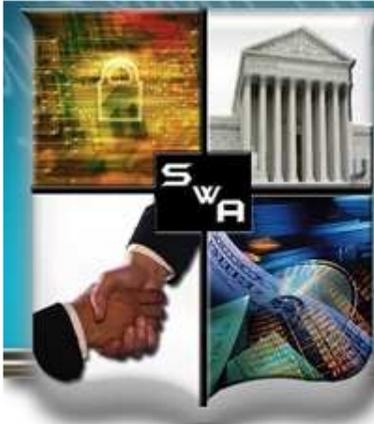




DoD-DHS-NIST  
Software Assurance Forum  
**Achieving and sustaining workforce  
readiness for implementation of  
assurance practices**  
*Birds of a Feather*



Homeland  
Security

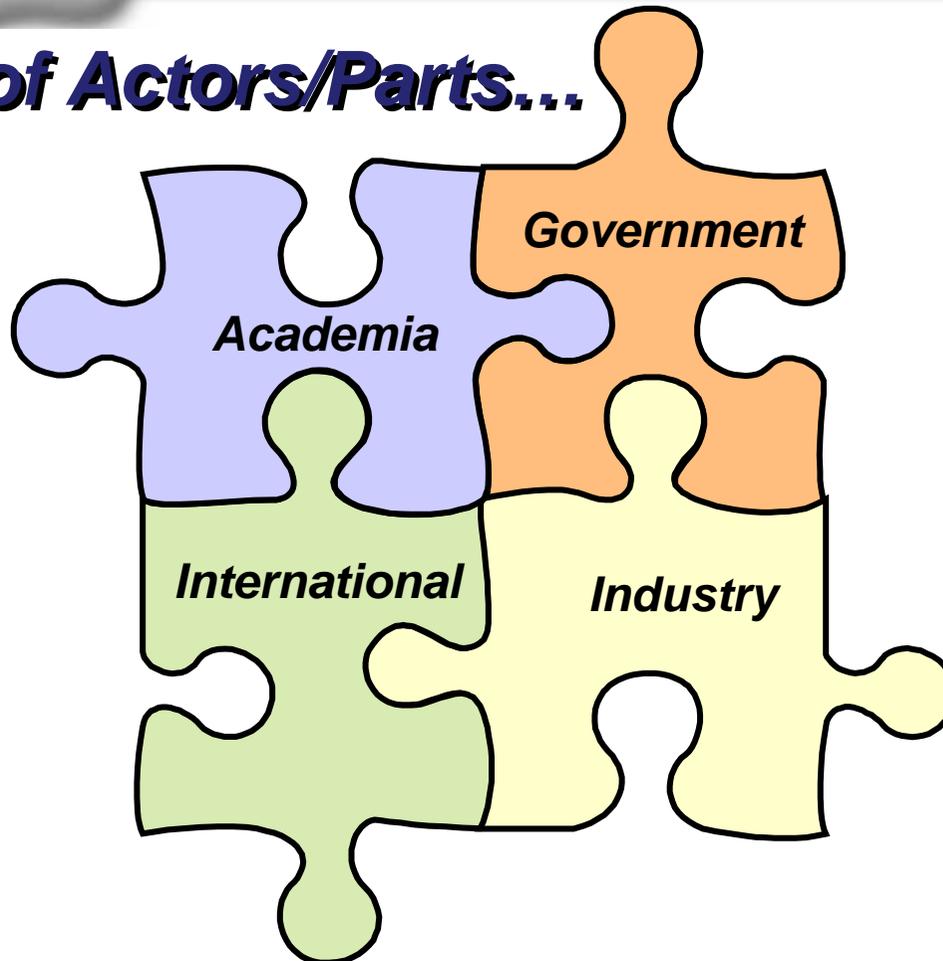


# SOFTWARE ASSURANCE FORUM

BUILDING SECURITY IN

To Be Successful We Must Work  
Together

**Lot's of Actors/Parts...**



*Are there common  
Work-products /  
Solutions ?*

**...all with  
different  
Challenges.**



## BOF Topics

- ▶ What CAN WE DO to improve adoption of SwA Education and Training? **Focus on the curriculum model and push for broader adoption**
- ▶ What can we do to increase the understanding and communication of what SwA Practices are and are not being done? **Focus on SwA practices and a push for broader adoption**
- ▶ How do SwA Practices and SwA Technologies work together through the SDLC ? **Focus on understanding product characteristics throughout the SDLC**

## Common Recommendations

- Identify and communicate what we have already accomplished
- Raise awareness of SwA Resources and Promote Implementation of practices through the use of tools
- Identify target audience(s)
- Identify the economic, mission, or other value of the resource(s) for each audience
- Identify speakers/messenger(s) to deliver to the target audience(s)
- Identify the message(s) for each audience
- What do we want the audience(s) to do?  
→ our measure of success is what action they take



**What CAN WE DO to work together with NICE to achieve and sustain workforce readiness for implementation of assurance practices?**

#### NICE Workstreams

- National Cybersecurity Awareness
- Formal Cybersecurity Education
- Federal Cybersecurity Workforce
- Cybersecurity Workforce Training and Professional Development

#### Questions for Discussion

- What are the areas where we can/should make progress together and how do we?
- What information should we share, at what points and how?
- What group(s) are best positioned to reach which audience – who can deliver the message/knowledge so that it is heard and understood? How should they do it?
- What are the lessons we have already learned ?



**Workforce Readiness and Practice Implementation**

**Government Sponsor**

The National Initiative for Cybersecurity Education (NICE), Ernest McDuffie

**SwA Education Landscape and Progress**

Nancy Mead (SEI) and Mark Ardis (Stevens Institute)

**SwA Measurement - An Enterprise Perspective**

Facilitator: Nadya Bartol (Booz Allen)

*Jim Cebula, SEI*

TBD

Dan Schutzer (FS ISAC)

**A Framework for Implementing and Measuring SwA Assurance Process**

Michele Moss (Booz Allen)

**SwA Practices - Getting to Effectiveness in Implementation**

Facilitator: Michele Moss (Booz Allen)

Sammy Miguez (Cigital)

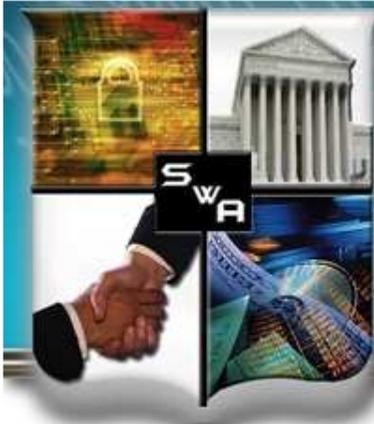
Dan Reddy (EMC)

Keith Turpin (Boeing)

Steve Lavenhar (Booz Allen)

**Workforce Training in the Software Assurance Landscape**

Marc Noble (ISC)<sup>2</sup>

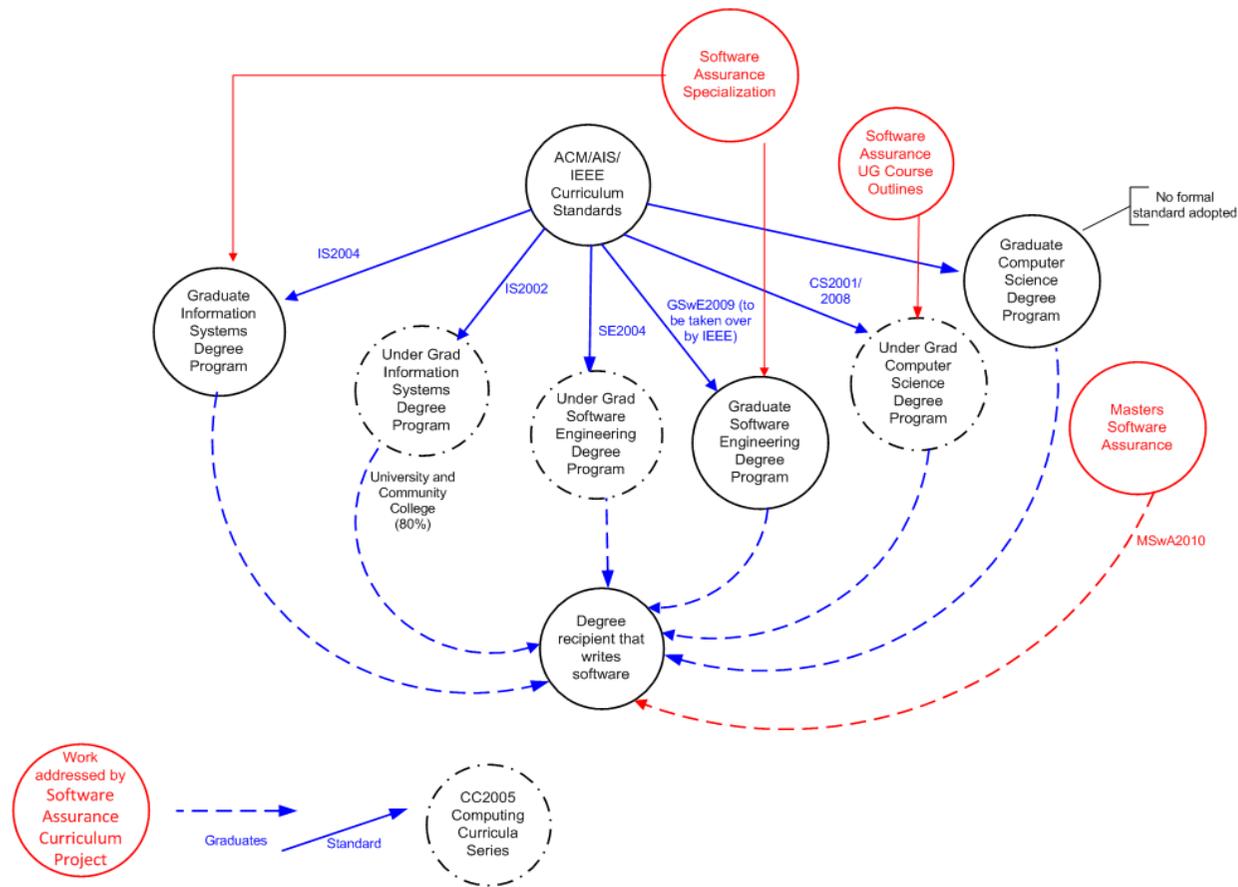


# SOFTWARE ASSURANCE FORUM

## BUILDING SECURITY IN

*SwA curriculum model & degree standards that are focused on graduates that build software*

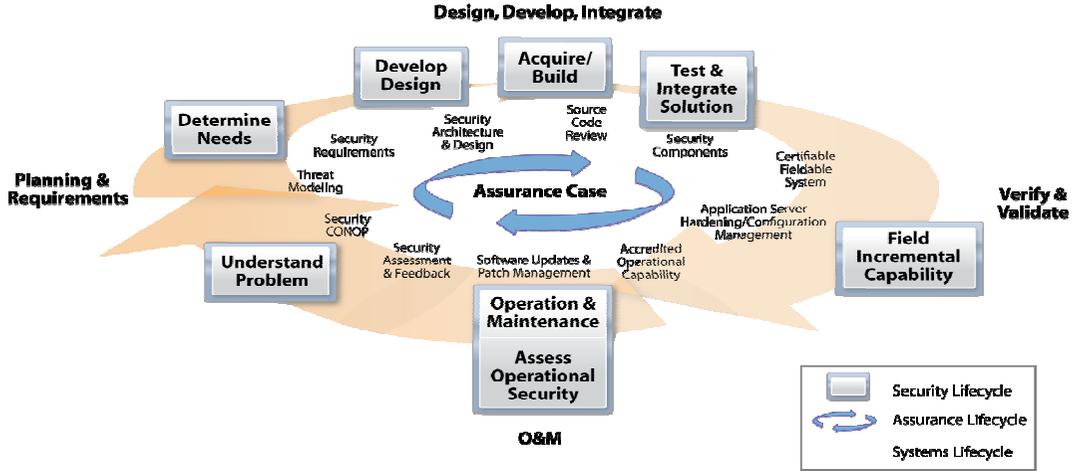
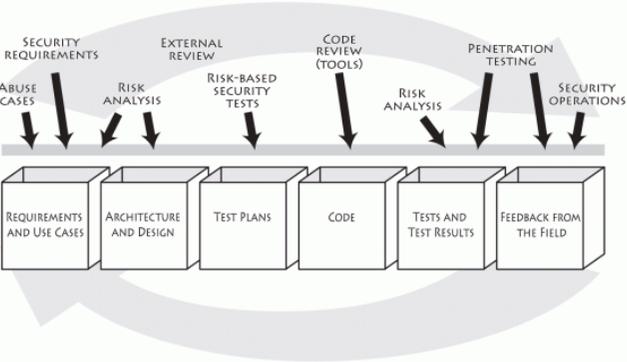
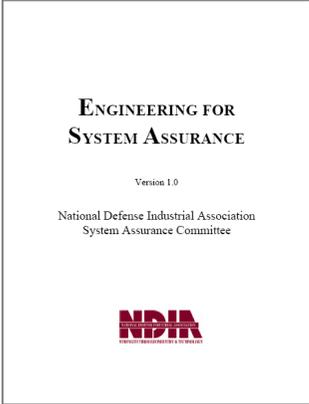
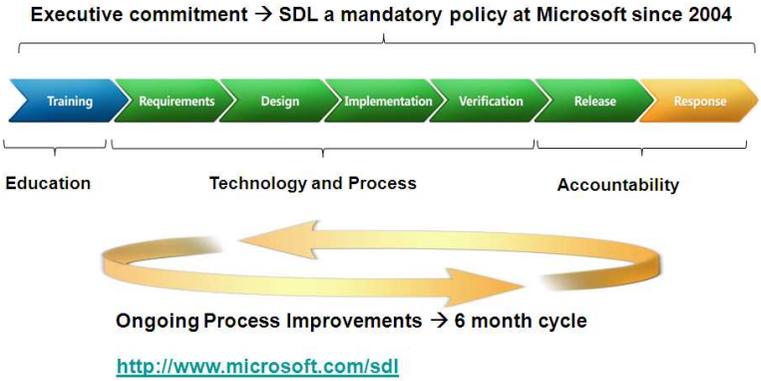
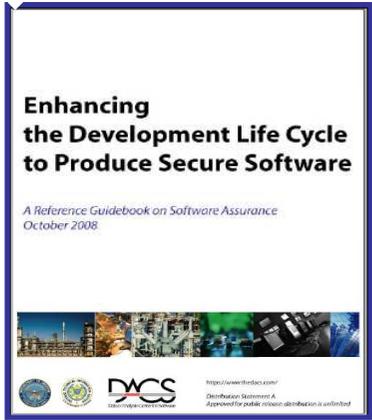
DHS Software Assurance for Computer Related Degree Programs



# SOFTWARE ASSURANCE FORUM

## BUILDING SECURITY IN

# Lifecycle Views

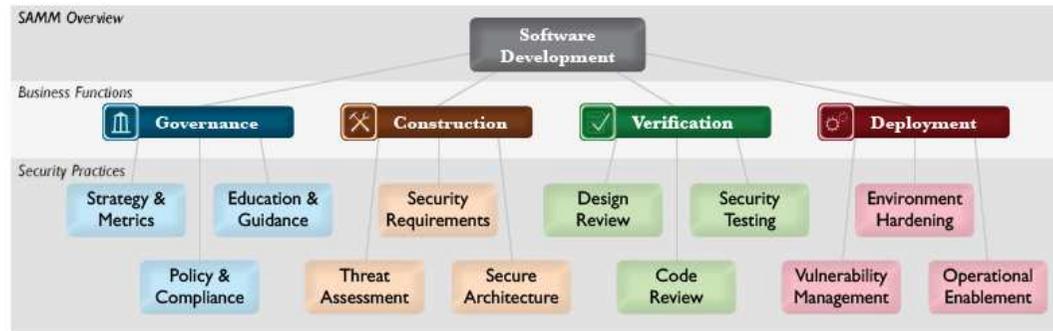




# SOFTWARE ASSURANCE FORUM

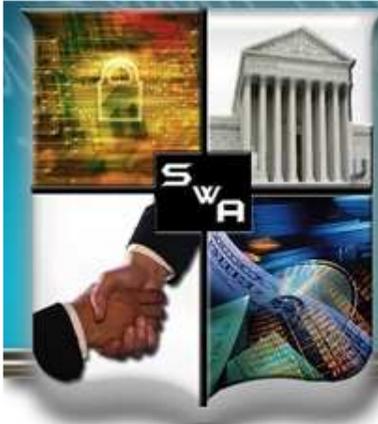
## BUILDING SECURITY IN

### SwA Views



**Open Software Assurance Maturity Model (SAMM)**  
<http://www.opensamm.org/>

**Building Security In Maturity Model (BSIMM)**  
<http://www.bsimm2.com/>

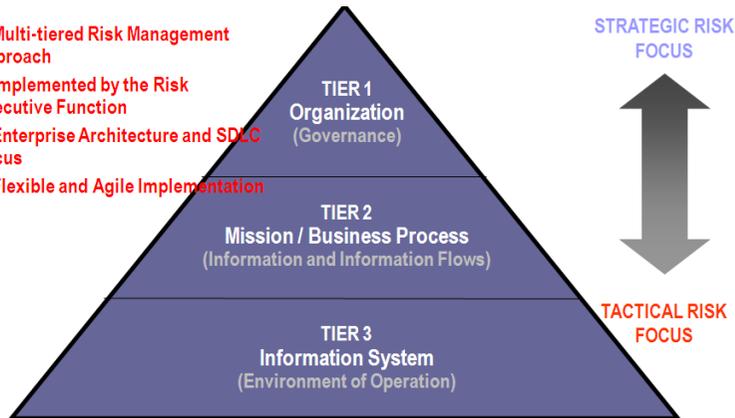


# SOFTWARE ASSURANCE FORUM

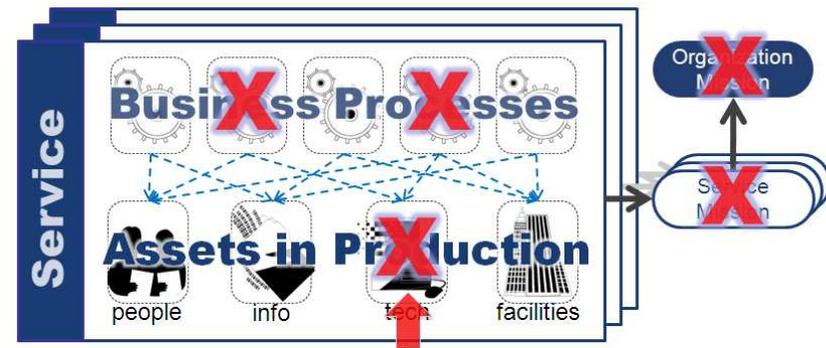
## BUILDING SECURITY IN

# Organizational Risk Management

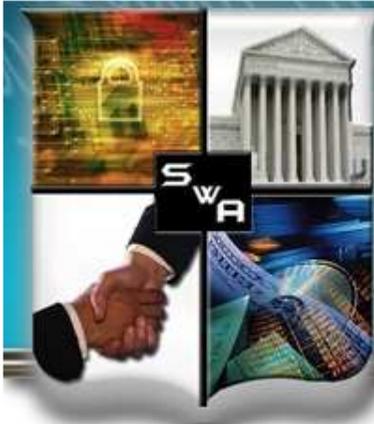
- Multi-tiered Risk Management Approach
- Implemented by the Risk Executive Function
- Enterprise Architecture and SDLC Focus
- Flexible and Agile Implementation



FISMA 2010 and Beyond  
Strategic and Tactical Risk Management and the Role of Software Assurance  
Ron Ross, NIST  
Software Assurance Workshops  
June 21, 2010



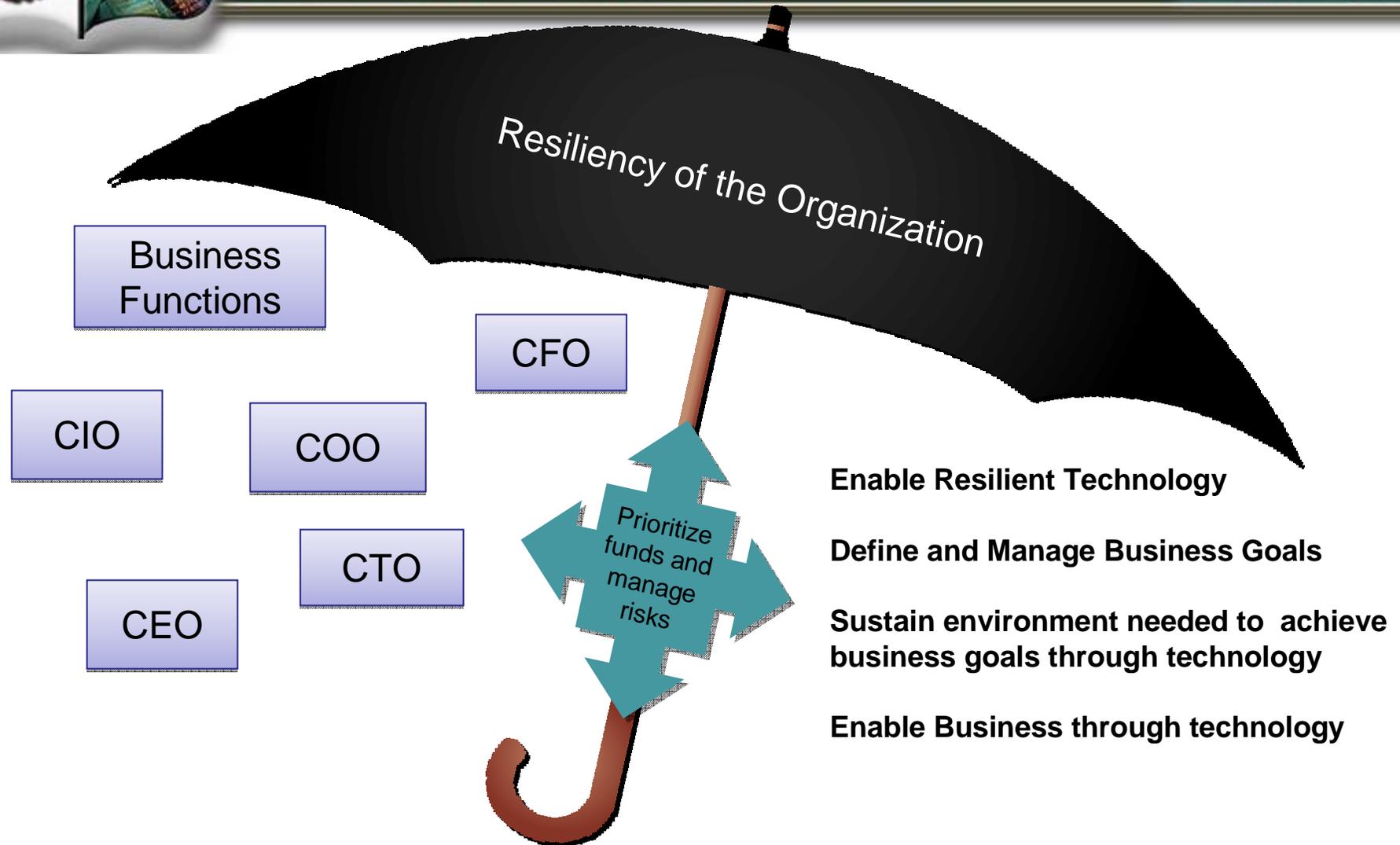
Software issues can impact availability and suitability of assets on which the organization depends



# SOFTWARE ASSURANCE FORUM

## BUILDING SECURITY IN

*We are working to create a Business View*





- Provide contributions that are targeted towards solving the problem on the table for this BOF
- Offer Solutions Vs Issues
- No Marketing Pitches
- Provide succinct (short vs lengthy) contributions to allow maximum contribution from all BOF participants



**What CAN WE DO to work together with NICE to achieve and sustain workforce readiness for implementation of assurance practices?**

Questions

- What are the areas where we can/should make progress together and how do we?
- What information should we share, at what points and how?
- What group(s) are best positioned to reach which audience – who can deliver the message/knowledge so that it is heard and understood? How should they do it?
- What are the lessons we have already learned ?

Discussion

- xxx



**What CAN WE DO to work together with NICE to achieve and sustain workforce readiness for implementation of assurance practices?**

### Questions

- What are the areas where we can/should make progress together and how do we?
- What information should we share, at what points and how?
- What group(s) are best positioned to reach which audience – who can deliver the message/knowledge so that it is heard and understood? How should they do it?
- What are the lessons we have already learned ?

### Discussion

- xxx



**What CAN WE DO to work together with NICE to achieve and sustain workforce readiness for implementation of assurance practices?**

Questions

- What are the areas where we can/should make progress together and how do we?
- What information should we share, at what points and how?
- What group(s) are best positioned to reach which audience – who can deliver the message/knowledge so that it is heard and understood? How should they do it?
- What are the lessons we have already learned ?

Discussion

- xxx



**What CAN WE DO to work together with NICE to achieve and sustain workforce readiness for implementation of assurance practices?**

Questions

- What are the areas where we can/should make progress together and how do we?
- What information should we share, at what points and how?
- What group(s) are best positioned to reach which audience – who can deliver the message/knowledge so that it is heard and understood? How should they do it?
- What are the lessons we have already learned ?

Discussion

- xxx