

Risk-Based Assessment and Scoping of IV&V Work Related to Information Assurance

Presented by Joelle Spagnuolo-Loretta, Richard Brockway, John C. Burget
September 14, 2014



Agenda

- Information Assurance
- Confidentiality
- Integrity
- Availability
- Selecting Projects
- Determining criticality
- Impact
- Likelihood
- Summary
- Acknowledgements

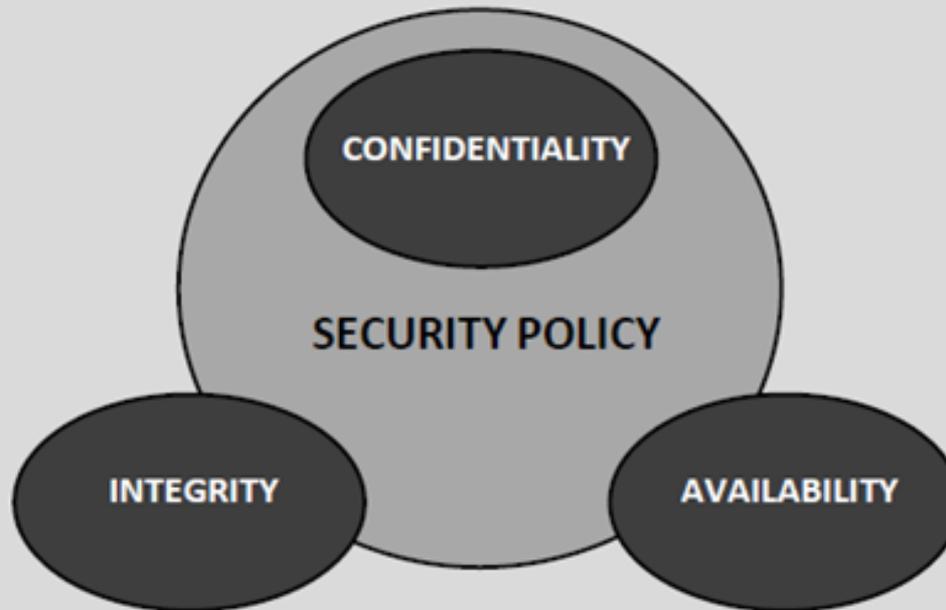


- Managing risk related to the systems that use, process, store, and transmit data
- NASA's focus
 - Protect data and systems from threats
 - Ensure continuity of operations
- What are some common threats?



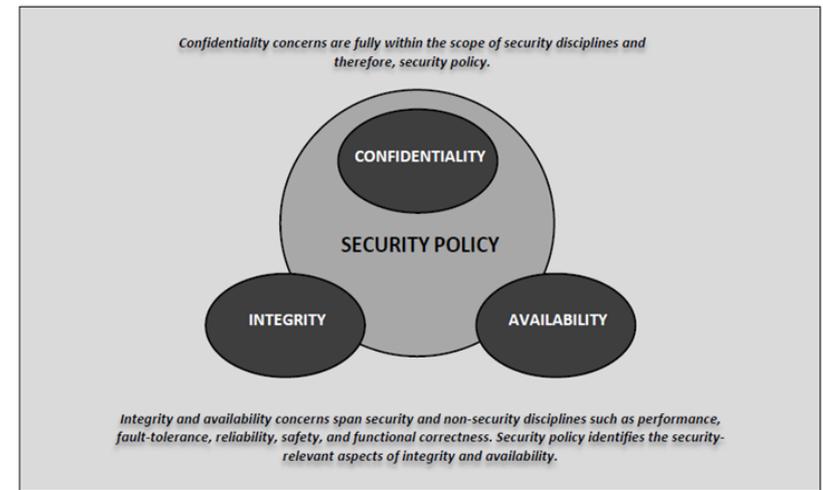
Internal	External
System Architecture	Natural Disasters
Developers	Espionage
Users	Hactivism

Confidentiality concerns are fully within the scope of security disciplines and therefore, security policy.



Integrity and availability concerns span security and non-security disciplines such as performance, fault-tolerance, reliability, safety, and functional correctness. Security policy identifies the security-relevant aspects of integrity and availability.

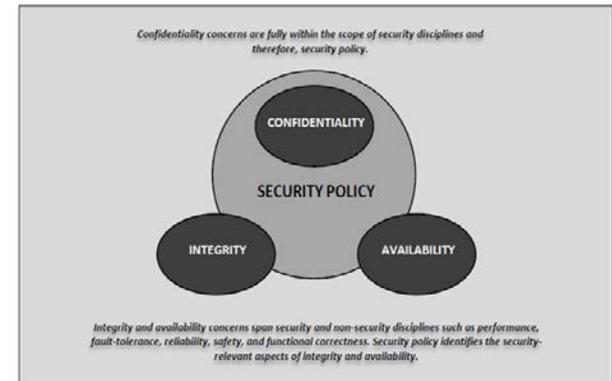
- Could the entity allow for the unauthorized disclosure of sensitive information to do harm to agency operations, agency assets, or individuals?
- Could the entity allow for the unauthorized disclosure of information to gain control of agency assets that might result in unauthorized modification of information, destruction of information, or denial of system services that would result in harm to agency operations, agency assets, or individuals?



- Could the entity allow for unauthorized modification or destruction of information to do harm to agency operations, agency assets, or individuals?

- Notes:

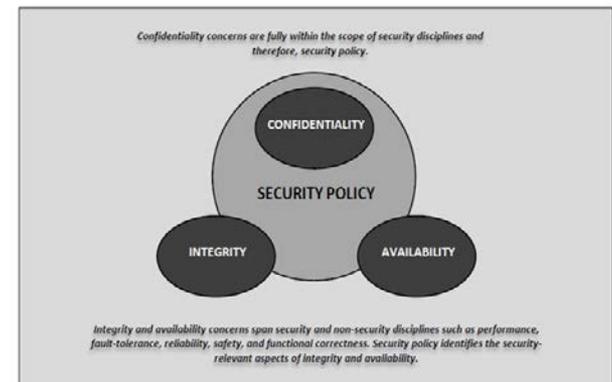
- *The most serious impacts of integrity compromise occur when some action is taken that is based on the modified information or the modified information is disseminated to other organizations or the public.*
- *Undetected loss of integrity can be catastrophic for many information types. The consequences of integrity compromise can be either direct (e.g., modification of a financial entry, medical alert, or criminal record) or indirect (e.g., facilitation of unauthorized access to sensitive or private information or deny access to information or information system services). Malicious use of write access to information and information systems can do enormous harm to an agency's mission and can be employed to use an agency system as a proxy for attacks on other systems.*
- *In many cases, the consequences of unauthorized modification or destruction of information to agency mission functions and public confidence in the agency can be expected to be limited. In other cases, integrity compromises can result in the endangerment of human life or other severe consequences. The impact can be particularly severe in the case of time-critical information.*



- Could the entity contribute to the withholding or disruption of access to or use of information or services to do harm to agency operations, agency assets, or individuals?

- Notes:

- *For many information types and information systems, the availability impact level depends on how long the information or system remains unavailable. Undetected loss of availability can be catastrophic for many information types. For example, permanent loss of budget execution, contingency planning, continuity of operations, service recovery, debt collection, taxation management, personnel management, payroll management, security management, inventory control, logistics management, or accounting information databases would be catastrophic for almost any agency. Complete reconstruction of such databases would be time consuming and expensive.*
- *In most cases, the adverse effects of a limited-duration availability compromise on an organization's mission functions and public confidence will be limited. In contrast, for time-critical information types, availability is less likely to be restored before serious harm is done to agency assets, operations, or personnel (or to public welfare). In such instances, the documented availability impact level recommendations should indicate the information is time-critical and the basis for criticality.*



Selecting Projects

- IV&V services are expanding to projects of varying domains (e.g. ground systems, integrated networks, etc.)
 - Somewhat different than the typical flight software projects supported in years past
 - Crucial that IV&V processes mature such that they maintain applicability
- What kind of projects need Information Assurance?
 - Those that store, use, process, or rely upon data
 - What projects don't do that??
 - What risks exist to projects that provide for Information Assurance?
 - Confidentiality
 - Integrity
 - Availability



- To determine criticality, the IV&V Program uses:
 - Portfolio Based Risk Assessments (PBRA)
 - Risk Based Assessments (RBA)
 - “is used to create a mission-specific view to support planning and scoping of NASA IV&V Project work on each individual IV&V Project”.
 - Results in a risk score for each system/software entity for a particular mission based on
 - Impact categories of:
 - Performance
 - personnel safety
 - operational software control
 - Likelihood categories of
 - Complexity
 - Testability
 - Degree of innovation
 - Developer characteristics



Why Incorporate the IA Perspective?

- Criteria tailored to allow for a thorough assessment of the system entities and their potential risk as it relates to maintaining system security/information assurance.
- Some aspects of security (e.g. integrity and availability) could be assessed per the existing impact criteria for performance
- Separately rating the entities based on their overall contribution to the system security to include confidentiality, integrity, & availability forces the individual perspective



Impact Criteria

Impact	Very Low(1)	Low (2)	Moderate (3)	High (4)	Very High (5)
SEC - System Security / Information Assurance (CIA - Confidentiality, Integrity, and Availability)	No effect on Information Assurance	The loss of C or I or A could be expected to have a limited adverse effect on mission capabilities, organizational operations, organizational assets, or individuals	The loss of C or I or A could be expected to have a serious adverse effect on mission capabilities, organizational operations, organizational assets, or individuals	The loss of C or I or A could be expected to have a severe adverse effect on mission capabilities, organizational operations, organizational assets, or individuals	The loss of C or I or A could be expected to have a catastrophic adverse effect on mission capabilities, organizational operations, organizational assets, or individuals
Elaborated Criteria	Does not cause degradation of mission capability but may cause user inconvenience	<p>A limited adverse effect means that, for example, the loss of confidentiality, integrity, or availability might:</p> <ul style="list-style-type: none"> (i) cause a degradation in mission capability to an extent and duration that the organization or mission is able to perform its primary objectives, but the effectiveness of the functions is noticeably reduced; (ii) result in minor damage to organizational or mission assets; (iii) result in minor financial loss; or (iv) result in minor harm to individuals. <p>See FIPS-199 further amplification</p>	<p>A serious adverse effect means that, for example, the loss of confidentiality, integrity, or availability might:</p> <ul style="list-style-type: none"> (i) cause a significant degradation in mission capability to an extent and duration that the organization or mission is able to perform its primary objective(s), but the effectiveness is significantly reduced; (ii) result in significant damage to organizational or mission assets; (iii) result in significant financial loss (Ex: Loss of sensitive data (Intellectual Property), Incurred recovery costs after incident); or (iv) result in significant harm to individuals that does not involve loss of life or serious life threatening injuries (Should also be classified under Personnel Safety if the security of it can affect human life). <p>See FIPS-199 further amplification</p>	<p>A severe adverse effect means that, for example, the loss of confidentiality, integrity, or availability might:</p> <ul style="list-style-type: none"> (i) cause a severe degradation in mission capability to an extent and duration that the organization or mission is not able to perform one or more of its primary objectives; (Ex: Marginal loss of agency's reputation, Loss of multiple mission objectives) (ii) result in major damage to organizational or mission assets; (iii) result in severe harm to individuals involving loss of life or serious life threatening injuries (Should also be classified under Personnel Safety if the security of it can affect human life). <p>See FIPS-199 further amplification</p>	<p>A catastrophic adverse effect means that, for example, the loss of confidentiality, integrity, or availability might:</p> <ul style="list-style-type: none"> (i) cause a loss of mission capability to an extent and duration that the organization or mission is not able to perform its primary objectives; (Ex: Substantial loss of agency's reputation, Loss of asset, Loss of all primary objectives(s), Loss of sensitive data) (ii) result in major damage to organizational or mission assets; (iii) result in major financial loss (Ex: Loss of sensitive data (Intellectual Property), Incurred recovery costs after incident); or (iv) result in catastrophic harm to individuals involving loss of life or serious life threatening injuries (Should also be classified under Personnel Safety if the security of it can affect human life). <p>See FIPS-199 further amplification</p>

Scoring Impact

- **Impact = max (PS, SEC, average (P, OSC))**
 - PS = Personnel Safety
 - P = Performance
 - OSC = Operational Software Control
 - SEC = Security
-
- *When assessing impact referencing the FIPS categorization can aid in determining the potential impact that the loss of C, I, or A could be to a mission/organization.*
 - *If available the information type identified in the FIPS categorization can be linked to the PBRA capability / RBA entity which can support your assessment on what the impact would be (Low, Moderate, or High) if a loss of C, I, or A occurs.*



Likelihood Criteria

Likelihood	Very Low(1)	Low (2)	Moderate (3)	High (4)	Very High (5)
Security Posture	<p>The system has a mature security infrastructure with well documented controls which have been evaluated for completeness and accuracy.</p> <p>Or</p> <p>A security vulnerability cannot be exploited</p> <p>Or</p> <p>The system is not exposed and not a target for threats</p>	<p>The system has a well-defined security infrastructure and has a small number of accepted risks.</p> <p>Or</p> <p>A security vulnerability is unlikely to be exploited</p> <p>Or</p> <p>The system has limited exposure and is an unlikely target for threats</p>	<p>The system has a security plan, but it also has a large number of risks to be accepted.</p> <p>Or</p> <p>A security vulnerability is somewhat likely to be exploited</p> <p>Or</p> <p>The system is moderately exposed and a moderate target for threats</p>	<p>The system does not have a well-defined security infrastructure, but a system security plan has been drafted.</p> <p>Or</p> <p>A security vulnerability is likely to be exploited</p> <p>Or</p> <p>The system is somewhat visible, has some exposure, and is a potential target for threats</p>	<p>The system has no security infrastructure and has no system security plan.</p> <p>Or</p> <p>A security vulnerability is highly likely to be exploited</p> <p>Or</p> <p>The system is highly visible, exposed, and a prime target for threats</p>
Elaborated Criteria	<p>Infrastructure encompasses security requirements, architecture, concept of operations, etc.</p> <p>Likelihood from IA perspective can be thought of from two perspectives: The likelihood of occurrence which can be driven down by having a mature security infrastructure and implementing proper security controls. The second perspective is the likelihood of exploitation if the vulnerability exists. Both of these perspectives should be considered when determining the likelihood. For example, the likelihood of occurrence could be high but the likelihood of exploitation could be low due various factors.</p> <p>Some examples (but not limited to) that may contribute to likelihood for becoming a target for threats: importance of data (sensitive, classified, etc.), physical location, isolated network, and access to internet.</p> <p>Threats also include environmental / natural disasters, etc.</p>				



- **Likelihood = max (SP, average (Complexity, Testability, Degree of Innovation, Development Characteristics))**
- SP = Security Posture



Summary

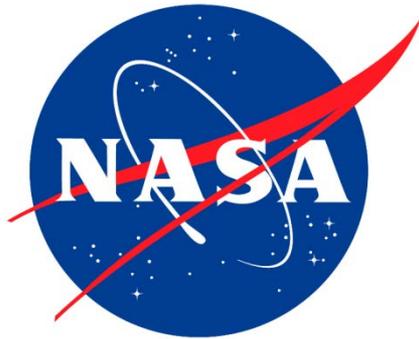
- Adding IA specific criteria forces the perspective for IV&V
- More rigor in defining criticality
- Supports FIPS & industry best practices



Acknowledgements

- **Brandon Bailey – Information Assurance Analysis Techniques CD lead**
- **Roger Harris – SGSS IV&V Project Manager**
- **SGSS IV&V Team**





TASC
INSIGHT APPLIED™