ISSEA Metrics

Goal	Type	Objective	Description	Purpose	Data Sources	Implementation Evidence	Formula	Frequency	Indicators
Administer Security Controls	Implementation / Activity	Establish responsibilities and accountability for security controls and communicate them to everyone in the organization.	%# of employees that have completed pre-employement security briefing	To identify the percent of employees who have attended the introductory security briefing which explains organizational security responsibility and accountability	All employees are required to complete a pre-employment security briefing. The employee file will be marked with the date of completion. HR is responsible for tracking this data for all employees	Reports will be generated by HR indicating percent compliance	% = (# of employees that have completed pre-employment security briefing) / (Total # of employees)	Monthly, Quarterly, or Annually	The target for this metric is 100%. All employees (even existing employees) are also required to attend this pre-employment security briefing.
Administer Security Controls	Implementation / Activity	Monitor the existance of systems within the network.	%# of systems that are located within the organization network	To identify and account for all systems connected to the organization network.	All systems connected to the network must be identified and registered.	Reports will be generated by IT indicating all systems connected to each subnet.	% = (# of legally registered systems in all subnets)/(Total # of systems identified in all subnets)	Monthy, Quarterly, or On Demand	The target for this metric is 100%. All systems connected to the network must be registered with the IT group.
Administer Security Controls	Results / Output	Manage the configuration of system security controls	%# of systems that are configured in accordance with baseline security best practices.	To identify the percentage of systems that are in compliance with best practices.	All systems are required to be configured in accordance with the baseline standards published by the security group. IT is responsible for tracking and insuring that all systems are configured in accordance with best practice.	Reports will be generated by IT indicating percent compliance	% = (# of systems that are configured in compliance best practices) / (Total # of systems)	Monthly, Quarterly, Annually, or On Demand	The target for this metric is 100%. All systems are required to be configured using best practices.
Administer Security Controls	Implementation / Activity	Manage security awareness training for all users	#/% of users that completed security awareness training	To identify the number of users who have completed a security awareness briefing.	All users are required by corporate security policy to complete annual security awareness training.	Reports will be generated by HR indicating percent compliance	% = (# of users that have completed security awareness training) / (Total # of users)	Monthly, Quarterly, or Annually	The target for this metric is 100%.
Administer Security Controls	Implementation / Activity	Manage security training and education programs for all users and administrators	#/% of users that completed security education and training	To identify the number of users who have met their training and education requirement	Each user may have different security training and education requirments based upon their job position. The security group will track these special training and education requirments.	Reports will be generated by Security indicating percent compliance	% = (# of users that have completed their required security education and training) / (Total # of users requiring special security education and training)	Monthly, Quarterly, or Annually	The target for this metric is 100%. Some users require training and education above and beyond that covered in the basic security awareness briefing.
Administer Security Controls	Results / Output	Manage security education for all users and administrators	%/# of confirmed to be qualified personnel	To identify the number of qualified personnel assigned to a job function	Security specific jobs will have their education requirements determined by the Security group. The Security group will track the qualifications of security personnel.	Reports will be generated by Security indicating percent compliance	% = (# of personnel who are currently qualified)(/# of qualified personnel required)	Monthly, Quarterly, or Annually	The target for the metric is 100%. Any score less than 100% requires a waiver issued by the CSO.
Administer Security Controls	Implementation / Activity	Manage periodic review of security services and control mechanisms	#/% of system log files reviewed for malicious or failure mode activity	To identify and measure the number of critical system log files that are periodically reviewed.	Both the IT and the Security groups are responsible for monitoring system log files for anomoly indications.	Reports will be generated by the IT and Security groups indicating percent reviewed	% = (# of critical log files reviewed daily)/(total # of critical log files identified)	Monthly, Quarterly, or Annually	The target for this metric is 100%.
Administer Security Controls	Results / Output	Manage periodic maintenance and administration of security services and control mechanisms	Average elapsed time between scheduled periodic maintenance and actual maintenance of security services and control mechanisms	To measure the time between the scheduled and actual maintanence of security services and control mechanisms	The Security team must report both the scheduled time and actual times for maintainence of security services and control mechnisms.	Reports will be generated by the Secuirty group indicating the average delay time.	AverageTimeDelay = (Sum of elapsed time between scheduled and actual periodic maintenance of security services and control mechanisms)/(Total # of Processes with data points in the reporting period)	Monthly, Quarterly, or Annually	The target for this metric is to continually reduce the elapsed time between periodic maintenance and administration of security services and control mechanisms.
Administer Security Controls	Results / Output	Manage periodic maintenance and administration of security services and control mechanisms	%/# of authorized changes	To identify the number of changes that have been authorized prior to change having been implemented	The Security team must authorize changes made to any of the security services and control mechinisms in accordance with the organizational policy.	Reports will be generated by the Security group indicating percent complaince.	% = (# of authorized changes)/(# of registered changes identified during periodic maintenance and administration of security services and control mechanisms)	Monthly, Quarterly, or Annually	The target for the metric is 100% authorization of all changes.
Assess Impact	Implementation / Activity	The purpose of Assess Impact is to identify impacts that are of concern with respect to the system and to assess the likelihood of the impacts occurring. Impacts may be tangible such as the loss of revenue or financial penalties, or intangible, such as loss of reputation or goodwill.	Percent of capabilities identified and prioritized (Percentage of capabilities identified, analyzed, and prioritized that support the key operational, business, or mission capabilities leveraged by the system.)	To quantify compliance with impact assessment process	A business impact analysis must be conducted tha takes in account the high level business objectives of the organization. The business processes and supporting resources identified in the analysis will help enumerate the organziational capabilities that can be adversley impacted.	Documentation provided by the risk assessment team.	% = (Number of capabilities characterized)/(tota number of capabilities)	Depends on the SDL phase	Capability is prioritized. Target is 100%. Increasing results indicates positive results. Decreases in results will be caused by significant updates. Capability complexity influences trends fluctuations.
Assess Impact	Implementation / Activity	The purpose of Assess Impact is to identify impacts that are of concern with respect to the system and to assess the likelihood of the impacts occurring. Impacts may be tangible such as the loss of revenue or financial penalties, or intangible, such as loss of reputation or goodwill.	Percent of assets identified and characterized (Percentage of assets identified and characterized for the system assets that support the key operational capabilities or the security objectives of the system.)	To quantify compliance with impact assessment process	A business impact analysis must be conducted tha takes in account the high level business objectives of the organization. The business processes and supporting resources identified in the analysis will help enumerate the organziational capabilities that can be adversley impacted.	Documentation provided by the risk assessment team.	% = (Number of assets characterized)/(total number of assets)	Depends on the SDL phase	Capability is quantified. Target is 100%. Increasing results indicates positive results. Decreases in results will be caused by significant updates. Asset complexity influences trends fluctuations.

ISSEA Metrics

Goal	Type	Objective	Description	Purpose	Data Sources	Implementation Evidence	Formula	Frequency	Indicators
Assess Impact	Implementation / Activity	The purpose of Assess Impact is to identify impacts that are of concern with respect to the system and to assess the likelihood of the impacts occurring. Impacts may be tangible such as the loss of revenue or financial penalties, or intangible, such as loss of reputation or goodwill.	Security impact metric selection (Whether or not impact metrics have been selected for this assessment.)	To quantify compliance with impact assessment process	The security team will define impact metrics to track the progress of the organizational security capability.	Specific, unambiguous impact metrics are defined and collected on a periodic basis.	Have impact metrics been selected? (Yes/No, i.e., a binary indicator)	Depends on the assurance need and complexity of the environment	Selection of impact metrics. Target = Yes. Selection of specific impact metrics indicates positive results. Ambiguity in metric formulation will cause delays in conducting an impact assessment and may be the result of significant and frequent system updates.
Assess Impact	Implementation / Activity	The purpose of Assess Impact is to identify impacts that are of concern with respect to the system and to assess the likelihood of the impacts occurring. Impacts may be tangible such as the loss of revenue or financial penalties, or intangible, such as loss of reputation or goodwill.	Security impact metric relationship identification (Whether or not the relationships between the selected metrics for this assessment, and metric conversion factors if required, have been identified.)	To quantify compliance with impact assessment process	The security team will define the functions necessary to combine multiple metrics into the desired composite metrics.	Specific, unambiguous composite metric functions are defined and calculated on a periodic basis.	Have impact metrics relationships been defined? (Yes/No, i.e., a binary indicator)	Depends on the assurance need and complexity of the environment	Definition of impact metric relationships. Target = Yes. Definition of specific impact metric relationships indicates positive results. Lack of definitions of metric relationships causes delays in conducting an impact assessment.
Assess Impact	Implementation / Activity	The purpose of Assess Impact is to identify impacts that are of concern with respect to the system and to assess the likelihood of the impacts occurring. Impacts may be tangible such as the loss of revenue or financial penalties, or intangible, such as loss of reputation or goodwill.	Estimated number of impacts (per specified period). For example, the number of virus incidents per quarter in conjunction with the cost per virus incident might be one category specified.	To quantify accuracy of impact assessment	The security team will define the scorecard that combines the capabilities and resources at risk with the metrics identified to measure the impacts to define a comprehensive exposure impact list.	A scorecard is defined that incorporates all of the impacts as defined in PA02.	Total number of impacts / defined period	Dependant on environment	Target is 0 impacts per defined period. Decreasing results indicates positive results. Establish a threshold that triggers a reassessment of the likelihood of specific impacts or reevaluation of monitoring period definition.
Assess Impact	Results / Output	The purpose of Assess Impact is to identify impacts that are of concern with respect to the system and to assess the likelihood of the impacts occurring. Impacts may be tangible such as the loss of revenue or financial penalties, or intangible, such as loss of reputation or goodwill.	Percent of registered unexpected and unwanted events.	To quantify accuracy of impact assessment	The security team tracks all unwanted and unexpected events.	Reports will be generated by the Security group indicating the number of events.	% = (Number of registered unexpected or unwanted events)/(total number of registered events)	Dependant on environment	Target is 0%. Decreasing results indicates positive results. Establish a threshold that triggers a refresh of impact assessments.
Assess Impact	Impact / Outcome	The purpose of Assess Impact is to identify impacts that are of concern with respect to the system and to assess the likelihood of the impacts occurring. Impacts may be tangible such as the loss of revenue or financial penalties, or intangible, such as loss of reputation or goodwill.	Average cost of event response (hours)	To quantify the business impact of the assessment process	The security team tracks all unwanted and unexpected events.	Reports will be generated by the Security group indicating the cost per event.	Total cost (hours) for all incident responses within specified period / total number of responses occurring within the same period	Dependant on severity of impact to environment	Target is defined by the organization. Decreasing results indicates positive results. Establish a threshold that triggers a refresh of impact assessments and whether or not specified response activities should have been done and to gauge direct impact of security incidents. Closely linked to the management of incident response activities in BP.08.06.
Assess Impact	Impact / Outcome – Results / Output – Implementation / Activity	The purpose of Assess Impact is to identify impacts that are of concern with respect to the system and to assess the likelihood of the impacts occurring. Impacts may be tangible such as the loss of revenue or financial penalties, or intangible, such as loss of reputation or goodwill.	Speed of event response (reaction time) Accuracy (correctness of response the first time) of response Projected vs. real impact Accuracy of impact is confidence in impact assessment Confidence is how well we are on the mark(?) Confidence interval of projected vs. real impact SPLIT INTO MULTIPLE LINES	To monitor the quality of impact monitoring processes and their associated properties.	See Example work product for PA in model	Project Specific	Speed: Start time and end time per event.	TBD	Reduction in speed and cost, which will point at improvement in accuracy. Metric needs to be analyzed by event category and severity. Acceptable deviation for projected vs. real impact should be determined. Monitor first and then try to effect better measurement.

Goal	Type	Objective	Description	Purpose	Data Sources	Implementation Evidence	Formula	Frequency	Indicators
Assess Security Risk: To ensure an understanding of the security risk associated with operating the system within a defined environment is achieved and that risks are prioritized according to a defined methodology.	Implementation/Activity	To identify the security risks involved with relying on a system in a defined environment	#/% of systems with risk assessments performed	To identify the number of systems that have been assessed for risk.	See Example work product for PA in model	Project Specific	% = (# of systems with risk assessments) / (Total # of systems)	Monthly, Quarterly, or Annually	The target for the metric is 100% of all systems have been assessed for risk.
Assess Security Risk: To ensure an understanding of the security risk associated with operating the system within a defined environment is achieved and that risks are prioritized according to a defined methodology.	Implementation/Activity	To identify the security risks involved with relying on a system in a defined environment	#/% of systems with current risk assessments performed within the current review period (The review period is defined by the organization)	To identify the number of systems that have been assessed for risk in the current period	See Example work product for PA in model	Project Specific	% = (# of systems with current risk assessments) / (Total # of systems)	Monthly, Quarterly, or Annually	The target for the metric is 100% of all systems have been assessed for risk within the current review period (The review period is defined by the organization).
Assess Security Risk: To ensure an understanding of the security risk associated with operating the system within a defined environment is achieved and that risks are prioritized according to a defined methodology.	Implementation/Activity	Identify the amount of exposure assessments completed across all systems	#/% of systems with a list of exposures (triples of threat, vulnerability, impact) identified and documented	To identify those systems where a through risk assessment has been conducted	See Example work product for PA in model	Project Specific	% = (# of systems with exposure list defined) / (Total # of systems)	Monthly, Quarterly, or Annually	This metric should always be reaching the target of 100%. This metric depends on the outputs of the threat, vulnerability and risk process areas.
Assess Security Risk: To ensure an understanding of the security risk associated with operating the system within a defined environment is achieved and that risks are prioritized according to a defined methodology.	Implementation/Activity	Prioritize risks	#/% of systems with risks prioritized	To quantify which systems have identified and prioritized risk	See Example work product for PA in model	Project Specific	% = (# of systems with risk priority list defined) / (Total # of systems)	Monthly, Quarterly, or Annually	This metric should always be reaching the target of 100%. Safeguards may address multiple risks, or multiple threats, vulnerabilities and impacts. This aspect can have the effect of changing the effective ordering of the risks to be addressed.

Goal	Type	Objective	Description	Purpose	Data Sources	Implementation Evidence	Formula	Frequency	Indicators
Assess Security Risk: To ensure an understanding of the security risk associated with operating the system within a defined environment is achieved and that risks are prioritized according to a defined methodology.	Results/Output	To identify the security risks involved with relying on a system in a defined environment	#/% of operational decisions based on risk assessments	To identify how many operational decisions are based on risk assessment data	See Example work product for PA in model	Project Specific	% = (# of operational decisions based on risk assessments) / (Total # of operational decisions)	Monthly, Quarterly, or Annually	The target for this metric is to continually increase the number of operational decisions based on risk assessments.
Assess Security Risk: To ensure an understanding of the security risk associated with operating the system within a defined environment is achieved and that risks are prioritized according to a defined methodology.	Results/Output	To identify the security risks involved with relying on a system in a defined environment	Average elapsed time to implement risk mitigation measures	To measure the expediency of the implementation of risk mitigation measures	See Example work product for PA in model	Project Specific	Ave = (Sum of elapsed time to implement risk mitigation measures)/(Total # of Implementations)	Monthly, Quarterly, or Annually	The target for this metric is to continually reduce the elapsed time to implement risk mitigation measures.
Assess Security Risk: To ensure an understanding of the security risk associated with operating the system within a defined environment is achieved and that risks are prioritized according to a defined methodology.	Impact/Outcome	To identify the security risks involved with relying on a system in a defined environment	Cost estimate of potential losses in dollars given the expected likelihood of current risks per evaluation period	To estimate potential losses should current risks materialize	See Example work product for PA in model	Project Specific	$ = Impact cost of potential risks * Likelihood of occurance. Note that this is equivalent to the Annual Loss Expectency if the period of evaluation is annually.	Monthly, Quarterly, or Annually	The target for this metric is to continually reduce the loss expectancy due to potential risks.
Assess Security Risk: To ensure an understanding of the security risk associated with operating the system within a defined environment is achieved and that risks are prioritized according to a defined methodology.	Impact/Outcome	To identify the security risks involved with relying on a system in a defined environment	Differential of expected Cost Savings (Potential Losses) and Actual Cost for additional security controls	To make accurate and informed decisions for which risk mitigation measures to implement	See Example work product for PA in model	Project Specific	$ = (Expected Cost Savings from implementing security controls) - Actual Cost of the security controls)	Monthly, Quarterly, or Annually	The target for this metric is to continually increase the overall number.

Goal	Type	Objective	Description	Purpose	Data Sources	Implementation Evidence	Formula	Frequency	Indicators
Assess Security Risk: To ensure an understanding of the security risk associated with operating the system within a defined environment is achieved and that risks are prioritized according to a defined methodology.	Implementation/Activity	Select the methods, techniques, and criteria by which security risks, for the system in a defined environment are analyzed, assessed and compared	Completeness in Risk Assessment	To assess that there is a clear documented risk assessment methodology containing definition of information asset, information owner, information custodian, and risk calculation criteria describing calculation on threat, impact, vulnerability, and probability for a given information asset in a specific scope (Project)	Risk Assessment methodology for a given project	Project specific	Has the risk assessement been defined and documented? (Yes/No, i.e., a binary indicator)	M,Q,A	Target - Yes, absence of a defined methodology may effect prioritisation difficulties.
Assess Security Risk: To ensure an understanding of the security risk associated with operating the system within a defined environment is achieved and that risks are prioritized according to a defined methodology.	Implementation/Activity	Select the methods, techniques, and criteria by which security risks, for the system in a defined environment are analyzed, assessed and compared	% of Data owners who contributed to the calculation of risk values	To ensure that the judgments made on risk assessment (I.e. determination of Threats,Impact, vulnerability, probability) have the consent of the data owner and data custodian.	Risk Records/risk register	Project specific	% = (# Data owners interviewed/Total Data Owners in the organisation)*100	M,Q,A	This metric should be 100% to ensure that the consent of the data owner resulted in risk assessment valuation
Threats to the security of the systems are identified and characterized	Implementation/Activity	Identify applicable threats arising from natural sources	Natural threats to the systems identified and characterized?	To identify the total number of natural threats defined for the current operating environment	See Example work product for PA in model	Project Specific	Are the applicable natural threat tables documenting the character and likelihood of natural threats available? (Yes/No, i.e. a binary indicator)	Quarterly or Annually	Target - Yes, absence of threat / likelihood tables hinders assessment accuracy.
Threats to the security of the systems are identified and characterized	Implementation/Activity	Identify applicable threats arising from man-made sources	Man-made threats to the systems identified and characterized?	To identify the total number of man made threats defined for the current operating environment	See Example work product for PA in model	Project Specific	Are the applicable natural threat tables documenting the character and likelihood of man-made threats available? (Yes/No, i.e. a binary indicator)	Quarterly or Annually	Target - Yes, absence of threat / likelihood tables hinders assessment accuracy.
Threats to the security of the systems are identified and characterized	Implementation/Activity	Identify threat units of measure and ranges	Threats units identified and ranges established?	To identify the units and ranges used in threat assessement	See Example work product for PA in model	Project Specific	Are the threat tables units and ranges defined? (Yes/No, i.e. a binary indicator)	Quarterly or Annually	Target - Yes, absence of threat unit definition and range limitations hinders assessment accuracy.
Threats to the security of the systems are identified and characterized	Implementation/Activity	Assess capability and motivation of threat agent from threats arising from man-made sources.	Percentage of systems or projects with identified threats	To characterize threats	See Example work product for PA in model	Project Specific	% = (# of system threat assessements completed) / (Total # of systems)	Monthly, Quarterly, or Annually	This metric should be approaching 100% to insure risk assessment accuracy.
Threats to the security of the systems are identified and characterized	Implementation/Activity	Monitor ongoing changes in the threat spectrum and changes to their characteristics	# of threat reviews	To identify how current the threat data is and ensure it is maintained	See Example work product for PA in model	Project Specific			
Threats to the security of the systems are identified and characterized	Implementation/Activity	Assess the likelihood of an occurance of a threat event	Number of systems or projects with threat likelihood defined	To assist in the characterization/prioritization of threats	See Example work product for PA in model	Project Specific			
Threats to the security of the systems are identified and characterized	Results/Output	Identify applicable threats arising from a natural source	Assessment of the existence of supporting	To establish ownership of the selected threats by operation managers (IT and non-IT areas).	Project Specific	Project Specific	3 Point scale - Yes(3), Incomplete(2), or No(1)	M,Q,A	Target - Yes(3), this shall ensure that the threat modeling has a business/operational ownership and that the threats are not chosen from an unrecognized resource.
Threats to the security of the systems are identified and characterized	Results/Output	Identify applicable threats arising from a natural source	Assessment of the existence of supporting	To establish that there is recognized professional expertise in threat selection/review resource (Personnel/data source)	Risk Records/risk register	Project Specific	3 Point scale - Yes(3), Incomplete(2), or No(1)	M,Q,A	Target - Yes(3), this shall ensure that there is a professional expertise available to the organisation for selecting applicable threats.

Goal	Type	Objective	Description	Purpose	Data Sources	Implementation Evidence	Formula	Frequency	Indicators
Threats to the security of the systems are identified and characterized	Results/Output	Monitor ongoing changes in the threat spectrum and changes to their characteristics	Assessment of the existence of supporting	To establish assurance that there is recognized list of events defined when the threat events will be reviewed.	Project Specific	Project Specific	3 Point scale - Yes(3), Incomplete(2), or No(1)	M,Q,A	Target - Yes(3), the evidence of this process shall ensure scale of pro-activeness to ongoing/future threat mapping initiatives.
Threats to the security of the systems are identified and characterized	Results/Output	Identify applicable threats arising from a natural source	All threat targets addressed in COOP	Ensure threat targets are considered in the COOP					
Threats to the security of the systems are identified and characterized	Results/Output		Percent of identified threats mitigated						
Threats to the security of the systems are identified and characterized	Business Impact		Cost of threat mitigation activities	Quantify the cost of mitigating identified threats					
	Results/Output		Number of methods/tools/techniques used to perform vulnerability analysis (e.g., risk assessment, penetration testing, code review, vulnerability scan, manual vs. automated).						
	Implementation/Activity	Cost of risk reduction/Cost of preparedness relative to value of assets protected	Cost associated with type or property vulnerbility assessment (e.g., manual vs. automated).	Reducing the number of high threats	COOP plan includes threat assessment data	All COOP targets addressed in COOP plan	Number, severity, likelihood of threats identified/ percent of systems impacted by threat/Number of reviews of threats		
Identify and characterize system security vulnerabilities	Implementation/Activity	Identify system security vulnerabilities	Percent of systems covered of total systems The number of occurrences (i.e., vulnerability scan) within each SDLC phase	To determine percentage of total systems covered	*Assume the target collection of systems is identified as function of BP05.01			Per each SDLC phase	
Identify and characterize system security vulnerabilities	Results/Output	Select the methods, techniques, and criteria by which security system vulnerabilities in a defined environment are identified and characterized	Assessment of the completeness	To ensure that there is a role/responsibility definition in existence who shall identify any new vulnerability and introducing to the overall risk context.	Assume that there is an evidence for BP.03.01	Project specific	3 Point scale - Yes(3), Incomplete(2), or No(1)	M,Q,A	Target - Yes(3), presence of a role/responsibility ensure existence of a recognized process
Identify and characterize system security vulnerabilities	Results/Output	Select the methods, techniques, and criteria by which security system vulnerabilities in a defined environment are identified and characterized	Assessment of the existence of supporting	Existence of Incident Reporting, and Learning made by the organisation	Organizational Incident Procedures	Project specific	3 Point scale - Yes(3), Incomplete(2), or No(1)	M,Q,A	Target - Yes(3), existence of Incident response, learning from incidents is a correlated effort to establish the effectiveness of security system vulnerability identification
Identify and characterize system security vulnerabilities	Results/Output	Select the methods, techniques, and criteria by which security system vulnerabilities in a defined environment are identified and characterized	Assessment of the existence of supporting	Existence of Vulnerability updates to IT infrastructure areas from external Knowledge/Vendor resources.	Organizational Vulnerability gathering practices	Project specific	3 Point scale - Yes(3), Incomplete(2), or No(1)	M,Q,A	Target - Yes(3), presence of an external specialist or a recognized vendor resource demonstrates the resource allocation and effectiveness.
Identify and characterize system security vulnerabilities	Results/Output	Select the methods, techniques, and criteria by which security system vulnerabilities in a defined environment are identified and characterized	Assessment of the existence of supporting	Updation of new system vulnerabilities to Ongoing Risk valuation	Assume that there is an evidence for BP.03.01	Project specific	3 Point scale - Yes(3), Incomplete(2), or No(1)	M,Q,A	Target - Yes(3), this shall ensure that not onl the vulnerabilities recognized but also incorporated in the overall risk management.
The security assurance work products and processes clearly provide the evidence that the customer's security needs have been met.	Implementation/Activity	The purpose of Build Assurance Argument is to clearly convey that the customer's security needs are met. An assurance argument is a set of stated assurance objectives that are supported by a combination of assurance evidence that may be derived from multiple sources and levels of abstraction.	Assurance objective existence (Whether or not assurance objectives that identify the customer's requirements for the level of confidence needed in a system's security features have been determined.)	To quantify compliance with build assurance argument process	See Example work product for PA in model	Project Specific	Do assurance objectives exist? (Yes/No, i.e., a binary indicator)	At beginning of SDLC and as required by identified assurance needs within 06.02 thereafter	Definition of assurance objectives. Target – Yes. Documentation of specific security assurance objectives indicates positive results. Objective formulation will guide the entire assurance evidence analysis effort, lack of objectives may be the result of an ill-defined target of assessment or vague lines of communication/responsibility within the security/IT support organization.

Goal	Type	Objective	Description	Purpose	Data Sources	Implementation Evidence	Formula	Frequency	Indicators
The security assurance work products and processes clearly provide the evidence that the customer's security needs have been met.	Implementation/Activity	The purpose of Build Assurance Argument is to clearly convey that the customer's security needs are met. An assurance argument is a set of stated assurance objectives that are supported by a combination of assurance evidence that may be derived from multiple sources and levels of abstraction.	Assurance strategy existence (Whether or not a security assurance strategy that describes the plan for meeting the customer's security assurance objectives, and identifies the responsible parties, has been documented.)	To quantify compliance with build assurance argument process	See Example work product for PA in model	Project Specific	Does a security assurance strategy exist? (Yes/No, i.e., a binary indicator)	As required by identified assurance needs	Definition of assurance strategy. Target – Yes. Documentation of security assurance strategy indicates positive results. Ambiguity in strategy formulation will impact the viability of the assurance argument, may be the result of an ill-defined target of assessment.
The security assurance work products and processes clearly provide the evidence that the customer's security needs have been met.	Implementation/Activity	The purpose of Build Assurance Argument is to clearly convey that the customer's security needs are met. An assurance argument is a set of stated assurance objectives that are supported by a combination of assurance evidence that may be derived from multiple sources and levels of abstraction.	Repository existence (Whether or not assurance evidence from other process areas has been gathered and controlled.)	To quantify compliance with build assurance argument process	See Example work product for PA in model	Project Specific	Does an evidence repository exist? (Yes/No, i.e., a binary indicator)	As required by the documented security assurance strategy	Target – Yes. Gathering of evidence into a controlled repository indicates positive results. Ambiguity in security assurance strategy formulation (BP 06.02) will impact the viability and quality of the repository contents.
The security assurance work products and processes clearly provide the evidence that the customer's security needs have been met.	Implementation/Activity	The purpose of Build Assurance Argument is to clearly convey that the customer's security needs are met. An assurance argument is a set of stated assurance objectives that are supported by a combination of assurance evidence that may be derived from multiple sources and levels of abstraction.	Analysis report frequency	To quantify compliance with build assurance argument process	See Example work product for PA in model	Project Specific	Does frequency of analysis report generation comply with policy? (Yes/No, i.e., a binary indicator)	As required by policy	Target – Yes. Repetition of analysis reports within the time-frame provisions of client policy, or other relevant governance, indicates positive results. Inability to comply with report frequency requirements my be result of disorganized evidence gathering efforts (BP 06.03) or unclear assurance strategy (BP 06.02). This may impact abilities to ensure currency with existing work products and relevancy with security assurance objectives.
The security assurance work products and processes clearly provide the evidence that the customer's security needs have been met.	Results/Output	The purpose of Build Assurance Argument is to clearly convey that the customer's security needs are met. An assurance argument is a set of stated assurance objectives that are supported by a combination of assurance evidence that may be derived from multiple sources and levels of abstraction.	a.Percent of objectives that adequately respond to corresponding assurance claims. b.Percent of assurance objectives identified before or during requirements definition. (THIS NEEDS TO BE SPLIT INTO MULTIPLE METRICS)	To quantify the accuracy of the build assurance argument process	See Example work product for PA in model	Project Specific	a.Number of objectives that adequately respond to corresponding assurance claims / total number of objectives. b.Number of assurance objectives identified before or during requirements definition / total number of objectives.	Depends on the assurance need	Target is 100%. Increasing results indicates positive results. Establish a threshold that triggers a formal restatement of security objectives. Closely linked to the generalized monitoring activity in BP.08.02 in that changes to system design or its security posture may modify assurance objectives.
The security assurance work products and processes clearly provide the evidence that the customer's security needs have been met.	Results/Output	The purpose of Build Assurance Argument is to clearly convey that the customer's security needs are met. An assurance argument is a set of stated assurance objectives that are supported by a combination of assurance evidence that may be derived from multiple sources and levels of abstraction.	a.Evidence age (appropriate for and in relation to activity) b.Currency of evidence with existing work products c.Accuracy of evidence (chain of custody) d.Accessibility of evidence (Ease of extraction from a process to make it available.) (THIS NEEDS TO BE SPLIT INTO MULTIPLE METRICS)	To quantify the accuracy of the build assurance argument process	See Example work product for PA in model	Project Specific	a.S evidence element ages / total number of types of evidence (see MWGE 06.04, metric "a.") b.Number of evidence elements collected current with product / total number of types of evidence elements c.Number of evidence elements with correct custody / total number of types of evidence elements d.S time to retrieve evidence elements / total number of types of evidence elements	Depends on the assurance need	a.Target – 0 (average unit of time for evidence age appropriate for and in relation to activity). In general, decreasing the time indicates positive results. Establishing activity appropriate age targets should yield overall improvements in the other effectiveness metrics. b.Target – 100% currency of evidence data elements. Increasing results indicates positive results. c.Target – 100% correct custody chain / data protection. Increasing results indicates positive results. d.Target – 0 (average unit of time to retrieve evidence). Decreasing the time indicates positive results. For all metrics in this group, establish a threshold that triggers a restatement of security strategy for communications with internal engineering groups and external groups.

Goal	Type	Objective	Description	Purpose	Data Sources	Implementation Evidence	Formula	Frequency	Indicators
The security assurance work products and processes clearly provide the evidence that the customer's security needs have been met.	Results/Output	The purpose of Build Assurance Argument is to clearly convey that the customer's security needs are met. An assurance argument is a set of stated assurance objectives that are supported by a combination of assurance evidence that may be derived from multiple sources and levels of abstraction.	a.Number of types of evidence (used in formulas for MWGE 06.03 metrics) b.Adequacy of evidence c.Assurance evidence ease of use d.Appropriateness of assurance evidence (THIS NEEDS TO BE SPLIT INTO MULTIPLE METRICS)	To quantify the accuracy of the build assurance argument process	See Example work product for PA in model	Project Specific	a.Count of types of evidence provided through set up of evidence repository. b.Number of evidence types with adequate evidence / total number of types of evidence c.S time to analyze evidence elements / total number of types of evidence d.Number of evidence types with evidence matching baseline description / total number of types of evidence	Depends on the assurance need	a.Target – the correct count of types of elements in the repository. Results matching the security assurance strategy are positive results. Deviations from strategy evidence requirements impact the analysis completeness, therefore attenuation of deviations indicates positive results. b.Target – 100%. Increasing results indicates positive results. Establish threshold that may necessitate modifications to security assurance strategy. c.Target – 0 (unit time appropriate for evidence type and associated analysis activity). Decreasing results indicates positive results. Establish threshold that may necessitate modifications to security assurance strategy. d.Target – 100%. Increasing results indicates positive results. Establish threshold value that may necessitate revisions to the system, security work products and processes that support the security objectives.
The security assurance work products and processes clearly provide the evidence that the customer's security needs have been met.	Results/Output	The purpose of Build Assurance Argument is to clearly convey that the customer's security needs are met. An assurance argument is a set of stated assurance objectives that are supported by a combination of assurance evidence that may be derived from multiple sources and levels of abstraction.	a.Percent of assurance objectives covered by supporting evidence (could be quantified by priority of assurance objectives) b.Percent of evidence deficiencies relative to assurance objectives c.Timeliness of assurance argument (THIS NEEDS TO BE SPLIT INTO MULTIPLE METRICS)	To quantify the accuracy of the build assurance argument process	See Example work product for PA in model	Project Specific	a.Number of assurance objectives covered by supporting evidence / total number of assurance objectives b.Total number of deficient assurance evidence types / total number of assurance evidence types / total number of assurance objectives c.Time from start of assurance analysis to its completion (unit of time appropriate to activity)	Depends on the assurance need	a.Target – 100%. Increasing results indicates positive results. Establish threshold that may necessitate modifications to security assurance strategy. b.Target – 0% per objective. Decreasing results indicates positive results. Establish threshold value that may necessitate revisions to the system, security work products and processes that support the security objectives. c.Target – 0 (Appropriate time-frame for and in relation to activity). Decreasing the time indicates positive results.
The security assurance work products and processes clearly provide the evidence that the customer's security needs have been met.	Impact/Outcome	The purpose of Build Assurance Argument is to clearly convey that the customer's security needs are met. An assurance argument is a set of stated assurance objectives that are supported by a combination of assurance evidence that may be derived from multiple sources and levels of abstraction.	a. Difference in cost/level of effort between Projects (system development or not) when assurance objectives were identified / not identified Compared between organizations that define assurance objectives vs. those that do not b. Rating of Customer satisfaction c. Rating of Employee satisfaction (THIS NEEDS TO BE SPLIT INTO MULTIPLE METRICS)	To quantify the business impact of the build assurance argument process	See Example work product for PA in model	Project Specific	a.[S Cost/LOE for projects without identified objectives (PWo) / total number of PWo] – [S Cost/LOE for Projects with identified objectives (PWi) / total number of PWi] b.[S Rating of Customer satisfaction for projects with identified objectives (PWi) / total number of PWi] – [S Rating of Customer satisfaction for projects without identified objectives (PWo) / total number of surveyed PWo] c.Same as "b." but with rating of Employee satisfaction rather than Customer satisfaction	As deemed appropriate by management	a.Target – Significant savings (definition of "significant" depends on size and complexity of project). b.And c. (Range of -100% to +100%.) Target – +100%. For all MWGI 06.01 metrics, increasing results indicates positive results. Negative result (or zero result) indicates negative Project-cost/Customer-satisfaction/Employee-satisfaction impact (or no change).
The security assurance work products and processes clearly provide the evidence that the customer's security needs have been met.	Impact/Outcome	The purpose of Build Assurance Argument is to clearly convey that the customer's security needs are met. An assurance argument is a set of stated assurance objectives that are supported by a combination of assurance evidence that may be derived from multiple sources and levels of abstraction.	a. Difference in cost/level of effort between Projects (system development or not) when assurance strategy was identified / not identified Compared between organizations that define an assurance strategy vs. those that do not b. Rating of Customer satisfaction c. Rating of Employee satisfaction (THIS NEEDS TO BE SPLIT INTO MULTIPLE METRICS)	To quantify the business impact of the build assurance argument process	See Example work product for PA in model	Project Specific	a.[S Cost/LOE for projects without an identified strategy (PWo) / total number of PWo] – [S Cost/LOE for Projects with identified strategy (PWi) / total number of PWi] b.[S Rating of Customer satisfaction for projects with an identified strategy (PWi) / total number of PWi] – [S Rating of Customer satisfaction for projects without identified strategy (PWo) / total number of surveyed PWo] c.Same as "b." but with rating of Employee satisfaction rather than Customer satisfaction	As deemed appropriate by management	a.Target – Significant savings (definition of "significant" depends on size and complexity of project). b.And c. (Range of -100% to +100%.) Target – +100%. For all MWGI 06.01 metrics, increasing results indicates positive results. Negative result (or zero result) indicates negative Project-cost/Customer-satisfaction/Employee-satisfaction impact (or no change).

Goal	Type	Objective	Description	Purpose	Data Sources	Implementation Evidence	Formula	Frequency	Indicators
The security assurance work products and processes clearly provide the evidence that the customer's security needs have been met.	Impact/Outcome	The purpose of Build Assurance Argument is to clearly convey that the customer's security needs are met. An assurance argument is a set of stated assurance objectives that are supported by a combination of assurance evidence that may be derived from multiple sources and levels of abstraction.	Ability to provide evidence-based assuranc argument	To quantify the business impact of the build assurance argument process	See Example work product for PA in model	Project Specific	S Cost (FTEs LOE) for all assessment tasks for all assurance argument developments / total number of assurance arguments developed / S Total time from start to finish of all assurance efforts	As required by assurance need	Target – 0 FTEs LOE per scheduled unit of time. Decreasing hours per unit of time indicates positive results. The larger the leve of effort (FTEs) per unit of time (e.g., month) represents a higher level of resource allocation to the assurance task, this indicates negative results. Coordination with external groups (e.g., client, systems security certifier, or user) as defined in PA07 Coordinate Security may also need to be incorporated into the LOE calculations to get a more reasonable estimate of the organizations ability to provide the assurance argument.
The security assurance work products and processes clearly provide the evidence that the customer's security needs have been met.	Impact/Outcome	The purpose of Build Assurance Argument is to clearly convey that the customer's security needs are met. An assurance argument is a set of stated assurance objectives that are supported by a combination of assurance evidence that may be derived from multiple sources and levels of abstraction.	a. Difference in cost/level of effort between Projects (system development or not) when assurance argument was identified / not identified b. and c. Comparison between organizations that define an assurance argument vs. those that do not via: (b.) Rating of Customer satisfaction, and (c.) Rating of Employee satisfaction d. Quality of assurance argument	To quantify the business impact of the build assurance argument process	See Example work product for PA in model	Project Specific	a.[S Cost/LOE for projects without an assurance argument (PWo) / total number of PWo] – [S Cost/LOE for Projects with identified strategy (PWi) / total number of PWi] b.[S Rating of Customer satisfaction for projects with an assurance argument (PWi) / total number of PWi] – [S Rating of Customer satisfaction for projects without an assurance argument (PWo) / total number of surveyed PWo] c.Same as "b." but with rating of Employee satisfaction rather than Customer satisfaction d.Cost (hours) rework per quality defect * S Number of quality defects / total number of assurance argument reports	As deemed appropriate by management	a.Target – Significant savings (definition of "significant" depends on size and complexity of project). b.And c. (Range of -100% to +100%.) Target – +100%. For all MWGI 06.01 metrics, increasing results indicates positive results. Negative result indicates negative Project-cost/Customer/Employee-satisfaction impact. d. Target – 0 hours rework per assurance argument report. Decreasing results indicates positive results.
Coordinate Security: To ensure all members of the project team are aware of and involved with security engineering activities to the extent necessary to perform their functions and that decisions and recommendations related to security are communicated and coordinated.	Implementation/Activity	That different groups need to be aware of and involved with security engineering activities and that coordination mechanisms for these activiites have been identified	%/# of security efforts that have completed the appropriate planning process	To quantify the number of security efforts that have met the planning process requirements	See Example work product for PA in model	Project Specific	% = (# of security efforts that have successfully completed the planning process)/(Total # security efforts)	Monthly, Quarterly, or Annually	The target for the metric is 100% of security efforts with successful completion of the planning process. [Focused on BPs 1,2].
Coordinate Security: To ensure all members of the project team are aware of and involved with security engineering activities to the extent necessary to perform their functions and that decisions and recommendations related to security are communicated and coordinated.	Results/Output	That conflicts and disputes are resolved in an appropriate productive manner	# of unresolved action items that are critical to the success of the security effort	To evaluate the quality of the conflict resolution process	See Example work product for PA in model	Project Specific	Count	Monthly, Quarterly, or Annually	The target for the metric is to reduce the number of unresolved critical action items.

ISSEA Metrics

Goal	Type	Objective	Description	Purpose	Data Sources	Implementation Evidence	Formula	Frequency	Indicators
Coordinate Security: To ensure all members of the project team are aware of and involved with security engineering activities to the extent necessary to perform their functions and that decisions and recommendations related to security are communicated and coordinated.	Impact/Outcome	To communicate security decisions and recommendations among the various security engineers, other engineering groups, external entities, and other appropriate parties	Cost of implementing/ integrating new/additional requirements	To quantify the cost of implementing new/additional requirements that were overlooked/omitted due to communication/ decision failures	See Example work product for PA in model	Project Specific	$ = Sum for all costs associated with additional work required	Monthly, Quarterly, or Annually	The target for the metric is to reduce the cost of additional work required.
To ensure both internal and external security related events are detected and tracked, incidents are responded to in accordance with policy, and changes to the operational security posture are identified and handled in accordance with the security objectives.	Results/Output	Analyze event records to determine the cause of an event, how it proceeded, and likely future events	# of corrective actions implemented with in X days based on review of event logs	To measure the expediency of the implementation of corrective actions	See Example work product for PA in model	Project Specific	number of implemented corrective actions/total number of required corrective actions based on event logs	Monthly, Quarterly, or Annually	The target for this metric is to continually increase the number of corrective actions implemented with in X days based on review of event logs where X is defined by organization's policy.
To ensure both internal and external security related events are detected and tracked, incidents are responded to in accordance with policy, and changes to the operational security posture are identified and handled in accordance with the security objectives.	Implementation/Activity	Monitor the performance and functional effectiveness of security safeguards	#/% of systems with required safeguards in place	To determine which systems lack the appropriate safeguards to mitigate security risks	See Example work product for PA in model	Project Specific	% = (# of systems with properly configured safeguards in place) / (Total # of systems)	Monthly, Quarterly, or Annually	The target for the metric is 100% of all systems with properly configured safeguards in place.

Goal	Type	Objective	Description	Purpose	Data Sources	Implementation Evidence	Formula	Frequency	Indicators
To ensure both internal and external security related events are detected and tracked, incidents are responded to in accordance with policy, and changes to the operational security posture are identified and handled in accordance with the security objectives.	Results/Output	Monitor the performance and functional effectiveness of security safeguards	%/# of Incidents due to failed safeguards	To determine which systems lack the appropriate safeguards to mitigate security risks	See Example work product for PA in model	Project Specific	% = (# of Incidents due to failed safeguards)/(Total # of tracked incidents)	Monthly, Quarterly, or Annually	The target for the metric is to obtain 0% of al incidents due to failed safeguards.
To ensure both internal and external security related events are detected and tracked, incidents are responded to in accordance with policy, and changes to the operational security posture are identified and handled in accordance with the security objectives.	Results/Output	Monitor the performance and functional effectiveness of security safeguards	%/# Incidents due to absence of implemented safeguards	To determine which systems lack the appropriate safeguards to mitigate security risks	See Example work product for PA in model	Project Specific	% = (# of Incidents due to absence of implemented safeguards) / (# of total tracked incidents)	Monthly, Quarterly, or Annually	The target for the metric is to obtain 0% of al incidents due to absent safeguards.
To ensure both internal and external security related events are detected and tracked, incidents are responded to in accordance with policy, and changes to the operational security posture are identified and handled in accordance with the security objectives.	Impact/Outcome	Monitor the performance and functional effectiveness of security safeguards	Cost of Incidents due to failed safeguards	To determine the cost of incidents due to failed safeguards	See Example work product for PA in model	Project Specific	$ = Sum for all applicable incidents (Cost of Los Asset+Cost of Lost User Productivity+Cost of Root/Cause Investigation+Cost of Labor to Implement changes/repairs)	Monthly, Quarterly, or Annually	The target for the metric is to reduce the cos of failed safeguards.

Goal	Type	Objective	Description	Purpose	Data Sources	Implementation Evidence	Formula	Frequency	Indicators
To ensure both internal and external security related events are detected and tracked, incidents are responded to in accordance with policy, and changes to the operational security posture are identified and handled in accordance with the security objectives.	Impact/Outcome	Monitor the performance and functional effectiveness of security safeguards	Cost of Incidents due to absence of implemented safeguards	To determine the opportunity cost of not implementing safeguards	See Example work product for PA in model	Project Specific	$ = Sum for all applicable incidents (Cost of Los Asset+Cost of Lost User Productivity+Cost of Root/Cause Investigation+Cost of Labor to Implement changes/repairs)	Monthly, Quarterly, or Annually	The target for the metric is to reduce the cost of failed safeguards.
To ensure both internal and external security related events are detected and tracked, incidents are responded to in accordance with policy, and changes to the operational security posture are identified and handled in accordance with the security objectives.	Implementation/Activity	Manage the response to security relevant incidents	#/% of systems with incident response capability	To determine the level of implementation of the incident response capability within the environment	See Example work product for PA in model	Project Specific	% = (# of systems with incident response capability) / (Total # of systems)	Monthly, Quarterly, or Annually	The target for the metric is 100% of all systems with incident response capability.
To ensure both internal and external security related events are detected and tracked, incidents are responded to in accordance with policy, and changes to the operational security posture are identified and handled in accordance with the security objectives.	Results/Output	Manage the response to security relevant incidents	Average decision time to determine the response to a security incident	To determine the level of implementation of the incident response capability within the environment	See Example work product for PA in model	Project Specific	Days = (Sum of elapsed time between when incidents are reported and when response decisions are made)/(Total # of decisions)	Monthly, Quarterly, or Annually	The lower the decision time the less risk of additional consequences occurring due to the incident. Required fields:[Times to capture for each incident: Incident occurred, incident reported, decision made about response, closure].

Goal	Type	Objective	Description	Purpose	Data Sources	Implementation Evidence	Formula	Frequency	Indicators
Tto provide system architects, designers, implementers, or users with the security information they need. This information includes security architecture, design, or implementation alternatives and security guidance.	Results/Output	Work with designers, developers, and users to ensure that appropriate parties have a common understanding of security input needs.	Percent of critical security needs being addressed by the solutions	Measure the effectiveness of the requirements team in translating known threats into design requirements and to measure the development team's ability to address the requirements in terms of defense programming.	See Example work product for PA in model	Project Specific	%=(Number of unmapped requirements/total number of requirements)	Verify prior to the development and test phase of the SDLC	Maintaining or decreasing the ratio of unmapped requirements throughout the SDLC.
Tto provide system architects, designers, implementers, or users with the security information they need. This information includes security architecture, design, or implementation alternatives and security guidance.	Results/Output	Analyze and prioritize engineering alternatives using security constraints and considerations.	Number of alternatives identified and how many were explored. Measurement of quality of alternative solution.	Maximize the use of alternative solutions to address security requirements	See Example work product for PA in model	Project Specific	Number of alternatives identifed and number of alternatives explored.	Verify prior to the development and test phase of the SDLC	Maintaining or decreasing the ratio of unmapped requirements throughout the SDLC.
Specify Security Needs: To ensure a common understanding of security needs is reached between all parties, including the customer.	Implementation/Activity	That all requirements and needs related to security for the system have been explicitly identified	%/# of systems that have completed the appropriate requirements analysis	To determine which systems have the appropriate level of security in place	See Example work product for PA in model	Project Specific	%=(# of systems that have completed the appropriate requirements analysis)/ (Total # of systems)	Monthly, Quarterly, or Annually	The target for the metric is 100% of all systems where an appropriate requirements analysis has been performed. [Focused on BPs 1,2,3].
Specify Security Needs: To ensure a common understanding of security needs is reached between all parties, including the customer.	Results/Output	To develop/maintain a high-level security oriented view of the enterprise, including roles, responsibilities, information flow, assets, resources, personnel protection, and physical protection	Ave Time to update the view of the security concept of operations	To determine the timeliness of updating the view of the security concept of operations	See Example work product for PA in model	Project Specific	Days = (Sum of elapsed time between when the physical change has occurred and when the changes are reflected in the view of the security concept of operations) /(Total # of changes)	Monthly, Quarterly, or Annually	The lower the change time the less risk of additional consequences occurring due to the outdated view of the security concept of operations. Required fields: [Times to capture for each change: Physical Change completed/reported, View change completed/reported].
Specify Security Needs: To ensure a common understanding of security needs is reached between all parties, including the customer.	Impact/Outcome	To obtain concurrence between all applicable parties on the security requirements in a timely manner	Average number of days required to gain concurrence regarding security requirements over the last period	To quantify the number of days required to gain concurrence regarding security requirements	See Example work product for PA in model	Project Specific	Average = (Sum of days per requirement)/(Total # of requirements)	Monthly, Quarterly, or Annually	The target for the metric is to reduce the total number of days required to gain concurrence regarding security requirements.

Goal	Type	Objective	Description	Purpose	Data Sources	Implementation Evidence	Formula	Frequency	Indicators
Verify and Validate Security: to ensure that solutions meet security requirements and meet the customer's operational security needs.	Implementation/Activity	Define the approach for verifying and validating security solutions	#/% of systems with Verification and Validation plan developed	To quantify which systems have an IVV process/plan in place	See Example work product for PA in model	Project Specific	% = (# of systems with verification and validation plans defined) / (Total # of systems)	Monthly, Quarterly, or Annually	The target for the metric is 100% of all systems with verification and validation plans defined.
Verify and Validate Security: to ensure that solutions meet security requirements and meet the customer's operational security needs.	Results/Output	Define the approach for verifying and validating security solutions	#/% of systems that has undergone Verification and Validation Process	To quantify the percentage of systems that have been exposed to the IVV process	See Example work product for PA in model	Project Specific	% = (# of systems in which verification and validation has been performed) / (Total # of systems)	Monthly, Quarterly, or Annually	The target for the metric is 100% of all systems which verification and validation has been performed.
Ensure Quality: To ensure process quality is defined and measured and expected work product quality is achieved.	Implementation/Activity	Quality Controls have been identified and implemented	# of Quality Controls monitored and reported on a regular basis	To determine the level at which Quality is being monitored, reported, and controlled within the environment	See Example work product for PA in model	Project Specific	Count	Monthly, Quarterly, or Annually	The target for the metric is an increasing value over time implementation of Quality Controls into a Security Program.
Ensure Quality: To ensure process quality is defined and measured and expected work product quality is achieved.	Results/Output	Recommendations for quality improvements or corrective actions are based on analyzing quality controls measurements	#/% of quality improvements or corrective actions implemented based on analyzing quality controls measurements	To quantify the percentage of improvements/corrective actions that were based on quality controls measurements and analysis	See Example work product for PA in model	Project Specific	% = (# of quality improvements or corrective actions based on analyzing quality controls measurements)/ (Total # of improvements or corrective actions)	Monthly, Quarterly, or Annually	The target for the metric is 100% implementation of Quality Controls into a Security Program.
Manage Configurations: To ensure Control over work product configurations is maintained.	Results/Output	Configuration being monitored and tracked	#/% of solutions where configurations are monitored and tracked according to process and by the identified units	To determine the number of solution configurations that are being monitored and tracked according to policy	See Example work product for PA in model	Project Specific	% = # of solutions where configurations are monitored and tracked according process and by the identified units / Total # of solutions	Monthly, Quarterly, or Annually	The target for the metric is 100% implementation of Configuration Management into a Security Program. The process refereed to in the metric assumes that only meaningful items are tracked.
Manage Configurations: To ensure Control over work product configurations is maintained.	Results/Output	Configuration changes are approved and documented prior to implementation	#/% of solutions where configuration changes are approved and documented according to process prior to implementation	To identify those solutions where changes to configuration are approved and documented	See Example work product for PA in model	Project Specific	% = (# of solutions where configuration changes are approved and documented according process prior to implementation) / (Total # of recorded configuration changes)	Monthly, Quarterly, or Annually	The target for the metric is 100% implementation of Configuration Management into a Security Program. This metric assumes that a mature CM process is in place and being followed.
Plan Technical Effort: To ensure all aspects of technical efforts are planned.	Implementation/Activity	That the Technical Plans for all technical efforts of sufficient detail	#/% of Technical plans in place complete with identified resources, costs, scope, and timeline	To identify the existence of adequate project plans	See Example work product for PA in model	Project Specific	% = (# of Technical plans in place complete with identified resources, costs, scope, and timeline) / (Total # of Technical plans)	Monthly, Quarterly, or Annually	The target for the metric is 100% implementation of Planned Technical Efforts into a Security Program.
Plan Technical Effort: To ensure all aspects of technical efforts are planned.	Results/Output	Technical Plans for all technical efforts are of sufficient detail	#/% of Technical plans that have been reviewed and approved	To quantify the number of project plans that have been reviewed and approved	See Example work product for PA in model	Project Specific	% = (# of Technical plans that have been reviewed and approved) / (Total # of Technical Plans)	Monthly, Quarterly, or Annually	The target for the metric is 100% implementation of Planned Technical Efforts into a Security Program.

ISSEA Metrics

Goal	Type	Objective	Description	Purpose	Data Sources	Implementation Evidence	Formula	Frequency	Indicators
Plan Technical Effort: To ensure all aspects of technical efforts are planned.	Impact/Outcome	Develop cost estimates for all technical resources required by the project	% of Cost variance from original estimate expressed as a percent of total cost	To measure the cost deviation from the original estimate in relations to the actual total cost	See Example work product for PA in model	Project Specific	$ = Cost Variation (Budgeted Cost of work to be performed)/ Actual Cost of work performed)	Monthly, Quarterly, or Annually	Low variance should be targeted. Each organization should establish specific acceptable variance.
Plan Technical Effort: To ensure all aspects of technical efforts are planned.	Impact/Outcome	To Develop technical schedules for the entire project life cycle	% of schedule deviation from original estimate expressed as a percent of days over/under schedule	To measure the time deviation from the original estimate in relations to the actual total time spent	See Example work product for PA in model	Project Specific	% = (Schedule deviation from original schedule) (length of period of performance)	Monthly, Quarterly, or Annually	Low variance should be targeted. Each organization should establish specific acceptable variance.
Provide Ongoing Skills and Knowledge: To ensure the organization has the skills necessary to achieve project and organizational objectives.	Results/Output	That Training Needs and Materials are assessed and maintained on a regular basis	#/% of changes or enhancements in the training program based on a needs assessment performed in the past quarter	To measure the number of changes/ enhancements to the training program that were based on current needs assessment data	See Example work product for PA in model	Project Specific	% = (# of changes or enhancements in the training program based on a needs assessment performed in the past quarter) / (Total # of changes or enhancements)	Monthly, Quarterly, or Annually	The target for the metric is to continually increase the share of changes based on needs assessments.
Provide Ongoing Skills and Knowledge: To ensure the organization has the skills necessary to achieve project and organizational objectives.	Implementation/Activity	That Training Records and Assessment Data are stored for future review	%/# of Training Records and Assessment Data stored for future review	To assess the longer-term viability of training based upon assessment data	See Example work product for PA in model	Project Specific	% personnel for whom training records and assessment data is stored for future review.	Monthly, Quarterly, or Annually	The target for this metric is tracking of 100% of training records for all personnel
Provide Ongoing Skills and Knowledge: To ensure the organization has the skills necessary to achieve project and organizational objectives.	Results/Output	That appropriate skill and knowledge are available to the systems engineering effort	%/# of personnel with appropriate skills & knowledge required by the system engineering effort	To evaluate the personnel needs assessment process quality	See Example work product for PA in model	Project Specific	% = (of personnel with appropriate skills & knowledge required by the system engineering effort)/(Total # of personnel involved in engineering effort)	Monthly, Quarterly, or Annually	The target for the metric is to achieve 100% of all personnel that possess the appropriate skills.