Get Your Board to Say “Yes” to a BSIMM Assessment

5 Ways Benchmarking Improves Software Security Oversight
The typical board of directors…

• Is more concerned than ever before about cyber risk
• Must demonstrate oversight to shareholders, customers, partners, and regulators
• Seeks opportunities for a competitive advantage
But…

- Has limited understanding of security activities
- Isn’t sure how to measure success
They often ask the "wrong" questions.

For example…
“What is the bug count in the software we develop?”

This is a “wrong” question because…

Bug count alone doesn’t consider severity of risk or size of your application portfolio.
“How long does it take us to recover from a security incident?”

This is a “wrong” question because…

This is largely out of your control; it can vary depending on the type of security breach.
They have limited context.

For example, if you tell your board…
“We’ve got # security staff for every developer.”

The board doesn’t know if that is high or low.
“We perform ad hoc source code review.”

The board doesn’t know if that is good or bad.
They focus on internal data.
Problems with an internal-only assessment

- May unwittingly inflate an organization’s software security activities
- Doesn’t consider the full universe of potential activities employed by advanced software security initiatives
- Relies on personal experience to plan for the future
The board can’t influence what they don’t understand.
As a result, your security program suffers

- Investments and hires are delayed or rejected.
- The organization has less incentive to comply with security policies.
- Confidence in security leadership decreases.
Change the conversation.

5 ways a BSIMM assessment helps your board see the big picture
They get an accurate picture of your software security initiative.
BSIMM shows your board...

- A full inventory of your software security activities in an easy-to-digest, standard framework
- An unbiased view of your operations, based on detailed interviews and documentation
They can compare your software security initiative to 100+ real-world SSIs.
BSIMM shows your board...

- Security activities that give you a competitive advantage over other organizations
- Areas where your organization lags behind best-in-class software security initiatives
They can understand the basis for investment decisions.
BSIMM shows your board...

- How peer organizations value investments in certain software security activities over others
- Opportunities to increase efficiencies and reduce risk by changing the mix of your security activities
They can follow a roadmap for future planning.
BSIMM shows your board...

- Maturity levels for each type of software security activity, based on prevalence and complexity
- The current position of your own organization on the maturity curve and strategies to reach the next level
They can see evidence of your progress.
BSIMM shows your board...

- How your software security initiative becomes more mature over time
- How your relative position to other organizations improves
“If the ladder is not leaning against the right wall, every step we take just gets us to the wrong place faster.”

—Steven Covey
Help your board see the big picture.

Talk to Synopsys about a BSIMM assessment today.