Accessibility and usability of the website: The FSB has adopted a two-pronged approach to resolve the website challenges that are currently being experienced, namely

- upgrading the internet infrastructure; and
- redesigning of the internet layout.

The infrastructure upgrade that is intended to resolve the challenges that were experienced in accessing the website and downloading documents was completed in January 2013. No further complaints have been received from the industry on accessing the website and downloading of documents.

The website redesign project that will address the layout and ease of use challenges is intended to modernise the layout of the FSB website to give it a more professional look and feel, as well as make the website user friendly. The website redesign project includes the implementation of technology that will enable the FSB to have a high availability website system where a secondary internet system will take over the website operation during outages of the primary internet system to ensure business continuity. It is envisaged that this project will be completed in September 2013.

Security principles and disaster recovery relating to the website: To date, no compromise of the FSB website has been reported. The FSB's security principles apply to the FSB website, which include the following:

- Logical Access Control (i.e. the controls for who may perform which actions on the website): modify and update access is restricted to authorised individuals. Access is granted according to the principle of least amount of privileges needed to perform a function. Thus users of the website will only be able to read content, not change content. Logical access controls address the need for the protection of the integrity of the website, i.e. the assurance that content on the website is a true reflection of the current state;
- External Attacks (i.e. attacks on the FSB website from external sources aimed at defacing or compromising the integrity and availability of the website): the website is protected by the FSB network security technologies. The FSB follows a multi-layer "defence in depth" strategy. In the event of a failure or breach in

one of the components or technologies, remaining components and technologies are in place to respond to the threats;

- Protection against malware (i.e. malicious software, such as viruses, aimed at compromising or damaging the website): the website is protected by anti-virus software;
- Physical security (i.e. the protection of the physical equipment on which the website is hosted): the website server is housed in a physically secure environment;
- Back-ups (i.e. making a copy of the website in the event of system failure or compromise): the website is backed up daily to ensure recoverability and availability.

The FSB has a disaster recovery plan in place, which includes the recovery of the FSB website. The Disaster Recovery plan was successfully tested in January 2013 under supervision of the FSB's internal auditors.

FSB ICT environment: The FSB ICT environment is governed by ICT governance principles, such as:

- Change management, whereby changes to systems and application must be formally tested and approved prior to implementation in the production environment;
- Vulnerability or patch management, which allows for the continuous identification and remediation of system vulnerabilities or weaknesses inherent to the operating system and technology used for the website through the application of corrective patches as system vulnerabilities and weaknesses may be exploited or targeted to compromise or damage the website.

Archiving and version control: Principles for website documentation management are being developed. It is envisaged that these principles will be developed and implemented by September 2013.