

# Practical Enterprise Assurance

by: **Paul J. Perrone**  
**pperrone@assuredtech.com**

Paul J. Perrone is the Founder, President and a Consultant for Assured Technologies, Inc. in Leesburg, Virginia.

There are two key conflicting goals often confronting a corporation involved with the development of software for enterprise systems. On the one hand, a corporation is typically under the gun to deploy a product or deliver a release of their software to meet either a contractual deadline or time-to-market demand. On the other hand, corporations are also faced with deploying or delivering their software according to certain standards of software assurance for security, reliability, availability, maintainability, and sometimes for safety. A myopic focus on time-to-market deployment may be at the cost of software assurance. Similarly, certain rigid procedures for providing software assurance may be followed at the cost of not delivering a system or perhaps even losing market share. Failure to satisfy either goal involves a cost to the corporation. Assessing these costs is often subjective, usually political, always non-trivial, and frequently not done at all.

## A Dilemma of Assurance and Delivery Costs

Costs associated with failing to deliver a system to a customer or perhaps failing to place some product into the marketplace in a timely fashion can often be devastating for a corporation. A delay reaching the marketplace before the competition can lead to irrecoverably lost market share. Missed deadlines and frequent delays for delivery to customers can lead to lost contracts, fees, and exposure to legal liability.

Such delivery pressures can force corporations to compromise on the time needed to employ effective software assurance measures. Yet, failure to meet acceptable levels of software assurance can also cost the corporation. A diminished future revenue base can result from prospective customer awareness of software assurance failures. Assurance failures will be even more likely to directly affect the satisfaction of current customers using the problematic software and thus may lead to a more imminent loss of revenue. Failure to develop a maintainable product can cost the corporation by making future development extensions and product growth very costly and prohibitive. Security holes or safety-related software failures can lead to direct costs via exposure to legal liability. Security and safety related failures could also have more significant intangible costs via harm to human beings, other living things, and the environment.

Of course there are also costs for accomplishing assurance goals too. Providing for enterprise systems assurance involves a cost for analyzing problems and weaknesses as well as designing, implementing, testing, validating, deploying, and maintaining assurance solutions.

The question before the corporation is one of minimizing overall cost given the goals of assurance versus time-to-market. In rapid development or time-to-market sensitive scenarios, decisions which trade-off delivery time and assurance implementation are usually based on gut feelings and past experiences. These are particularly problematic compromises for the development of distributed enterprise systems that frequently affect many users and significant amounts of corporate resources.

## General Assurance Process

The diagram in Figure 1 depicts a high-level overview of a process for providing enterprise software assurance. This process can be generally applied to all forms of software assurance including assurance for security, reliability, availability, maintainability, and safety. The general flow involves the identification of assurance problems with a system or product, assessing the risk of these problems, generating risk reduction plans, and then assessing the residual risk with such plans in place as well as the cost of the risk reduction plan. While many assurance processes recommend rigid rules, expensive procedures, and expensive tools for accomplishing many of these steps, the corporation experiencing complicated delivery time constraints and lacking any significant assurance program in place may need to employ a simplified

procedure. Specifically, such corporations may decide to simply capture intermediate process results and information in a series of simple technical memos or perhaps establish a simple data repository.

The inputs to such an assurance process of most use are typically previous project expertise and data on assurance issues. Of course system and product technical data for the current system or product under analysis must be utilized for specific determination of assurance issues. Outside expertise and information on potential assurance pitfalls may also be utilized.

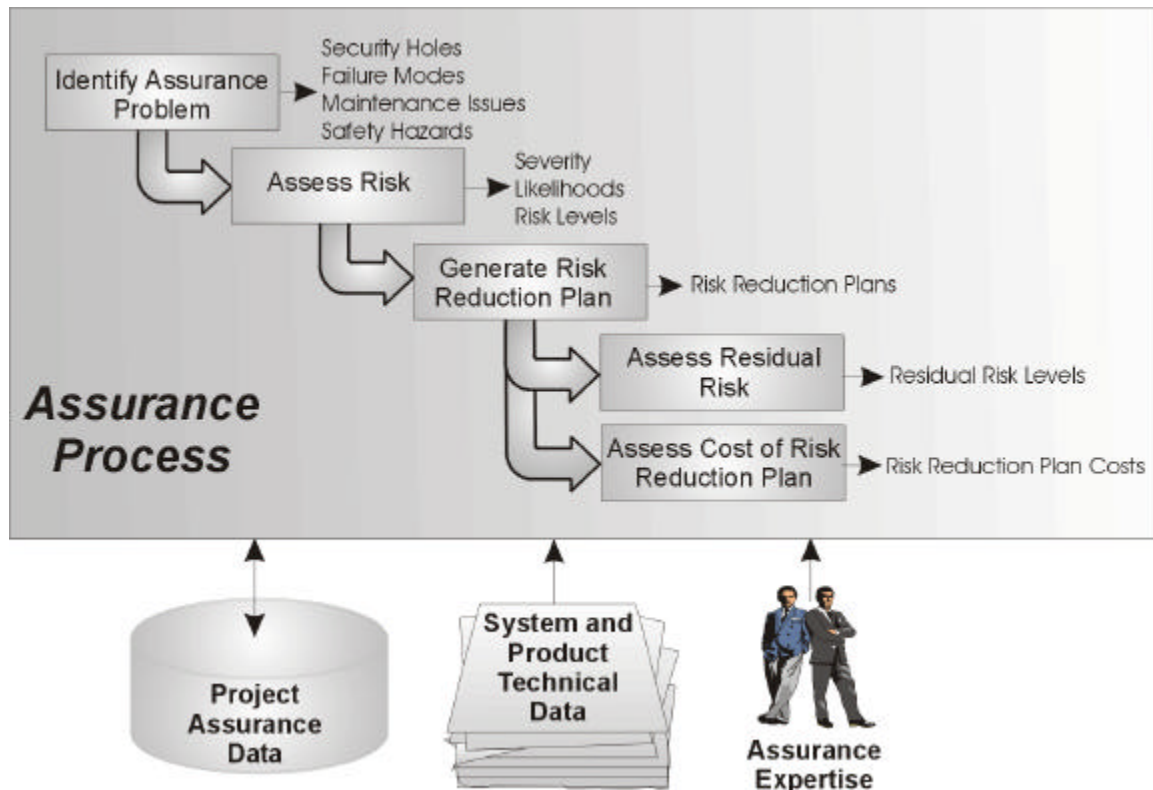


Figure 1. General Assurance Process

### Identify the Assurance Problem

There are a variety of techniques for identifying assurance issues. However, with the use of previous project assurance data, system and product technical data, and perhaps some outside assurance mentoring, a practical solution for many corporations is to simply direct their technical engineering staff to identify potential assurance problems via the generation of technical memos. Depending on the size of the project, one or more project members on a part-time basis can help collect this data into a centralized repository and help coordinate the timely flow of the remaining assurance process steps. An identified assurance problem should be expressed in terms of one or more causes that lead to one or more possible effects. Assurance problems needing identification by the technical staff are:

- **Security Problems:** Security holes, weaknesses, and potential threats.
- **Reliability Problems:** Potential failure modes, potential bottlenecks, and code usage assumptions.
- **Availability Problems:** Potential single points of failure, denial of service possibilities, scalability concerns, and code usage assumptions.
- **Maintainability Problems:** Difficult to maintain designs, code dependencies, code modules lacking encapsulation, software configuration, processing distribution, and extensibility to future demands.
- **Safety Problems:** Hazardous scenarios, safety-critical code modules, and fail-safe components.

## Assess Risk

Upon identification of an assurance problem, a risk assessment should be performed. This is often difficult for corporations under the rapid development gun due to a lack of resources for gathering and assembling meaningful concrete data and statistics. Thus, the best way for many corporations to assess such risk is to employ a simplified set of evaluation steps as follows:

- Evaluate Severity:** Severity is the estimated cost of the possible damaging consequences resulting from the effects of an identified assurance problem. These costs should include those associated with lost customer bases due to customer dissatisfaction and bad publicity. The costs associated with any liability arising from such failures and the costs for repairing problems that occur should also be incorporated. Often, the easiest way to quickly categorize such costs is to utilize a set of qualitative severity levels whereby each level corresponds to a range of approximate cost values. Four to five severity levels are often resolute enough for most projects.
- Evaluate Assurance Failure Likelihood/Rate:** The likelihood of an identified assurance problem leading to an actual failure per base operational unit of time should also be estimated. This likelihood can be partitioned into two distinct likelihood estimates: 1) the likelihood that an assurance problem will be realized or exposed and 2) the likelihood that such an exposed problem will lead to the actual failure that results in the aforementioned severity cost. Five qualitative likelihood levels are usually sufficient for estimating each distinct likelihood type. The two distinct likelihood levels can then be combined (i.e. multiplied) into a single assurance failure likelihood and subsequently cast in terms of a failure rate level.
- Evaluate Assurance Failure Occurrence:** The assurance failure likelihood level previously identified assumed a base operational unit of time and can be expressed in terms of a failure rate level. The more time a system is spent in operation, the greater amount of risk exposure exists for any potential assurance problem to be revealed. This operational time includes the duration that a system is spent in operation including all user instances of the deployed system. The assurance failure occurrence level over an established operational time can be determined by multiplying the assurance failure rate level by the assumed operational time for the deployed system.
- Evaluate Risk Level:** The risk level of an identified assurance problem may be estimated by multiplying the severity by the estimated number of assurance failure occurrences. A risk assessment decision matrix is best employed here to generate risk levels via the intersection of a particular severity level with the estimated assurance failure occurrences as demonstrated in Figure 2. More severity levels or likelihood/occurrence levels may be employed for finer-grained risk level assignment. Confidence levels in severity and likelihood estimates may also be incorporated into the risk assessment process whereby a lower confidence level in an estimate will result in a higher risk level. Thus, while one may have higher confidence in a worst-case severity or likelihood estimate, a rough swag that produces a lower likelihood or severity level estimate will have a lower confidence level and may actually result in an equivalent risk level.

Occurrence Level	Severity Level			
	Catastrophic	Critical	Marginal	Negligible
Frequent	Business-Critical (>\$10M)	Business-Critical (>\$10M)	Very High (\$1M - \$10M)	High (\$100K - \$1M)
Probable	Business-Critical (>\$10M)	Very High (\$1M - \$10M)	High (\$100K - \$1M)	Significant (\$10K - \$100K)
Occasional	Very High (\$1M - \$10M)	High (\$100K - \$1M)	Significant (\$10K - \$100K)	Moderate (\$1K - \$10K)
Remote	High (\$100K - \$1M)	Significant (\$10K - \$100K)	Moderate (\$1K - \$10K)	Low (< \$1K)
Improbable	Significant (\$10K - \$100K)	Moderate (\$1K - \$10K)	Low (< \$1K)	Low (< \$1K)

Levels are similar to those exemplified by MIL-STD-882C; Military Standard System Safety Program Requirements; January 19, 1993

**Figure 2. Risk Assessment Decision Matrix Example**

## **Generate Risk Reduction Plan**

Risk reduction planning involves establishing assurance solutions to potential assurance problems. Security measures, code reviews, testing techniques, rollback mechanisms, fail-safe error detection, and component-based development are all examples of techniques employed to provide a higher-assurance system. A key consideration during risk reduction planning is to determine common design guidelines and common assurance frameworks to help provide a reusable platform on top of which a higher assurance system can be provided while minimizing the costs associated with providing assurance.

## **Assess Cost of Risk Reduction Plan**

The cost of the risk reduction plans should be estimated and include any additional expenses needed to commonly apply a plan to similar assurance problems (e.g. extra COTS product licenses). Costs should include expenses for analyzing assurance problems as well as for designing, implementing, testing, deploying, and maintaining assurance solutions. Any assurance costs spent on employing assurance expertise should also be evaluated and incorporated into the overall risk reduction plan cost. However, any additional time required by non-experts for developing risk reduction plans to account for learning curve time should be considered when generating the cost of internal plan development. Thus, it may pay to have assurance expertise with breadth of enterprise development experience and offering assurance as part of an overall package rather than risking any conflicts of interest or wasted resources for providing costly assurance solutions in scenarios where time-to-market will deem it impractical.

## **Assess Residual Risk**

Putting an assurance plan in place will often not completely negate an assurance problem. Thus, the residual risk remaining even with assurance mechanisms in place via proposed risk reduction plans should be evaluated. The previously defined risk assessment procedures involving severity levels, likelihood levels, and risk levels can be used during these risk assessment steps as well. The severity will often be the same, but the assurance failure likelihood levels and associated risk levels should demonstrate a decrease in risk with the risk reduction plan in place.

## **Failed Delivery Costs**

While there are costs associated with employing assurance and benefits associated with reducing corporate risk, there are also costs associated with delayed and aborted deliveries. These failed delivery costs can also be estimated in terms of a risk level for the corporation.

The delivery severity may be estimated as a function of the costs arising from failing to deliver a system or product on time. These costs may be directly computable from stipulated contractual obligations regarding fees associated with delayed deliveries or missed deadlines. Delivery severity costs may also be associated with the loss of market share resulting from a delayed time-to-market. As can be imagined, these exact quantitative costs will be difficult to assess. The use of qualitative severity levels will be more useful for rapid cost assessment.

The likelihood of a delivery failure should be estimated along with the delivery failure occurrence level. The delivery failure occurrence level can be estimated by multiplying the likelihood of a delivery failure by the number of proposed deliveries associated with the failed delivery severity level. Different deliveries may warrant different severity levels and can be evaluated separately to help determine how risk levels vary per delivery. Finally, the risk level can be generated for a set of failed deliveries via a risk assessment decision matrix, by intersecting the severity level with the occurrence level as in Figure 2.

## **Making Decisions**

The assurance and delivery risk levels and associated costs can now be used to determine the practicality of particular assurance plans. Each individually identified assurance problem will have some assessed initial risk value. For a particular risk reduction plan to be practical, the assessed initial risk must be greater than the sum of the proposed risk reduction plan cost, the residual risk, and the failed delivery risk resulting from potentially pursuing such an assurance plan.

While the truth of this rule can help guide the decision to pursue a particular assurance plan, the falsity of this rule does not necessarily justify ignoring the pursuit an assurance plan. Rather, the reuse of an enterprise assurance plan to address multiple identified risks may be used to make the pursuit of particular plans practical. Thus, a particular risk reduction plan will be practical if the sum of the initially assessed risks for a set of assurance problems is greater than the sum of the proposed plan cost for addressing these problems, the total residual risk, and the risk of failed delivery resulting from the pursuit of the plan.

These procedures help bridge the gap between technical staff, project management, corporate management, and legal departments by providing a common interface language for explaining problems and technical decisions: risk and cost. For example, corporate management may be inclined to give project management risk budgets for constraining the overall allowable assurance risk to be assumed by a project based on the support possible from corporate liability coffers. Project management may also be inclined to give assurance budgets to the project technical staff to constrain the overall cost of assurance plans.

Management can also use such a framework to plan deployment increments. Thus, corporations may decide to ship a product under exposure to an assurance problem for early releases which presumably may be in operation for only a small amount of time relative to longer-term plans for future releases. Another increment or delivery that follows soon thereafter may permit just enough time to reduce the assurance risk via pursuit of an assurance plan while also minimizing future failed delivery cost risk. Consciously or subconsciously, this is the decision process employed by many successful corporations that understand the balance between high-assurance and time-to-market demands.

## **Conclusions**

The identification of assurance problems, initial risk, risk reduction plan proposals, risk reduction plan costs, and residual risks are key steps in providing practical enterprise assurance. This assurance data and the estimated delivery risks associated with pursuing assurance plans can be quickly captured in technical memos or in other data repositories. All of this information can be used by corporations to determine what is most optimal from a business perspective by trading off the pursuit of assurance with the pursuit of deployment. Overall cost can decrease when reuse is achieved from the application of a risk reduction plan to a set of similar assurance problems. All of this analysis information can also provide corporations with a framework for planning releases and identifying when particular assurance problems will be addressed while minimizing failed delivery risk. Practical enterprise assurance helps ensure that corporations work toward optimization for minimal cost and risk.