NIST is seeking information on the current usage of these existing approaches throughout industry, the robustness and applicability of these frameworks and standards, and what would encourage their increased usage. Please provide information related to the following:

1. What additional approaches already exist? ISACA has distributed the Computer Forensics and Cybersecurity Governance Model, and frameworks such as COBIT 5, Risk IT and Val IT. COBIT 5 has been issued with a high level framework to help an enterprise implement the framework. The scope of Risk IT framework is fully covered within the scope of the COBIT 5 framework.

The International Organization for Standardization (ISO) is a worldwide federation of national standards bodies (ISO member bodies). This organization is responsible for preparing international standards through its committees staffed by members from government, business and nonprofit organizations on a worldwide basis.

To ensure a knowledgeable and skilled workforce the DoD has taken the necessary steps to develop a directive that involves the credentialing and continuing education of all DoD employees with privileged access to DoD information systems. The ISC2 CISSP Common Body of Knowledge (CBK) has been carefully mapped to the **DoD 8570.1** directive, which requires every full- and part-time military service member, defense contractor, civilian and foreign employee with privileged access to a DoD system, regardless of job series or occupational specialty, to obtain a commercial certification credential that has been accredited by the American National Standards Institute (ANSI).

2. Which of these approaches apply across sectors? The frameworks provide globally accepted guidance, tools and models designed to help business and IT leaders maximize trust in, and value from their enterprise IT assets.

3. Which organizations use these approaches? They are globally used.

4. What, if any, are the limitations of using such approaches?

- Each framework has to be customized for each enterprise's business model, technology environment, industry, location and corporate culture.
- ISO is in the process of developing a standard (**Error! Reference source not found.** JTC 1**Error! Reference source not found.**/WG6 **Error! Reference source not found.**N 261) to assist its members in initiating and implementing governance on an accurate and complete basis. Yet, a step-by–step, unified approach to follow in implementing Governance Enterprise of IT does not readily exist.
- They do not idenify the specific business level risks that a user needs to review relating to enterprise IT security management, infrastructure security management, security device management and transaction monitoring. These frameworks are IT-centric and focused.

5. What, if any, modifications could make these approaches more useful?

- Make it mobile-relevant
- Make it fraud-online relevant

- Make it personal
- Make it less technical
- Metrics for the implementation of best practices to gauge improvement in controls

As Winn Schwartau indicated in an ISC2 webinar in 2011, we are experiencing the "perfect storm of security…Billions of intelligent mobile endpoints, an inherently weak backbone infrastructure, clueless users and smart bad guys."

6. How do these approaches take into account sector-specific needs? They discuss:

- Defense in depth. Security is a layered approach of infrastructure, applications, logical and physical security.

7. When using an existing framework, should there be a related sector-specific standards development process or voluntary program? Yes, there should be a sector-specific set of standards since each sector or industry has its own specific risks, issues and concerns. Yet, there are overarching controls and best practices that transcend industries or sectors.

8. What can the role of sector-specific agencies and related sector coordinating councils be in developing and promoting the use of these approaches? These groups can be used to:

1. Create with their customers to market case studies of the implementation of the approaches,

2. Encourage their customers to implement generally accepted best practices for cyber security and encourage security awareness,

3. Publicize security incidents and function as a sounding board for identifying framework improvements.

9. What other outreach efforts would be helpful?

- Mini-courses for the business and information technology professional
- Teach online behavior for children in terms of safety, security and ethics. This should cover: social networking, instant messaging, chat rooms, sexting, cyberbullying, gaming and overall security awareness.
- Constant education of the threat vectors and their prevention.