, PTO Package, Design Package, Technical Data Package, and Documentation Package based on the Test Package and verify the packages are accurately cross-referenced	SRS/RTM or SRSF, SDD, Technical Data Package, STP, Documentation, PTO Package, Approved Section Product *PTF (Tailoring)*	PL

We would ensure the requirements, code, testing and user documentation is updated for consistency and assess the security risk associated with the changes

Tailored Process – Testing

- **Peer Reviews are a critical asset used to review test documentation to ensure the system functions properly and meets the needs of the user**

24	Execute **Peer Review Process** to verify work products created/updated for consistency, accuracy, completeness and adherence to standards	Test Package, Documentation Package, Work Products	PL

Based on peer review results, re-analyze the requirements, code, testing and user documentation to determine what additional rework must be performed.

Tailored Process – Testing Phase Checklist

Project Checklist - Testing Phase									
				Integration Test		System Test		Acceptance Test	
ID	Level	Artifact	Question	Response	Comments	Response	Comments	Response	Comments
1	Standards	Test Pkg	Does the test artifact document the testing environment?						
2	Organization	Test Pkg	Were the artifacts required by the OSP Testing Process produced?						
3	Organization	Test Pkg	Do the artifacts in the defined Test Package adhere to the approved templates?						
4	Organization	Test Pkg	Are the documented requirements, design, implementation and testing components cross-referenced to provide bi-directional traceability?						
5	Organization	DSF	Has the Moderator verified reviewer consensus was reached on the validity, severity and source of each defect save/issue?						
6	Organization	DSF	Is the effort for the review team recorded correctly?						
7	Organization	DSF	Were reviewers independent of management and implementation tasks?						
8	Organization	DSF	Were standards/references used?						
9	Organization	Test Pkg	Are the documented test for each documented requirement defined?						
10	Organization	Test Pkg	Does the Test Package indicate that testing has been performed?						
11	Organization	PSF, MRF	If this phase was identified as a critical milestone, have the appropriate milestone review activities been performed and recorded?						

Tailored Process – Completion

- **Involve Security representatives as part of project closeout meeting to review defect saves and corrective actions assigned based on security**

13	Verify review results, analysis data, Section Security Representative approval of classified document markings, and proposed actions for future project improvements are recorded in the MRF along with the FLS approval date	PMF MRF	PL

Tailored Process – Completion Phase Checklist

Project Checklist - Completion Phase					
ID	**Level**	**Artifact**	**Question**	**Response**	**Comments**
1	Organization	Documentation Pkg	Does the documentation artifact describe the system in terms of installation, user guide, programmer's guide, etc?		
2	Organization	CI Pkg	Were the artifacts required by the OSP produced?		
3	Organization	CI Pkg	Do the artifacts in the defined CI Package adhere to the approved templates?		
4	Organization	CI Pkg	Are the documented requirements, design, implementation and testing components cross-referenced to provide bi-directional traceability?		
5	Organization	CI Pkg, PMF	Was the close out analysis conducted with the FLS and PL to review the accuracy of all documented project data, to verify all risk, open issues, action items and waivers are closed and to analyze project performance?		
6	Organization	MRF	Does the MRF analysis comments indicate the project performance has been reviewed using the MIG to address trends in requirement volatility, schedule (est vs act), effort (est vs act), productivity (est vs act), defect save containment, and quality goal achievement (goal vs act)?		
7	Organization	MRF	Were process improvements documented based on PMF trends to aide in the success of future projects?		
8	Organization	MRF, PMF	Have the required milestone review activities been performed/recorded?		
9	Organization	PSF	Are the start and completion fields completed correctly?		
10	Organization	PSF, SERTS	Do the effort/schedule estimates in the PSF match SERTS?		
11	Organization	SERTS	Is the SERF analysis complete?		
12	Organization	SERF, LLF, CR	Has corrective action been taken based on causal analysis and project trends identified to prevent future defects?		
13	Organization	Project Artifacts	Have best practices been submitted to the SECG?		

Tailored Process – Improvement Models

- **Capability Maturity Model Integration (CMMI) – technique to establish and instantiate proven software and systems engineering practices**
- **Air Force Smart Operations for the 21st Century (AFSO21) – technique to identify/remove waste as processes are streamlined**
- **Project Management Body of Knowledge (PMBOK) – technique to identify/track test management and execution activities such as roll wave planning and closeout reviews**

Analysis – Data Collection

- **Minimize redundancy**
- **Minimize quantity**
- **Evaluate accuracy**
- **Evaluate consistency**
- **Automate whenever possible**
- **Avoid using single data points to make critical change or performance decisions**

Analysis – Test Metrics

Baseline	% Post Release Defects
5.0 Baseline	23%
6.0 Baseline	14%
7.0 Baseline	9%

14% decrease in post release defects!

How much does a post release defect cost the organization?

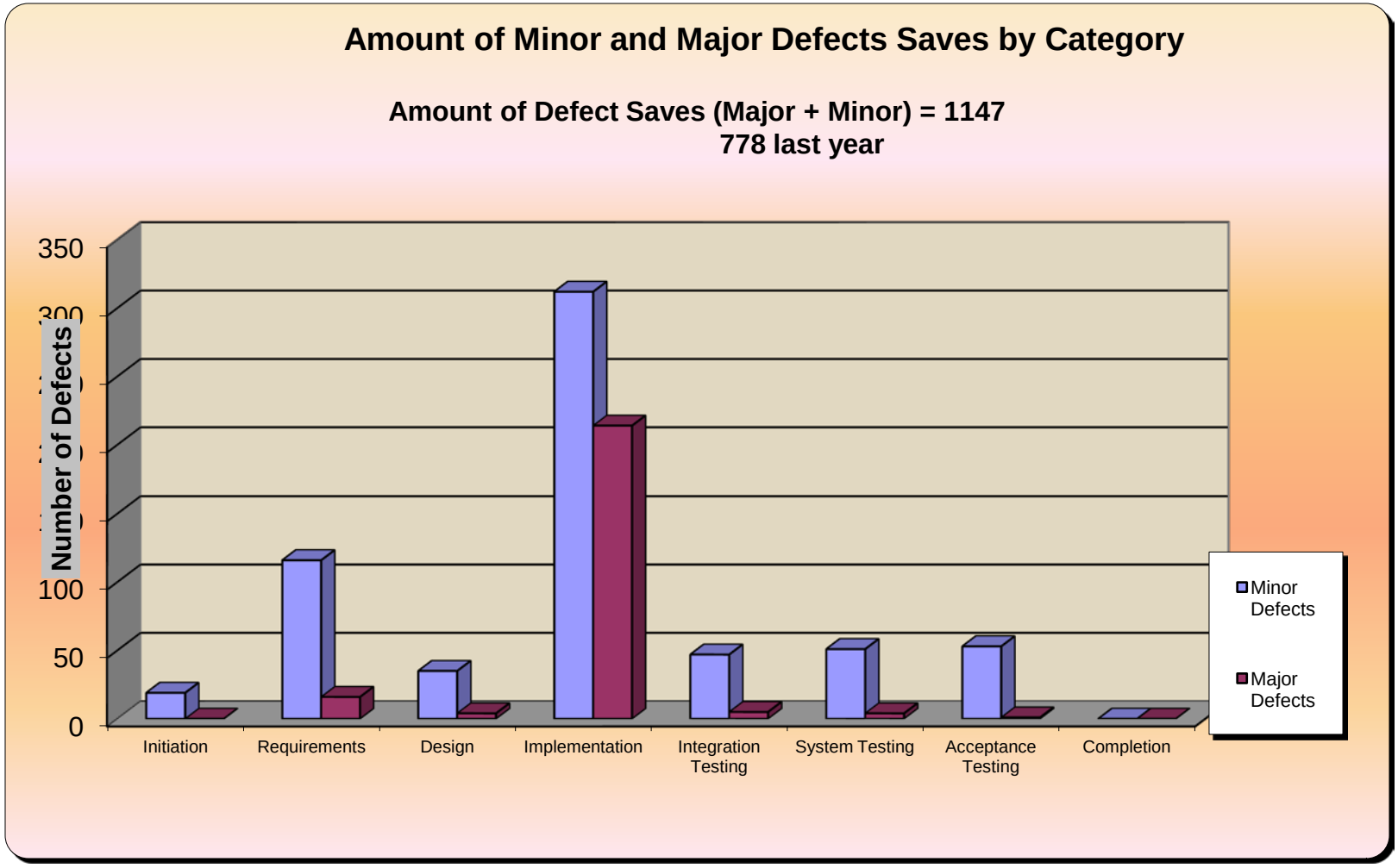
6.0 Baseline Data: What was the cost?

- 232 corrective changes identified out of 1606 data points (17% contained no data)
- 95 data points with corrective changes only - expended 3780 hours

# Defects	Method	Hours Req'd	Cost @ $45	Cost Ratio
95	Post Release	3780	$170,100	1:16
95	Testing	(95/.18) = 528	$23,760	1:2
95	Peer Review	(95/.40) = 238	$10,710	1:1

DISTRIBUTION A. Approved for public release; distribution unlimited.

Analysis – Test Metrics



Analysis – Test Metrics

Major Defect Save Containment Matrix

Injected → / Detected ↓	Init	Req't	Project Plan	Design	Imp	Int Test	Sys Test	Acc Test	Delivery	Completion
Initiation	0									
Req't	0	9								
Project Plan	0	0	0							
Design	0	2	0	3						
Imp	0	4	0	1	29					
Int Test	0	0	0	0	11	5				
Sys Test	0	1	0	0	3	0	4			
Acc Test	0	0	0	0	2	0	0	1		
Completion	0	0	0	0	0	0	0	0		

Good Containment

Checklists have been updated to address/catch these issues in the future

Analysis – Statistical Control

- **Reducing process variation is the key to improving productivity and quality**
- **Six Sigma principles used to analyze stability and capability of our performance baselines using DMAIC Approach**
  - **Define focus on "*What is important*"**
  - **Measure focus on "*How we are doing*"**
  - **Analyze focus on "*What is wrong*"**
  - **Improve focus on "*What needs to be done*"**
  - **Control focus on "*How do we guarantee performance*"**

Improvements – Lessons Learned/Best Practices

- Lessons Learned
  - Identify pass/fail criteria for security requirements early in the lifecycle
  - Identify trusted components in the test environment to understand where security risks exist
  - Test cases must be cost effective and maintainable
  - Identify and track security stakeholder involvement throughout the lifecycle
- Best Practices
  - Automated tools improve effectiveness of testing

Real World Example

Build Security into Software Development

Example #1. STIG – ID 3550

Group Title: APP3550

Rule ID: SV-17808r2_rule

Severity: CAT I

Rule Version (STIG-ID): APP3550

Rule Title: The designer will ensure the application is not vulnerable to integer arithmetic issues.

Vulnerability Discussion: Integer overflows occur when an integer has not been properly checked and is used in memory allocation, copying, and concatenation. Also, when incrementing integers past their maximum possible value, it could potentially become a very small or negative number. Integer overflows can lead to infinite looping when loop index variables are compromised and cause a denial of service. If the integer is used in data references, the data can become corrupt. Also, using the integer in memory allocation can cause buffer overflows, and a denial of service. Integers used in access control mechanisms can potentially trigger buffer overflows, which can be used to execute arbitrary code.

STIG – ID 3550 Solution

Improvement: Updated coding standards to add the following standard:

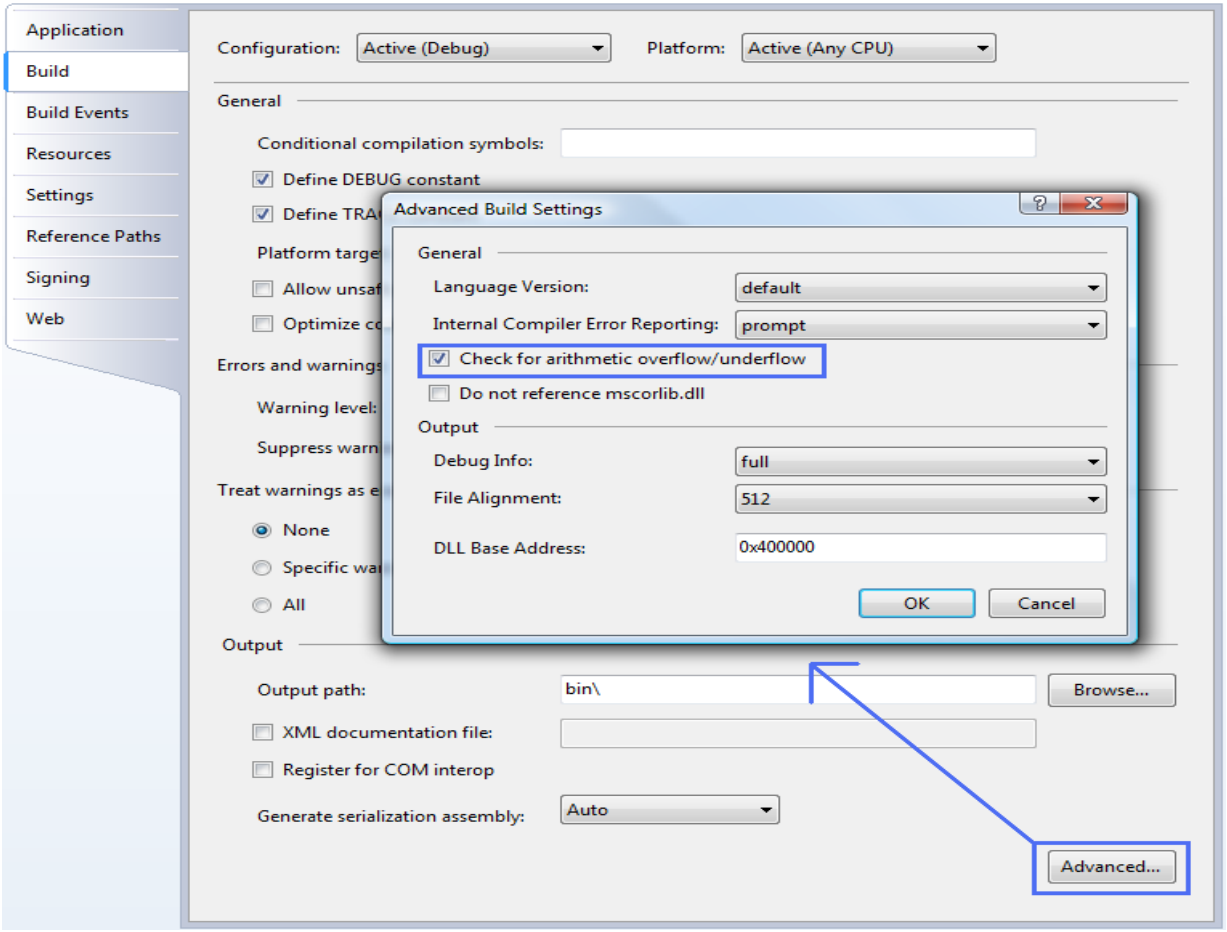
1. Always explicitly wrap overflow- or underflow-prone operations in `checked` or `unchecked` blocks, depending on the expected behavior. See section 2.6 for guidance on `checked` compilation. [APP3550]

```
public int CalcPower(int number, int power)
{
        int result = 1;
        for(int count = 1; count <= power; count++)
        {
                checked
                {
                        result *= number;
                }
        }
        return result;
}

public override int GetHashCode()
{
        unchecked
        {
                // hash calculations go here
        }
}
```

STIG – ID 3550 Solution

2. Always set Debug builds to 'Check for arithmetic overflow/underflow'. Never set this option for Release builds (for performance reasons). [APP3550]



Example #2. STIG – ID 3580

Group ID (Vulid): V-16811

Group Title: APP3580

Rule ID: SV-17811r3_rule

Severity: CAT I

Rule Version (STIG-ID): APP3580

Rule Title: The designer will ensure the application does not have cross site scripting (XSS) vulnerabilities.

Vulnerability Discussion: XSS vulnerabilities exist when an attacker uses a trusted website to inject malicious scripts into applications with improperly validated input.

STIG – ID 3580 Solution

Improvement: Updated coding standards to add the following standard:

1. Always properly encode user entered data (`Server.HtmlEncode()`) before displaying it on the page. This applies to any data the user may potentially manipulate, including query string parameters. [APP3580]

2. Always set cookies to be HTTP-only unless the cookie is required to be accessed by JavaScript and the contents of the cookie have been thoroughly analyzed to ensure it does not contain sensitive or exploitable information (e.g. user information, session ID). [APP3580]

Improvement: Updated Peer Review Helper Checklist:

15	Is all user-entered data correctly encoded before being displayed to the screen (e.g. Server.HTMLEncode(userData))? This applies to any data the user may potentially manipulate, including query string parameters. [APP3580]

The Way Ahead

- **Centralize the Knowledge**
- **Acquire Automated Tools**
- **Define Training Requirements**
- **Assess Building Security in Maturity Model (BSIMM3)**

Centralize the Knowledge

- **Squadron Director formally chartered an organizational Technical Work Group (TWG) comprised of subject matter experts to address**
  - **Purpose**
  - **Scope**
  - **Mission**
  - **Responsibilities**
  - **Resources**
  - **Qualifications**
  - **Completion Criteria**

Centralize the Knowledge

- **TWG periodically performs gap analysis between STIG versions to identify organizational impacts**

This Application Security and Development Security Technical Implementation Guide (STIG) ***provides security guidance*** *for use* ***throughout*** *the application* ***development*** *lifecycle. This STIG provides the guidance needed to promote the development, integration, and updating of secure applications. Subjects covered in this document are:* ***Development, design, testing, conversions and upgrades for existing applications, maintenance, software configuration management, education, and training****. Defense Information Systems Agency (DISA) encourages sites to* ***use these guidelines as early as possible*** *in the application development process. Some vulnerabilities may require significant application changes to correct. The earlier the STIG requirements are integrated into the development lifecycle, the less disruptive the remediation process will be. [STIG version 3, release 1, page 11 of 125]*

Centralize the Knowledge

- **TWG provides gap analysis to representative software development teams**
- **Software development team addresses testing for the security items and provides action plan back to the TWG**
- **TWG tracks and monitors testing status for C&A ATO renewals based on expiration dates of C&A packages**

Acquire Automated Tools

- **FxCop tool**
  - **Provides static code analysis tools within Visual Studio**
- **Fortify tool**
  - **Provides an automated way to analyze code for security vulnerabilities for static testing**

Define Training Requirements

- **Identify training required for SMEs participating in TWG**
- **Identify training required for Project Leaders and Team members to ensure proactive evaluation of security risks within applications**

Summary

- Defined processes enable security to be built into testing activities, resources and environment
- Past performance is our best measure of future success
- Successful testing environments require disciplined, data-driven assets
- Security will continue to be a challenge as new platforms, languages and devices evolve

We MUST take proactive measures to understand the changes and how they are impacting our systems!

Questions