SOFTWARE EXCELLENCE ACADEMY
WESTFALLTEAM

Risk-Based Peer Reviews

By Linda Westfall

lwestfall@westfallteam.com

Risk-Based Peer Reviews

Risk-based peer reviews focus on the identification of software work products with the highest risk exposure. In risk-based peer reviews, risk probability is the estimated likelihood that a yet undiscovered, important defect will exist in the work product after the completion of the peer review. Multiple factors or probability indicators may contribute to a work product having a higher or lower risk probability. These probability indicators may vary from project to project or from environment to environment. Therefore, each organization or project should determine and maintain a list of probability indicators to consider when assigning risk probabilities to its software work product.

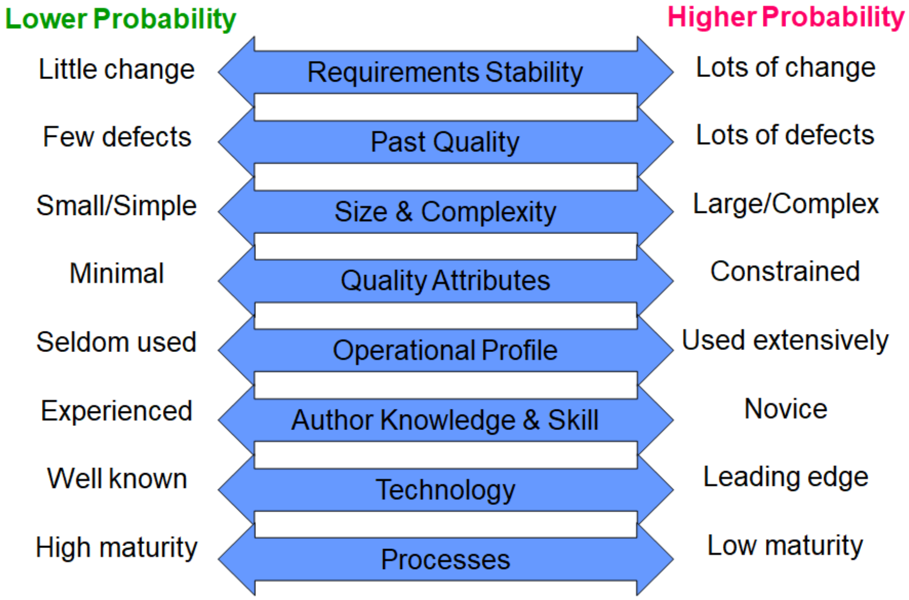


Figure 1: Probability Indicators – Examples

Figure 1 illustrates examples of probability indicators, including:

- Requirements Stability: The more churn there has been in the requirements allocated to the software item, the more likely it is that there are defects in that item

- Past Quality: Software items that have had a history of defects in the past are more likely to have additional defects
- Size and Complexity: Larger and/or more complex software items are more likely to have defects than smaller and/or more simple software items
- Quality Attributes: The higher the constraints on the quality attribute (for example, reliability, performance, safety, security, maintainability), the more likely it is that there are related defects in that software item
- Operational Profile: The more used an item in the software is the more likely it is that the users will encounter any defects that might exist in that part of the software
- Author Knowledge and Skill: Novice software developers with less knowledge and skill tend to make more mistakes than experienced developers resulting in more defects in their work products
- Technology: If the developer is very familiar with the programming language, tool set and business domain they are less likely to make mistakes than if they are working with new or leading-edge technology
- Processes: Higher maturity processes are more likely to help prevent defects from getting into the work products

Risk-based peer reviews also analyze risk impact, which is the estimated cost of the result or consequence if one or more undiscovered defects escape detection during the peer review. Again multiple and varying factors or impact indicators may contribute to a work product having a higher or lower risk impact. Each organization or project should determine and maintain a list of impact indicators to consider when assigning risk impacts to its work products. Examples of impact indicators include:

- Schedule and effort impacts
- Development and testing costs
- Internal and external failure costs
- Corrective action costs
- High maintenance costs
- Customer dissatisfaction or negative publicity
- Lost market opportunities
- Litigation, warranty costs, or penalties
- Non-compliance with regulatory requirements

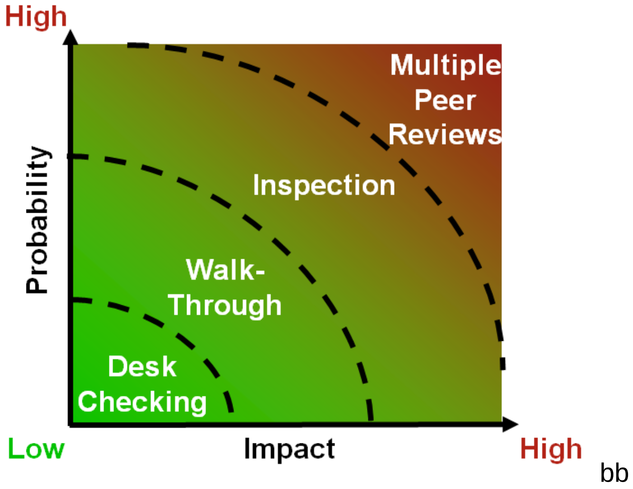


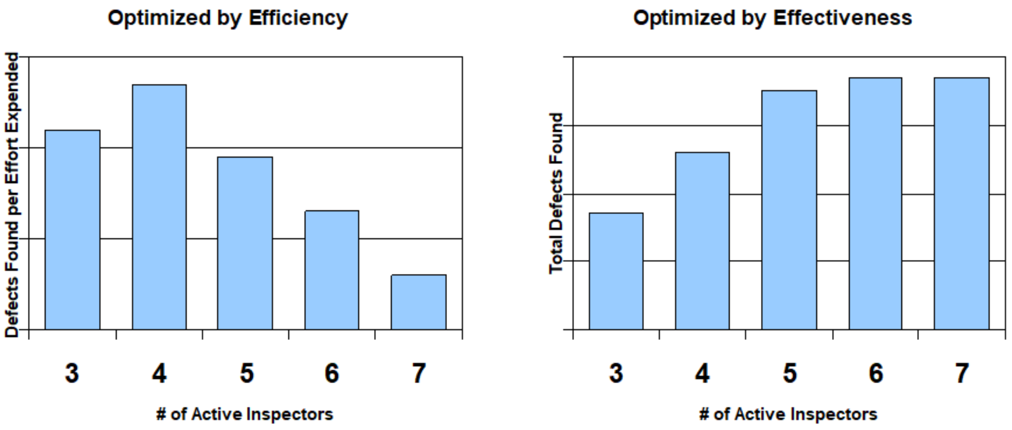
Figure 2: Risk-Based Selection of Peer Review Types

Risk-Based Choices

Once the risk probability and risk impact are analyzed, the risk exposure is determined and used to make risk-based decisions about conducting the peer review. These decisions include:

- **Type of Peer Review and Level of Formality:** As illustrated in Figure 2, if there is both a low probability and a low impact (low-risk exposure), then informal desk checking may be appropriate, as illustrated in Figure 2. As the probability and impact increase, the type of appropriate peer reviews moves from more formal desk checking to informal walk-throughs to more formal walk-throughs to formal inspections. For work products with a very high very high risk, having multiple peer reviews may be appropriate. For example, a product may be desk checked or have a walk-through early in development, and then be inspected late in its development just before it is released.
- **Number of participants**: The number of people performing the peer review may also be varied based on risk. For very low-risk work products, having a single individual perform a desk check may be appropriate. For slightly higher-risk work products, it may be appropriate to have multiple people perform the desk check. For products worthy of an investment in an inspection, less risky work products may be assigned a smaller inspection team of 2-4 people and higher risk products may be assigned an inspection team of 5-7 people.

Metrics from the peer review process can be used to help guide these risk-based decisions. For example, as the metrics in Figure 3 illustrate, an organization determined that their most efficient inspections (defects found per hour) happen with 4-person inspection teams and their most effective inspections (total defects found) happen with 6-person inspection teams. This organization then used 6-person inspection teams for their inspections for work products with very high-risk exposure and 4-person inspection teams on work products with lower risk exposure.



[based on Potter-01]

Figure 3: Optimum Number of Participant Metrics

Another risk-based peer review decision is peer review sufficiency – when to stop peer reviewing. After defects are found and fixed, or improvements are made as a result of holding a peer review, should the work product be peer reviewed again? There is the possibility that not all the defects were found the first time or that new defects were introduced when changes were made. Risk-based peer reviews embrace the "Law of Diminishing Return." When a software work product is first peer reviewed, many of the defects that exist in the product are discovered with little effort. As additional peer reviews are held, the probability of discovering any additional defects starts to decrease. At some point, the return-on-investment (value-add) to discover those last few defects is outweighed by the cost of additional peer reviews. As illustrated in Figure 4, the probability of undiscovered defects still existing in the product and the potential impact associated with those defects must be balanced against the cost of performing additional peer reviews and the benefit of those reviews (just because an additional peer review is held, does not mean that additional defects will be found).

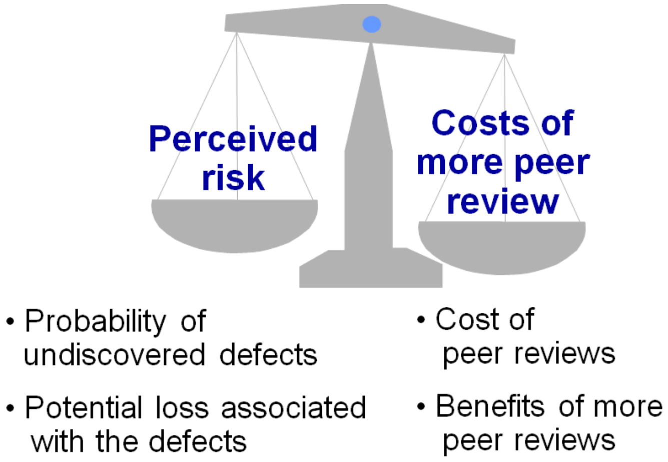

Perceived risk
Costs of more peer review
• Probability of undiscovered defects
• Potential loss associated with the defects
• Cost of peer reviews
• Benefits of more peer reviews

Figure 4: Peer Review Sufficiency

Conclusions

Industry experience shows that peer reviews, especially inspections, are beneficial in improving the quality of our software work products. However, most projects have limited resources and peer reviews are just one of many activities that have to be accomplished within those limitations. By using a risk-based approach to selecting the type of peer reviews we hold, their level of formality, the number of participants, and the peer review sufficiency needed for each work product, we can focus our resource investments where we can receive the highest return in improved quality and avoid overkill by expending resources where they are not value-added.

References

Gilb-93 Tom Gilb, *Software Inspections*, Addison-Wesley, Wokingham, England, 1993.

Potter-01 Neil Potter and Mary Sakry, *Inspection Moderator Training*, The Process Group, 2001.

Westfall-08 Linda Westfall, *The CSQE Handbook 2nd Edition*, Quality Press, 2017.

Wieger-02 Karl Wieger, *Peer Reviews in Software*, Addison-Wesley, Boston, 2002.