Audit

Organizations, often seek to have their internal Information Technology (IT) infrastructure audited to see how it stands up to best practices. The process of audit also provides an independent view of areas of risk that might have been overlooked by staff of the organization. These audits are not typical accounting audits but rather look at the security measures that have been adopted by the organization and how they have been implemented. Sometimes, measures implemented are not appropriate. Sometimes vital measures have been overlooked. Other times, the implementation of a particular security measure has been done incorrectly or poorly and does not perform as required.

The audit is a valuable process that can help organizations improve their specific security practices protecting their Information Communication Technology (ICT) functions and usage. In some jurisdictions or specific businesses there may be mandatory or regulatory requirements for audits to be done at regular intervals.

Actually, performing an audit is fairly methodical and similar steps are followed by most folks that offer such a service. It is time consuming and cannot be done externally, via surveys, or in other time saving ways. The structure is very straight forward:

1. Find and select a suitable audit professional. These can be found in public accounting firms and well as consulting organizations and there are individuals that specialize in this process. And, of course, RFPs can be offered to any combination of these deemed suitable – within the selection process.
2. After a contractor is selected, negotiating the contract, the terms and reference for the work, to agree on what is to be delivered when the audit is complete, and a formal directive as to how organization sensitive information and documents will be handled would be next.
3. When the first two elements have been completed satisfactorily, the parties should enter into a Non-Disclosure Agreement (NDA). This is meant to protect and indemnify the organization in the event the contractor(s) were to reveal confidential information obtained during the audit. The nature of an audit is such that the contractor must have access to all of the relevant information associated with the ICT functions in order to properly assess their effectiveness.
4. The contractor will be given written formal authority to access the necessary parts of the organization in order to obtain information about what is currently being done within the ICT functions as well as copies of the contract, terms of reference, the agreed description of deliverables, formal sensitive documents and information handling document (storage and protection), and the NDA.
5. The contractor will, during the course of the audit process: observe, conduct interviews, require specific documents (for example a copy of the formal ICT policy document), and view all ICT operations and facilities.
6. During this process many aspects of the ICT function will be assessed and compared to best practice. These assessments will be compiled over the course of the activity for inclusion in the auditor’s final formal report. This information will be stored and protected based on the agreed method.
7. Some interviews may be repeated because information discovered later in the investigation has revealed the need for additional information or clarification.
8. Depending on the size of the organization being audited, the process may take many weeks or months (for a large organization).
9. Many elements of the organizations ICT functions will be inspected, reviewed, and analysed in order to do a thorough and proper audit. There are a set of standard elements, however, every

organization is a little bit different and the auditor will determine what elements are to be investigated (these will be influenced by the terms of reference as well). No two audits are the same.