Reifer Consultants, Inc.

CONIPMO Workshop

Donald J. Reifer

2006 PSM Users' Group
Conference Workshop

Workshop Goals

Background

- COCOMO-like model being developed to estimate the costs of implementing network defenses
  - Perimeter defense
  - Defense in depth
- Tradeoff model looking at both investments and operational costs
- Model is requirements-based and based on successful COSYSMO
- MDA SBIR Phase I funded
- Phase II requires an invite

Goals

- Solidify size constructs and cost drivers for network defense & AT cost models
  - Critical Program Information (CPI) identified in PPP
  - Requirements-based.
  - Scenario-driven (DITSCAP)
- Complete Round 2 of the CONIPMO Delphi
  - Firm up the model framework
  - Finalize cost driver calibration
  - Work issues raised during Delphi and at workshop
  - Solicit inputs and opinions from experts/potential users

Workshop Agenda

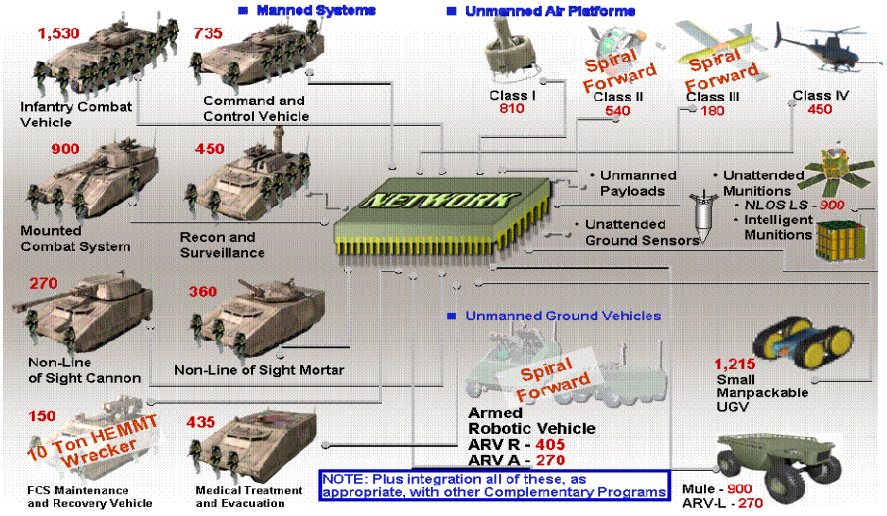
Agenda

- Introduce you to CONIPMO
- Review the model, its scope, its life cycle and its parameters
- Summarize the results of the Round 1 Delphi
- Determine whether the model reflects your experience in the network defense domain
- Conduct a Round 2 Delphi to update the model as part of the discussions

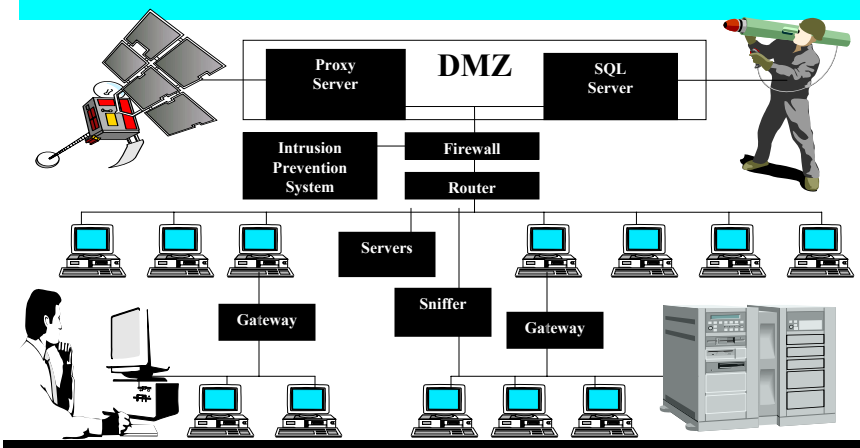
Intended Outputs

- Recommendations for enhancing the model
- Delphi Round 2 expert inputs for the model parameters
- Recommended early adopter projects who can act as data sources
- Letters of support for pursuing the second phase of the effort

Setting the Stage: DOD's Network Centric Warfare Vision



Network Security –At What Cost?



Defense-in-depth is a necessary, but expensive proposition requiring additional equipment and software to provide layers of protection against intruders, both insiders and outsiders. Costs need to be justified by the protection provided.

What Does Network Security Cost?

- Establishing network defenses (and AT)
  - How much should you budget?
    - Acquisitions?
    - Labor?
    - Licenses?
    - Support?
  - What are the cost tradeoffs?
  - What would you do if you did not get enough money?
- Maintaining network defenses
  - How much does it take to maintain your defenses?
    - Acquisitions?
    - Labor?
    - Licenses?
    - Support?
  - How do you justify these costs in the POM?
  - What would you do if you were short changed?

Effects of Security on Effort

- For software developers:
  - Source lines of code increases
  - Effort to generate software increases
    - Security functional requirements
    - Security assurance requirements
  - Effort to transition also increases
    - More documentation
    - Certification and accreditation costs

Being addressed by COSECMO

- For systems engineers:
  - Effort to develop system increases
    - Network defense requirements
    - Network defense operational concepts
    - Program protection requirements
    - Anti-tamper implementation
  - Effort to transition also increases
    - DITSCAP and red teaming

Being addressed by CONIPMO

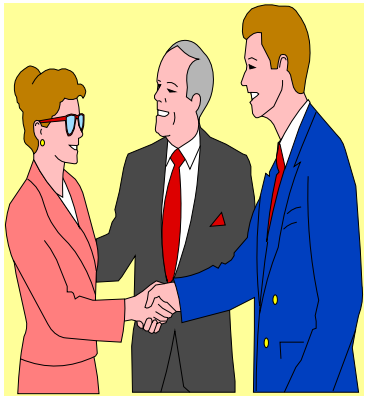
Answering the Question: Model Development Process

Steps

- ✓ Collaborator group formed
- ✓ Goals set and effort bounded
- ✓ Goals mapped to EIA 632 life cycle activities
- ✓ Notation cost model structure developed
- ✓ Focus placed on initial effort on early estimation models
- **Next** - validate that it is feasible to develop a model
- **Future** - embark on the model development journey in Phase II

Goals Established for Effort

- Three primary goals for the effort were established using the GQM approach
  - Be able to generate an accurate estimate of the time and effort needed to secure the network infrastructure defenses
  - Be able to validate the estimate using actuals
  - Be able to predict the effort involved should anti-tamper be a requirement

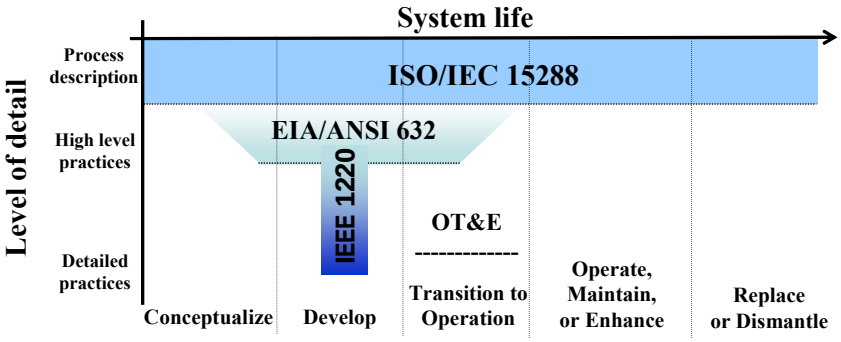


Collaborators Group

Network Defense Model Framework

Conceptualize	Develop	OT&E	Transition to Operations	Operate, Maintain or Enhance	Replace (or Dismantle)
1. Requirements specification 2. Architecture development 3. Project planning	4. Product assessments 5. HW and SW acquisitions 6. Software development, integration & test	7. OT&E	8. Transition and turnover 9. DITSCAP	10. Operations 11. Maintenance	12. Replace (or destroy)
Heuristics model	***Parametric model***	***Heuristic model***			
Program Protection Tasks (if required)					
13. Program protection planning	14. HW and SW acquisitions 15. HW and SW modifications/	16. Red teaming	17. Independent T&E 18. DITSCAP	19. Maintenance	20. Destroy
Heuristic model					

Relationship to Key SE Standards



Purpose of the Standards:

ISO/IEC 15288 - *Establish a common framework for* ***describing the life cycle of systems***

EIA/ANSI 632 - *Provide an integrated set of fundamental* ***processes to aid a developer*** *in the engineering or re-engineering of a system*

IEEE 1220 - *Provide a standard for* ***managing systems engineering***

Source : Draft Report ISO Study Group May 2, 2000

Network Defense Model

Network Defense Infrastructure Estimating Model	
Conceptualize	See Figure 6
Development	See Figure 6
Operational Test & Evaluation	Effort $_{OT\&E}$ (PM) = Effort $_{function\ (no.\ of\ test\ scenarios\ required\ for\ acceptance)}$ (PM) (see Page 8) Duration $_{OT\&E}$ (CM)= function (effort and available schedule time)
Transition to Operations	Effort $_{Turnover}$ (PM) = Effort $_{Transition}$ (PM) + Effort $_{DITSCAP}$ (PM) Where: Effort $_{Transition}$ = Estimated Level-of-Effort based on available manpower Effort $_{DITSCAP}$ = Estimated Level-of-Effort based on past experience (see Page 8) Duration $_{Turnover}$ (CM) = Fixed at one year for transition and eighteen months for DITSCAP
Operate & Maintain	Effort $_{O\&M}$ (PM) = Effort $_{Ops}$ (PM) + Effort $_{Maintenance}$ (PM) Where: Effort $_{Ops}$ = Estimated Level-of-Effort based on budgeted manpower (see Page 9) Effort $_{Maintenance}$ = Estimated using code fragment changed model + additional inputs to accommodate COTS packages + hardware repairs, updates and replacement + recertification costs (see Page 9) Duration $_{O\&M}$ (CM) = Fixed on a annual basis for operations and release plans for maintenance
Replace (or Destroy)	Effort $_{Replace}$ (PM) = Effort $_{function\ (system\ size)}$ (PM) + Effort $_{Recertify}$ (PM) (see Page 8) Where: Effort $_{Recertify}$ = Estimated Level-of-Effort based on no. of requirements and availability of regression tests and test scripts Duration $_{Replace}$ (CM) = function (effort) and upgrade plans

PM = Person Month
CM = Calendar Month

Rules of Thumb for Network Defense Model for Effort Estimation

Life Cycle Phase	Parameter Computed	Rules of Thumb		
Operational Test & Evaluation	Effort $_{OT\&E}$ (PM) Effort Range = function (difficulty)	**Small** 1 to 10 scenarios **4 to 6 PM**	**Moderate** 11 to 25 scenarios (assume that operational test & evaluation is highly automated) **8 to 12 PM**	**Large** Over 25 scenarios **18 to 24 PM**
Transition to Operations	Effort $_{DITSCAP}$ (PM) Effort Range = function (difficulty)	**Limited** Self contained , little external agency coordination, informal customer test and acceptance **8 to 12 PM**	**Average** Some external coordination, formal test and acceptance **24 to 36 PM**	**Extensive** Lots of external coordination, tests witnessed by and very formal **48 to 60 PM**
Replace (or Destroy)	Effort $_{f\,(system\ size)}$(PM) Effort Range = function (difficulty)	**Small** ≤ 1K requirements **6 to 8 PM**	**Moderate** Between 1 and 10K system requirements **12 to 18 PM**	**Large** > 10K requirements **18 to 24 PM**
	Effort $_{Recertify}$ (PM) Effort Range = function (difficulty)	**Small** < 10 tests **4 to 6 PM**	**Moderate** 10 to 50 tests (assume that recertification testing is highly automated) **8 to 12 PM**	**Large** More than 50 tests **18 to 24 PM**

Network Defense Early Phase Cost Model

Size
- -No of requirements
- -No. of interfaces
- -No. of operational scenarios
- -No. of critical algorithms
- -No. of false alarms
- -+ **Volatility Factor**

$$\text{Effort} = A\,(B)\prod_{i=1}^{12} D_i\,(\text{Size})^{C}$$

Effort (PM)
Duration (CM)

Calibration

Duration = Function (Effort)

Where Effort = All hours to perform engineering tasks (requirements, architecture, development, test and integration; includes task management, in PM (152 hours/month))

A = Calibration constant
B = Architecture constant (see Page 13)
C = Power law
D_i = Cost Drivers Where: $\prod D_i$ = product of their ratings
Size = No. of weighted predictors scaled for a given false alarm rate

See descriptions for cost drivers on following pages

Note: The model takes the form of a regression model. We are currently working with our collaborators to reduce the number of cost drivers to the set that captures the variations in effort as noted by our experts. The size drivers are taken from the COSYSMO model as representative of systems comprised of both hardware and software components. Acquisitions are excluded and their costs must be added to the estimates generated.

Architectural Constant

Architecture Constant (B): ***A constant used to adjust the model to reflect the following range of network defense requirements/architectures.***

Architecture	Description	Value
No defenses	Maybe a firewall, but that is it	1.22
Basic defenses	Hardware firewall; router authorization; OS patches up-to-date; local authentication	1.11
Standard defenses	Basic plus IDS; network scanner to identify intrusions; log files analyzed ; system swept to identify vulnerabilities	1.00
Advanced defenses	Standard plus DMZ configuration; IPS; layered defenses aimed at identifying and recovering from insider & outsider attacks	0.91
State-of-the-art defenses	Advanced plus proxy server configuration; defense-in-depth with active alerts on situation displays; honeypots for forensics	0.84

Delphi Round 1 Results

	Conceptualize	Develop	OT&E	Transition to Operations	Operate, Maintain or Enhance	Replace of Dismantle
% of Total SE Effort	10%	20%	15%	20%	20%	15%
Delphi results	10%	15%	20%	20%	25%	10%

Architectural Constant	Initial Value	Delphi Value
• No defenses	1.22	1.25
• Basic defenses	1.11	1.10
• Standard defenses	1.00	1.00
• Advanced defenses	0.91	0.90
• State-of-the-art defenses	0.84	0.80

Values provided by experts change values only slightly.

Size Drivers (Network Defense)

- **No. of System Requirements**
  - Represents the weighted number of network defense requirements in system-of-interest at a specific level of design. Requirements may be functional, performance, feature or service-oriented in nature depending on specification methodology.
- **No. of Major Interfaces**
  - Represents the weighted number of shared major physical and logical boundaries between network defense system components or functions (internal interfaces) and those external to the system (external interfaces).
- **No. of Operational Scenarios**
  - Represents the weighted number of operational scenarios that the network defense system must satisfy. Such threads typically result in end-to-end tests that are developed to validate the system satisfies all of its requirements.
- **No. of Critical Algorithms**
  - Represents the weighted number of newly defined or significantly altered functions that require unique mathematical algorithms to be derived to achieve the network defense system performance requirements.

Number of False Alarms

- **No. of False Alarms (quality normalization factor)**
  - Sets the false alarm goal for the network defense system. This is the cumulative number of false alarms per day that are displayed on situational awareness consoles.
  - False alarm rate used as a weighting factor for the size driver summation.

$$\text{Size} = (\text{Weighting Factor}) \sum w_i \, SD_i$$

Number of False Alarms	Description	Weighting Factor
Very Low	No. of false alarms less than one per day on average	0.75
Low	No. of false alarms less than two per day on average	0.87/**0.90**
Nominal	No. of false alarms between two and five per day during nominal traffic load on the network	1.00
High	No. of false alarms between five and eight per day on average	1.35/**1.30**
Very High	No. of false alarms greater than eight per day	1.56/**1.70**

Size Drivers – Delphi Results

- Lots of confusion over these parameters
  - Relative effort relates to what it takes to implement network defense requirements
- Drivers of interest include: Relative Effort
  - Number of system requirements 1/1
  - Number of major interfaces 4/2
  - Number of operational scenarios 10/10
  - Number of algorithms 6/6

(relative effort relates to the effort expended for requirements; e.g., scenarios take ten times the nominal effort for requirements)

- Ranges for drivers
  - Improperly filled out Need to better define

Cost Driver Definitions (12)

- **Architectural Understanding**
  - This driver rates the relative difficulty of determining and managing the network defense architecture in terms of platforms, standards, components, connectors (protocols), and constraints.
- **Degree of Innovation**
  - This driver rates the ability of the team to innovate when implementing designs aimed at satisfying overarching security requirements and constraints for network defense.
- **Level of Service Requirements**
  - This driver rates the difficulty of satisfying critical performance goals for the system like security, interoperability, response time, etc. as network defenses are mounted and all aspects of the infrastructure are enabled. Often these are expressed as Key Performance Parameters.
- **Migration Complexity**
  - Rates the complexity of migrating components, databases, procedures and workflows to the new network defense architecture.

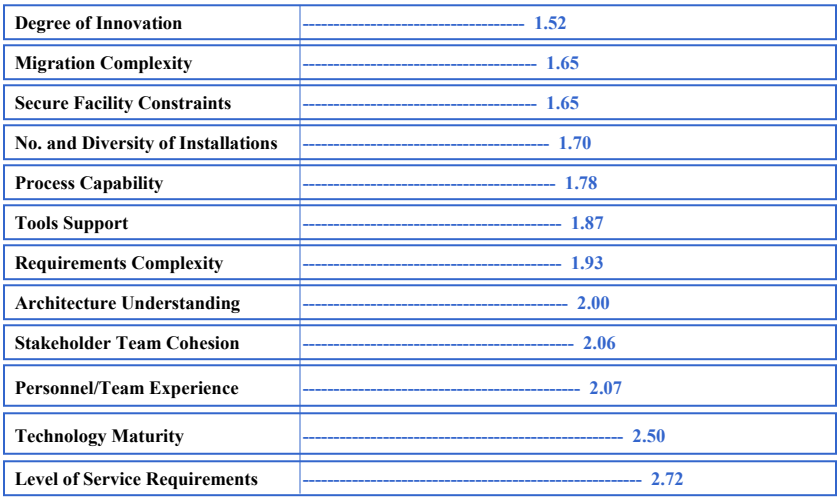
Driver Definitions (Continued)

- **Number and Diversity of Vendor Products & Platforms/ Installations**
  - Rates the ability to mount defenses based on the number of vendors products being used and platforms/installations that need to be defended.
  - Effort tends to increase non-linearly as number of vendors/platforms increases.
- **Personnel/Team Experience**
  - Rates the capabilities and experience of the security team when implementing defenses similar to those being proposed for the network.
- **Process Capability**
  - Rates the effectiveness and robustness of the processes used by the security team in establishing the network infrastructure defenses.
- **Requirements Complexity**
  - Rates the precedentedness, difficulty and volatility of the overarching requirements established for network defense (common criteria assurance and functional levels, etc.).

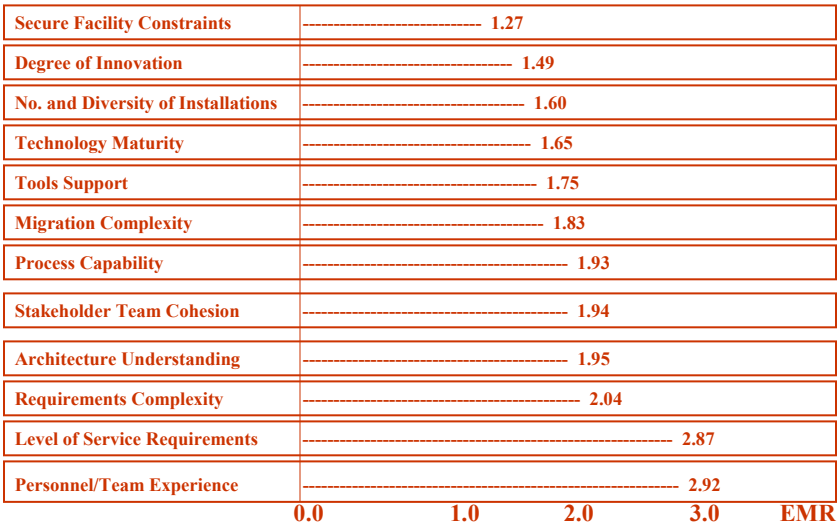
Driver Definitions (Completed)

- **Secure Facility Constraints**
  - Rates the difficulty of performing work as a function of physical security constraints placed on the team implementing network security (cipher locks, guards, security processes, etc.).
- **Stakeholder Team Cohesion**
  - Rates the degree of shared vision and cooperation exhibited by the different organizations working on security the network infrastructure (customer, developer, auditor, etc.).
- **Technology Maturity**
  - Rates the relative maturity of the technology selected for use in the defense of the network using NASA's Technology Readiness Levels.
- **Tools Support**
  - Rates the coverage, integration and maturity of the tools used, both hardware and software, to mount network defenses (includes test automation for revalidating defenses once they are changed).

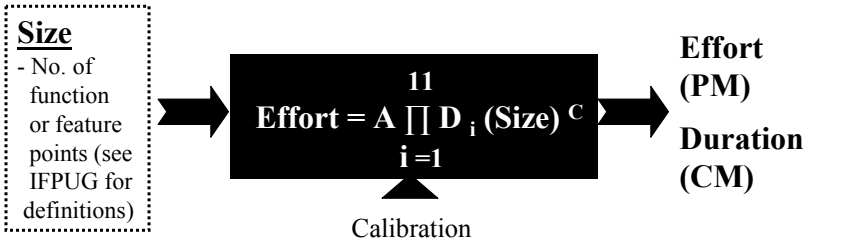
EMR Results (Collaborator Group)



EMR Results (Delphi Round 1)



Anti-Tamper Early Phase Cost Model



Where Effort = all hours to perform engineering tasks in PM (152 hours/month)
A = calibration constant
C = power law
∏ D i = product of their ratings
D i = cost drivers (see amplifying description for each of the drivers)
Size = effective size of the application being protected

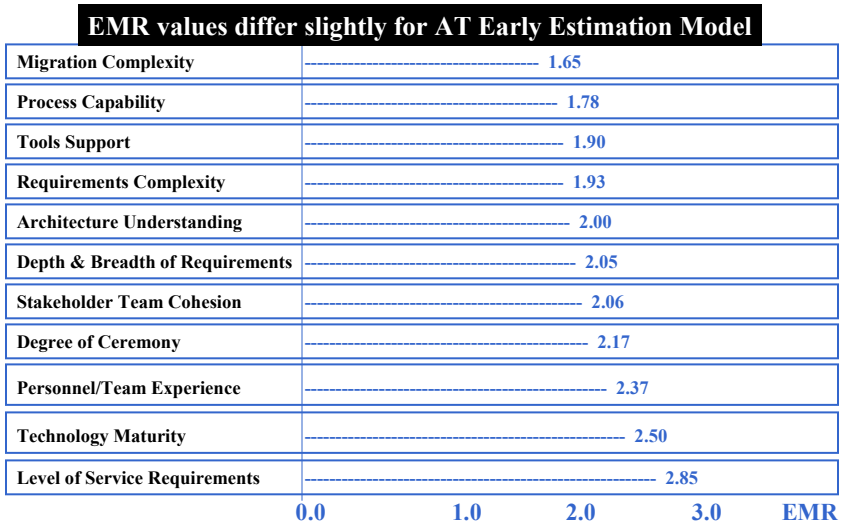
Candidate Cost Drivers for Anti-Tamper Early Phase Cost Model

Cost Drivers	
• Architecture Complexity	• Process Capability
• Degree of Ceremony	• Requirements Complexity
• Depth and Breadth of Protection Requirements (in PPP)	• Stakeholder Team Cohesion
• Level of Service Requirements	• Technology Maturity
• Number and Diversity of Platforms/ Installations	Tools Support (for protection)
• Personnel/Team Experience	

AT Unique Cost Drivers

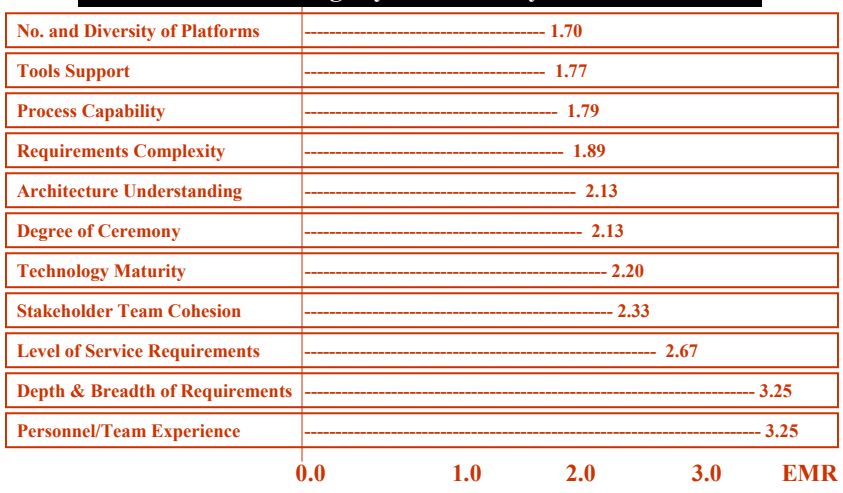
- **Degree of Ceremony**
  - Rates the formality in which the team operates during development, testing, red teaming and DITSCAP certification. Ratings are a function of support that needs to be provided along with documentation.
- **Depth and Breadth of Protection Requirements**
  - Rates the breadth and depth of protection required in terms of how much protection, both hardware and software, must be mechanized to satisfy the requirements in the Program Protection Plan.
- **Tool Support (for protection)**
  - Rates the degree of coverage, integration and maturity of the tools used, both hardware and software, to mechanize protection (includes the test automation available for revalidating protection once the defenses are changed for whatever reason).

EMR Results (Collaborators Group)



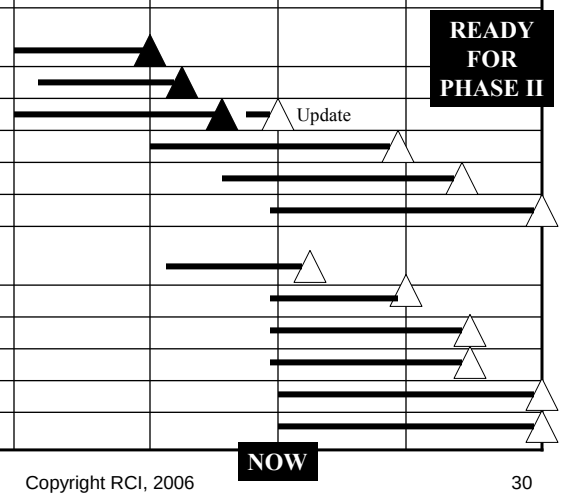
EMR Results (Round 1 Delphi)

EMR values differ slightly for AT Early Estimation Model



Next Steps – CY2006 Schedule

Task	1st Quarter	2nd Quarter	3rd Quarter	4th Quarter
Model Development				
1. Define drivers				
2. Develop counting rules				
3. Rate drivers via Delphi				
4. Develop model definition manual				
5. Build spreadsheet model				
6. Calibrate prototype model				
Data Collection				
1. Develop data collection questionnaire				
2. Test questionnaire utility via trial use				
3. Capture data				
4. Build Excel database				
5. Statistically analyze data				
6. Calibrate model and its parameters				



Issues Raised in Round 1

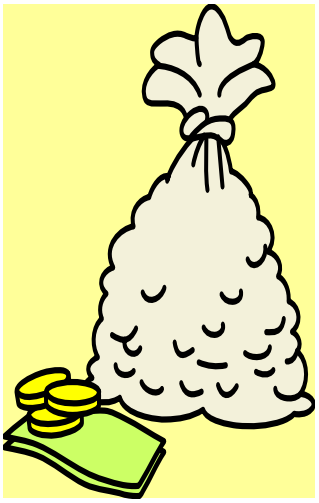
- Many security products used commercially are COTS
  - Security considerations must be included as an integral part of the COTS selection, tailoring and integration processes
  - May have to have to add new scenarios to check for malware and test the COTS prior to its usage in the system
- Security team part of systems effort and not separable
  - Only separable effort the security certification and accreditation activity (DITSCAP)
  - May need to look at different teams doing security work (e.g., engineering, operational and certification teams)
  - Hard to determine percent effort and schedule for security
- Number of platforms a function of number of sites the system deployed
  - May want to consider this a size rather than cost driver

More Issues Raised in Round 1

- Process capability should address the certification and accreditation team as well as systems engineering personnel working security issues
- Technology maturity is viewed negatively for security
  - Both maturity and immaturity infers vulnerabilities
- Size driver definitions need to be clearer especially in terms of the impacts of interfaces and operational scenarios
- False alarms is a good normalization factor to use for the model
- Risk should be assessed from a security risk tolerance point-of-view (normally little allowed)

Future Needs/Challenges

- Getting people to talk, share ideas, provide data and collaborate
  - Often close-mouthed due to classification issues
- Access to real data for use in validating model
- Winning a Phase II support
  - Must acquire a steady stream of funds for several years of data collection



Data Safeguarding Procedures

- Data identification
  - Only collaborator & I know the OID (XXX) and only affiliate knows PID (YYY)
- Data storage
  - Stand-alone computer with no access to the network
  - In a file with cipher lock & limited access
- Data access
  - Non-disclosure agreements will be signed
  - Controlled access to data by researchers (US Citizens only)

What Are We Doing Next?

- Complete the questionnaire
  - Ask questions when in doubt
  - Provide your best guess relative to answers
  - Collaborate if you are from same company
  - Help us finalize the initial model
- Conduct a post-mortem aimed at making the model clearer
  - Issues will be addressed in model definition manual

Backup

Number of System Requirements

Requirements are the Basis for Size

Number of System Requirements

This driver represents the weighted number of requirements for the network defense system-of-interest at a specific level of design. Requirements may be functional, performance, feature, or service-oriented in nature depending on the methodology used for specification. They may also be defined by the customer or contractor. System requirements can typically be quantified by counting the number of applicable "shall's" or "will's" in the system specification for the defensive system. Do attempt to capture all of the requirements. Do not attempt to include a requirements expansion ratio – only provide a count for the requirements of the system-of-interest as defined by the system specification for the network defense system.

Easy	Nominal	Difficult
- Well specified	- Loosely specified	- Poorly specified
- Traceable to source	- Can be traced to source with some effort	- Hard to trace to source
- Little requirements overlap	- Some overlap	- High degree of requirements overlap

Weights

Number of Major Interfaces

Number of Major Interfaces

This driver represents the weighted number of shared major physical and logical boundaries between network system components or functions (internal interfaces) and those external to the system (external interfaces). These interfaces typically can be quantified by counting the number of interfaces identified in either the system's context diagram and/or by counting the significant interfaces in all applicable Interface Control Documents. Typically such interfaces represent gateways to other networks with which the defended network must communicate with.

Easy	Nominal	Difficult
- Well defined	- Loosely defined	- Ill defined
- Uncoupled	- Loosely coupled	- Highly coupled
- Cohesive	- Moderate cohesion	- Low cohesion
- Well behaved	- Predictable behavior	- Poorly behaved

Weights

Number of Operational Scenarios

Number of Operational Scenarios

This driver represents the weighted number of operational scenarios that a network defense system must satisfy. Such threads typically result in end-to-end test scenarios that are developed to validate that the system satisfies all of its requirements. The number of scenarios can typically be quantified by counting the number of unique end-to-end tests used to validate the system functionality and performance or by counting the number of high-level use cases developed as part of the operational architecture. If DITSCAP is required, the number of end-to-end tests necessary to get ready for such testing in the OT&E and transition to operations phases of the life cycle must be included in the count.

Easy	Nominal	Difficult
- Well defined	- Loosely defined	- Ill defined
- Loosely coupled	- Moderately coupled	- Tightly coupled or many dependencies/conflicting requirements
- Timelines not an issue	- Timelines a constraint	- Tight timelines through scenario network

Weights

Number of Unique Algorithms

Number of Critical Algorithms

This driver represents the weighted number of newly defined or significantly altered functions that require unique mathematical algorithms to be derived in order to achieve the network defense system performance requirements. As an example, this could include algorithms being derived to reduce the number of false positives being detected via the intrusion detection system. As another example, it would include fuzzy logic filters used to identify incidences which require immediate responses. The number can be quantified by counting the number of unique algorithms needed to support each of the math functions specified in the system specification or other documents.

Easy	Nominal	Difficult
- Existing algorithms	- Some new algorithms	- Many new algorithms
- Basic math	- Algebraic by nature	- Difficult math (calculus)
- Straightforward structure	- Nested structure with decision logic	- Recursive in structure with distributed control
- Simple data	- Relational data	- Persistent data
- Timing not an issue	- Timing a constraint	- Dynamic, with timing issues
- Library-based solution	- Some modeling involved	- Simulation and modeling involved

Weights

Number of False Alarms

- **No. of False Alarms**
  - Sets the false alarm goal for the network defense system. This is the cumulative number of false alarms per day that are displayed on situational awareness consoles.
  - False alarm rate used as a weighting factor for the size driver summation.

$$\text{Size} = (\text{Weighting Factor}) \sum w_i \, SD_i$$

Number of False Alarms	Description	Weighting Factor
Very Low	No. of false alarms less than one per day on average	0.75
Low	No. of false alarms less than two per day on average	0.87
Nominal	No. of false alarms between two and five per day during nominal traffic load on the network	1.0
High	No. of false alarms between five and eight per day on average	1.35
Very High	No. of false alarms greater than eight per day	1.56

Cost Driver Candidates for Network Defense Early Phase Cost Model

Cost Drivers	
• Architecture Understanding	• Process Capability
• Degree of Innovation	• Requirements Complexity
• Level of Service Requirements	• Secure Facility Constraints
• Migration Complexity	• Stakeholder Team Cohesion
• Number and Diversity of Platforms/Installations	• Technology Maturity
• Personnel/Team Experience	• Tool Support

Architectural Understanding

Architecture Understanding
This driver rates the relative difficulty of determining and managing the network defense architecture in terms of platforms, standards, components, connectors (protocols), and constraints.

Very low	Low	Nominal	High	Very High
Poor understanding of architecture and components, unprecedented system	Minimal understanding of architecture and components, many undefined areas	Reasonable understanding of architecture and components, some weak areas	Strong understanding of architecture and components, few undefined areas	Full understanding of architecture, familiar system and components
	Defined at the 2nd level of the WBS	Defined at the 3rd to 4th level of the WBS	Defined at the 5th to 6th level of the WBS	Defined at >6th level of the WBS

Degree of Innovation

Degree of Innovation
This driver rates the ability of the team to innovate when implementing designs aimed at satisfying overarching security requirements and constraints established for network defense.

Very low	Low	Nominal	High	Very High
Strictly by-the-book; take no initiative what-so-ever	Innovation is permitted but only as a last resort; policies dictate actions to be performed by network defense system	Management endorses a "by exception" approach to innovation; however, approvals are required before venturing forward.	Innovation is neither encouraged nor discouraged. Bright people are encouraged to excel using guidelines offered by management.	Management encourages balancing agility with discipline; team innovates when the risks are high and there is a high chance that attacker will succeed in penetrating the defenses.

Security personnel take conservative approaches because of the risks involved

Level of Service (KPP) Requirements

Level of Service (KPP) Requirements
This driver rates the ***difficulty*** of satisfying ***critical*** performance goals for the system like safety, security, interoperability, reliability, response time, etc. as network defenses are mounted and all aspects of the infrastructure are enabled.

Viewpoints	Very low	Low	Nominal	High	Very High
Difficulty	Simple	Low difficulty, coupling	Moderately complex, coupled	Difficult, coupled KPPs, some conflicts in realizing goals	Very complex, tightly coupled, many conflicts in realizing goals
Criticality	Slight inconvenience	Easily recoverable losses	Some loss	High financial loss	Risk to human life through losses of critical information about defenses

Typical conflicts that exist occur when the system is trying to realize performance goals in a secure manner

Migration Complexity

Migration Complexity
This driver rates the complexity of migrating components, databases, procedures and workflows to the new network defense architecture.

Viewpoints	Nominal	High	Very High	Extra High
Legacy contractor	Self; legacy system is well documented	Self; original development team not available; most documentation available	Different contractor; limited documentation	Original contractor out of business; no documentation available
Sites/ Installations	Single site; new system; legacy system is completely replaced or non-existent	2 to 3 sites; parallel operation of new and legacy systems required	4 to 5 sites; current operational capabilities cannot be degraded (operate 24/7)	>6 sites; current operational capabilities cannot be degraded (operate 24/7)
Operating environment	Facility meets all security operating requirements	Facility does not meet all security operating requirements	Multiple agency coordination required to be compliant	Multiple agency coordination required to pass certifications
Legacy components retained	0%	<25%	25% to 50%	>50%
Transition down time requirement	Not an issue	1 day or more	Between 1 day and 1 hour	1 second or less

Number and Diversity of Installations/Platforms

Number and diversity of installations/platforms

This driver rates the ability to mount defenses based on the number of vendors products being used and platforms/installations that need to be defended. Effort tends to increase non-linearly as number of vendors/platforms increases.

Viewpoints	Nominal	High	Very High	Extra High
Sites/ installations	Single installation site or configuration	2-3 sites or diverse installation configurations	4-5 sites or diverse installation configurations	>6 sites or diverse installation configurations
Operating environment	Not a driving factor; office environment	Moderate environmental constraints; controlled environment (i.e., air conditioning)	Ruggedized mobile land-based requirements; some information security requirements	Harsh environment (space, sea airborne) sensitive information security requirements
Platforms	< 3 types of platforms being installed and/or being phased out/replaced	4-7 types of platforms being installed and/or being phased out/replaced	8-10 types of platforms being installed and/or being phased out/replaced	>10 types of platforms being installed and/or being phased out/replaced
	Homogeneous platforms	Compatible platforms	Heterogeneous, but compatible platforms	Heterogeneous, incompatible platforms
	Typically networked using a single industry standard protocol	Typically networked using a single industry standard protocol and multiple operating systems	Typically networked using a mix of industry standard and proprietary protocols; single operating systems	Typically networked using a mix of industry standard protocols and proprietary protocols; multiple operating systems

Personnel/Team Experience

Personnel/Team Experience

This driver rates the ***capabilities*** and **experience** of the security team when implementing network defenses similar to those being proposed for the network.

Viewpoints	Very low	Low	Nominal	High	Very High
Capability	15th percentile	35th percentile	55th percentile	75th percentile	90th percentile
Experience	< 6 months to 1 year of continuous experience	1 to 3 years continuous experience, other related experience in similar job	3 to 5 years of continuous experience	5 to 10 years of continuous experience	> 10 years of continuous experience

Experience cited deals with setting up, operating and enhancing network defenses for system of similar size and complexity.

Process Capability

Process Capability
This driver rates the ***effectiveness*** and ***robustness*** of the processes used by the security team in establishing the network infrastructure defenses.

Viewpoints	Very low	Low	Nominal	High	Very High	Extra High
Effectiveness	Ad hoc processes employed	Basic network admin processes	Project establishes its own processes and defensive infrastructure	Organization has defined processes and provides support for those who use them to build defensive infrastructures	Processes are continually improved using quantitative feedback based on metrics to enhance defenses	Processes are being continuously optimized and improved using statistical process control techniques
Robustness	Robustness not a consideration	Robustness a function of customer requirements	Robustness of processes driven by company policies and customer requirements	Robustness a process design consideration; feedback on what works and what doesn't used to update processes	Robustness determined using metrics; processes continually reworked to optimize them	Robustness determined using statistical process control techniques; processes continuously reworked to optimize them

Requirements Complexity

Requirements Complexity
Rates the ***precedentedness***, ***difficulty*** and ***volatility*** of the overarching requirements established for network defense (common criteria assurance and functional levels, etc.).

Viewpoints	Very low	Low	Nominal	High	Very High	Extra High
Precedentedness	Thoroughly familiar	Largely familiar	Somewhat familiar	Generally unprecedented	Largely unprecedented	Thoroughly unprecedented
Difficulty	Requirements embrace tried and true solutions	Requirements embrace state-of-practice solutions	Requirements embrace state-of-the-art solutions	Challenges exist in satisfying requirements which are often overlapping and complex	Large degree of difficulty in satisfying often overlapping and complex set of requirements many of which have not been addressed before	Extremely ambitious set of requirements; pushes the state-of-the-art; performance issues dominate; defenses like this have never been tried before
Volatility	Changes totally under control	Changes anticipated and planned for	Changes managed	Changes frequent and expected, but under control	Changes common and expected, some control	Changes common and expected, but random because unprecedented

Secure Facility Constraints

Secure Facility Constraints
This driver rates the difficulty of performing work as a function of physical security constraints placed on the team implementing network security (cipher locks, guards, security processes, etc.).

Viewpoints	Low	Nominal	High	Very High
Physical Security	Locked doors and desks, when warranted to protect information	Locked area, safes for important documents, reliance on processes and procedures	Cipher locks, biometric readers, guards and other added forms of security	Secure Compartmentalized Facilities (SCF) plus other forms of security rated "High"
Communications	Wide bandwidth, highly interactive, some constraints	Narrow bandwidth, largely interactive, some constraints	Narrow bandwidth, controlled, often constrained	Limited bandwidth, strictly controlled, performed on a strict "need-to-know" basis

Stakeholder Team Cohesion

Stakeholder Team Cohesion
This driver rates the degree of ***shared vision*** and ***cooperation*** exhibited by the different organizations working on security the network infrastructure (customer, developer, auditor, etc.).

Viewpoints	Very Low	Low	Nominal	High	Very High
Shared vision	▪Stakeholders with differing goals, expertise, tasking and cultures ▪ Often hostility and distrust ▪ Limited shared vision	▪Heterogeneous and often cantankerous stakeholder community ▪Shared vision forming	▪Shared project vision	▪Strong team cohesion ▪Shared vision ▪ Vision shaped by common infrastructure (DOD, phone industry, etc.)	▪Virtually homogeneous stakeholder communities ▪Institutionalized security vision and infrastructure
Cooperation	▪ Security roles not fully defined ▪ Uncooperative environment	▪ Security roles cloudy ▪ Low degree of cooperation	▪ Roles overlapping ▪ Some cooperation	▪Clear roles ▪ High degree of cooperation	▪High stakeholder trust level

Technology Maturity

Technology Maturity

This driver rates the relative ***maturity***, ***readiness*** and ***degree of obsolescence*** of the technology selected for use in the defense of the network using NASA's Technology Readiness Levels (TRL's).

Viewpoints	Very Low	Low	Nominal	High	Very High
Maturity	Still in the laboratory	Ready for pilot use	Proven on pilot projects and ready to roll-out for production jobs	Proven through actual use and ready for widespread adoption	Technology proven and widely used throughout industry
Readiness	Concept defined (TRL 3 & 4)	Proof of concept validated (TRL 5)	Concept demonstrated (TRL 6)	Concept qualified (TRL 7 & 8)	Mission proven (TRL 9)
Obsolescence	- Technology is outdated and use should be avoided in new systems - Spare parts supply is scarce	- Technology is stale - New and better technology is on the horizon in the near-term	- Technology is the state-of-the-practice - Emerging technology could compete in future		

Tools Support

Tool Support

This driver rates the degree of ***coverage***, ***integration*** and ***maturity*** of the tools used, both hardware and software, to mount network defenses (includes test automation for revalidating defenses once they are changed).

Viewpoints	Very low	Low	Nominal	High	Very High
Coverage	No protection tools	Simple protection tools	Basic protection toolset (firewalls, authentication, etc.)	Advanced toolset (IDS, encryption, etc.)	State-of-the-art toolset (proxy servers, IPS, identity checks, etc.)
Integration	None	Little	Life cycle integration	Integration with Situation Display	Integration with active forensics
Maturity	N/A	Frequent updates, some bugs	Periodic updates, few bugs	Periodic updates, signatures updated daily, few bugs	Periodic updates, signatures updated actively, few bugs

Cost Driver Results

Note 1: The Effort Multiplier Ratio (EMR) is the ratio of the large value over the small one (i.e., Architecture Understanding EMR is 1.51/0.71 = 2.13)
Note 2: Cost drivers are listed in order of appearance during the first round of the Delphi survey
Note 3: Intermediate values (Low, High, and Very High) were updated as geometric ratios rather than arithmetic differences. EMR's did not change.

Cost Driver	Very Low	Low	Nominal	High	Very High	Extra High	EMR
Architecture Understanding	1.50	1.25	1.00	0.85	0.77		1.95
Degree of Innovation	1.25	1.15	1.00	0.90	0.84		1.49
Level of Service Requirements	0.68	0.85	1.00	1.50	1.95		2.87
Migration Complexity			1.00	1.25	1.50	1.83	1.83
No. and diversity of installations/platforms			1.00	1.20	1.40	1.60	1.60
Personnel/team experience	1.90	1.45	1.00	0.85	0.65		2.92
Process capability	1.35	1.20	1.00	0.90	0.80	0.70	1.93
Requirements complexity	1.43	1.25	1.00	0.90	0.80	0.70	2.04
Secure facility constraints		0.95	1.00	1.10	1.21		1.27
Stakeholder team cohesion	1.55	1.25	1.00	0.90	0.80		1.94
Technology Maturity	1.40	1.20	1.00	0.92	0.85		1.65
Tool support	1.40	1.20	1.00	0.90	0.80		1.75

AT Unique Cost Drivers

- **Degree of Ceremony**
  - Rates the formality in which the team operates during development, testing, red teaming and DITSCAP certification. Ratings are a function of support that needs to be provided along with documentation.
- **Depth and Breadth of Protection Requirements**
  - Rates the breadth and depth of protection required in terms of how much protection, both hardware and software, must be mechanized to satisfy the requirements in the Program Protection Plan.
- **Tool Support (for protection)**
  - Rates the degree of coverage, integration and maturity of the tools used, both hardware and software, to mechanize protection (includes the test automation available for revalidating protection once the defenses are changed for whatever reason).

Degree of Ceremony

Degree of Ceremony
This driver rates the formality in which the team operates during development, testing, red teaming and DITSCAP certification. Ratings are a function of support that needs to be provided along with documentation.

Viewpoints	Low	Nominal	High	Very High
Reviews	No additional reviews required	External reviews by AT PMO	Reviews by demanding external expert review teams	Reviews by NSA and certification authorities
Test & analysis	Normal practices sufficient	Independent testing required	Red teaming required	DITSCAP required
Additional documentation	Normal security documentation sufficient	Added AT documentation in terms of PPP plus reports	Some additional documentation required	Extensive additional documentation required

Depth and Breadth of Protection Requirements

Depth and Breadth of Protection Requirements
This driver rates the Rates the ***depth*** and ***breadth*** of protection required in terms of how much protection, both hardware and software, must be mechanized to satisfy the requirements in the Program Protection Plan.

Viewpoints	Low	Nominal	High	Very High
Depth	Only classified data needs protection	Software data, designs and algorithms need protection at binary level	Hardware and software design requires nominal protection at all levels	Hardware and software design requires extensive protection at all levels
Breadth	Protection functions only within memory	Protection functions at interconnects and within memory	Protection at board level, within interconnects and for memory	Protection at all levels of design required, both active and passive

Tool Support (for Protection)

Tool Support
This driver rates the degree of ***coverage***, ***integration*** and ***maturity*** of the tools used, both hardware and software, to mechanize protection (includes the test automation available for revalidating protection once the defenses are changed for whatever reason).

Viewpoints	Very low	Low	Nominal	High	Very High
Coverage	No protection tools	Simple protection tools	Basic protection toolset (agents, guards, sneaks, etc.)	Advanced toolset (active response using signatures and footprints)	State-of-the-art toolset (active response plus forensics to gather evidence)
Integration	None	Little	Life cycle integration	Integration across platforms	Integration with active alert capability
Maturity	N/A	Frequent updates, some bugs	Periodic updates, few bugs	Updates with releases, few bugs	Updates in stealth mode, few bugs

Cost Driver Results

Note 1: The Effort Multiplier Ratio (EMR) is the ratio of the large value over the small one (i.e., Architecture Understanding EMR is 1.51/0.75 = 2.00)
Note 2: Cost drivers are listed in order of appearance during the first round of the Delphi survey
Note 3: Intermediate values (Low, High, and Very High) were updated as geometric ratios rather than arithmetic differences. EMR's did not change.

Cost Driver	Very Low	Low	Nominal	High	Very High	Extra High	EMR
Architecture Understanding	1.60	1.30	1.00	0.88	0.75		2.13
Degree of Ceremony		0.92	1.00	1.45	2.00		2.13
Depth and Breadth of Protection Requirements			1.00	1.75	3.25		3.25
Level of Service Requirements	0.75	0.88	1.00	1.50	2.00		2.67
No. and diversity of installations/platforms			1.00	1.25	1.50	1.70	1.70
Personnel/team experience	1.95	1.50	1.00	0.85	0.60		3.25
Process capability	1.25	1.12	1.00	0.92	0.81	0.70	1.79
Requirements complexity	1.42	1.25	1.00	0.90	0.83	0.75	1.89
Stakeholder team cohesion	1.75	1.40	1.00	0.88	0.75		2.33
Technology Maturity	1.65	1.35	1.00	0.82	0.75		2.20
Tool support (for protection)	1.45	1.25	1.00	0.91	0.82		1.77