# Seven Objectives of Software Assurance Sound Practices

There are seven objectives that are key to understanding the nature of software assurance “best” practices for the stakeholder community of practice. The sound practices are consensus-based “best” practices.

1. People implement practices. The sound practices are intended for daily use by the many thousands of individuals who develop software and support the nation’s critical infrastructure. To this end, the sound practices address the following four values: applicability to individual job functions, appreciation for the value, accessibility, and continuous improvement. Even though sound practices have been developed to be easily understood, their essence is often not immediately apparent to those who are inexperienced with the associated job functions. Therefore, caution should be given to ensure that those managing sound practices within organizations have sufficient experience.
2. Sound practices do not endorse commercial or specific documents, products, or services, but rather stress the essence of the guidance provided by such resources (e.g., formal quality management). Helpful examples are identified in the references available on the BSI site.
3. Sound practices are more effective and appropriate when they address (help prevent, mitigate, etc.) classes of problems. Detailed fixes to specific problems are not sound practices. For example, we do not provide security patches on this site. However, we do discuss detailed coding techniques that could be used during development to help prevent problems.
4. Sound practices are already implemented by some, if not many, organizations. Many fascinating and impressive ideas can be generated by the highly regarded list of organizations assembled for this effort. However, such ideas do not qualify as sound practices if no one is practicing them. Although we don’t necessarily have measurement data, the recommended sound practices have been demonstrated to be effective, feasible, and capable of being implemented.
5. Sound practices are developed by industry consensus. In particular, the parties with “skin in the game” (e.g., service providers, software suppliers) are able to bring their expertise from across the industry to weigh in on the “best” approach to addressing a concern. All of the material on this site has had external review, and although we have not yet arrived at full consensus, we expect that consensus will evolve by a combination of the feedback mechanism on the site and continued participation by the community.
6. Sound practices are reviewed by a broader set of stakeholders to ensure that those who have not been a part of the process can provide feedback.
7. Sound practices are presented to the community only after sufficient rigor and deliberation has warranted the inclusion of both the conceptual issue and the particular wording of the practice. Discussions among experts and stakeholders include consideration of
   - existing implementation level of a proposed sound practice
   - effectiveness of a proposed sound practice
   - feasibility of implementing a proposed sound practice
   - risk involved in not implementing a proposed sound practice
   - alternatives to the proposed sound practice

Joe Jarzombek
National Cyber Security Division
Department of Homeland Security