Executive Summary
Briefly, the goals and objectives of the project are listed below:

- To identify and address the internal and external security exposure of each CGIAR member’s information systems
- To develop and implement a CGIAR-wide security architecture
- To develop and implement a CGIAR-wide Business Continuity Plan
- To equip selected CGIAR personnel with the appropriate skills to implement and manage the detailed strategies identified

The overall implementation phases at both pilot and non-pilot sites were as follows:

Phase 1: Project Launch
Orientation of Asian and African regional and non-pilot Center representatives on the project approach, methodology, tools, templates, responsibilities, and schedule was conducted by the SGV consultants at the two pilot Centers, IRRI and ILRI. At non-pilot Centers, the regional resource persons facilitated the kickoff meetings. WorldFish and IWMI opted to have an institution-wide kickoff meeting, while CIFOR and ICRISAT kickoff meetings were limited to the IT group only and attended by the key officers.

Phase 2: Risk Assessment
The risk assessment phase was facilitated by SGV in both pilot Centers using document templates. For the non-pilot Centers, the Asian and African regional resource persons facilitated the risk assessment using a modified framework and document templates. Information assets (such as software, hardware, information) were identified and assigned the corresponding risks for the Asian pilot Centers. Non-pilot Centers such as CIFOR and ICRISAT were unable to sufficiently document the information assets and their corresponding values in terms of confidentiality, integrity, and availability. WorldFish and IWMI, on the other hand, were able to complete the documentation of their core information assets.

Risk assessments were carried out in the two pilot Centers. The impact of each risk and the likelihood of it happening were assessed for each information asset identified, and the recommended mitigating controls were subsequently selected. Risk treatment plans were developed in light of the risks for each information asset identified and then mitigating controls were identified and subsequently selected. Responses to risks varied from accepting to mitigating and transferring.

Phase 3: Technical Security Assessment
With help from the SGV consultants, both pilot Centers were able to identify their external and internal security exposures, and two major tests were performed: (1) penetration testing from the Internet, intranet, extranet, and remote access for each Center and (2) vulnerability assessment of all mission-critical servers and network devices. Hacker tools such as password cracking, denial of service attacks, packet sniffing, and website defacement were employed by the SGV consultants. The tests were done in four major areas: Internet, remote access service (RAS), extranet, and intranet.
For the non-pilot Centers, the technical security assessments were conducted by the Enterprise Security (ES) regional resource persons. Except for IITA and Bioversity, all non-pilot Centers in both Africa and Asia were able to complete these assessments.

**Phase 4: Business Impact Analysis**
Building on the results of the risk assessment, asset identification, and valuation performed above, business impact analyses were carried out. Specific tasks in this activity included defining failure scenarios and a business impact analysis survey, taking into consideration impact with respect to the following areas: financial, reputation, contractual and legal, customer service, and environmental. The SGV consultants facilitated the sessions using document templates for both pilot Centers. Except for IWMI and WorldFish, all the other non-pilot Centers in both Asia and Africa were unable to complete the business impact analysis.

**Phase 5: Policy, Procedures, and Standards Development**
Both IRRI and ILRI received a set of recommended security policies that covered the given domains to meet ISO requirements. This is currently being reviewed and edited under the leadership of ILRI’s IT manager.

**Phase 6: Implementation Strategy Development**
Strategy development ranged from, where possible, removing the threat altogether to minimizing the likelihood of occurrence, and minimizing the effect of occurrence.