DNV·GL


# INFORMATION SECURITY MANAGEMENT SYSTEM

## Self Assessment

### Have you implemented the 10 essential information security controls?

No matter what the size of your business or scope of operation, managing your information security risks is vital. ISMS (Information Security Management System) certification provides the confidence that any risk to information held by the organization is systematically managed.

There are 10 essential controls that are fundamental building blocks for information security management systems. This sample question set allows you to self assess your information security controls against those 10 essentials.

## 1. Information Security Policy

1.1.1 We have written security policy document(s) approved by top management.

- ❑ Fully
- ❑ Largely
- ❑ Partly
- ❑ Not done

1.1.2 The security policies are available and communicated to all staff.

- ❑ Fully
- ❑ Largely
- ❑ Partly
- ❑ Not done

1.1.3 The security policies are updated periodically.

- ❑ Fully
- ❑ Largely
- ❑ Partly
- ❑ Not done

1.1.4 We conduct regular reviews to confirm compliance with security policies and standards e.g. technical compliance checks, system audits.

- ❑ Fully
- ❑ Largely
- ❑ Partly
- ❑ Not done

## 2. Assessment of security risks

2.1.1 We have identified an appropriate method for security risk assessment.

- ❑ Fully
- ❑ Largely
- ❑ Partly
- ❑ Not done

2.1.2 We have systematically considered the business harm and the likelihood of security breaches.

- ❑ Fully
- ❑ Largely
- ❑ Partly
- ❑ Not done

2.1.3 We have evaluated the security risks against criteria for acceptance and are taking appropriate actions for risks outside the criteria.

- ❑ Fully
- ❑ Largely
- ❑ Partly
- ❑ Not done

## 3. Allocation of security responsibilities

3.1.1 We have defined the overall responsibilities for protection of information and IT assets.

- ❑ Fully
- ❑ Largely
- ❑ Partly
- ❑ Not done

3.1.2 Each information system is the responsibility of a defined system owner.

- ❑ Fully
- ❑ Largely
- ❑ Partly
- ❑ Not done

3.1.3 Responsibilities for the implementation of security processes is also clearly defined.

- ❑ Fully
- ❑ Largely
- ❑ Partly
- ❑ Not done

## 4. Training awareness and education

4.1.1 Users receive appropriate training in security policies and procedures.

- ❑ Fully
- ❑ Largely
- ❑ Partly
- ❑ Not done

4.1.2 There is an active security awareness programme in operation.

- ❑ Fully
- ❑ Largely
- ❑ Partly
- ❑ Not done

4.1.3 Users receive training in the correct use of information systems.

- ❑ Fully
- ❑ Largely
- ❑ Partly
- ❑ Not done

4.1.4 This training also extends to third party users.

- ❑ Fully
- ❑ Largely
- ❑ Partly
- ❑ Not done

4.1.5 Staff and 3rd parties with access to our information systems sign non-disclosure agreements.

- ❑ Fully
- ❑ Largely
- ❑ Partly
- ❑ Not done

## 5. Security incident management

5.1.1 There is a formal reporting procedure for security incidents.

- ❑ Fully
- ❑ Largely
- ❑ Partly
- ❑ Not done

5.1.2 All staff and third parties are made aware of the incident reporting procedure.

- ❑ Fully
- ❑ Largely
- ❑ Partly
- ❑ Not done

5.1.3 Security incidents are reported quickly through management channels.

- ❑ Fully
- ❑ Largely
- ❑ Partly
- ❑ Not done

5.1.4 There is a formal disciplinary process for security breaches.

- ❑ Fully
- ❑ Largely
- ❑ Partly
- ❑ Not done

## 6. Protection from cyberspace attack

6.1.1 We prohibit the use of unauthorised software.

- ❑ Fully
- ❑ Largely
- ❑ Partly
- ❑ Not done

6.1.2 We have deployed programs and measures to protect against malicious software e.g. viruses, trojan horses, malware.

- ❑ Fully
- ❑ Largely
- ❑ Partly
- ❑ Not done

6.1.3 We have deployed measures to protect against external 'hacker' attacks e.g. IDS, Firewalls, DMZ.

- ❑ Fully
- ❑ Largely
- ❑ Partly
- ❑ Not done

6.1.4 There are regular reviews of software and data on critical systems to detect any unauthorised programs or data.

- ❑ Fully
- ❑ Largely
- ❑ Partly
- ❑ Not done

## 7. Business continuity planning

7.1.1 We develop and maintain business continuity plans according to a managed process.

- ❑ Fully
- ❑ Largely
- ❑ Partly
- ❑ Not done

7.1.2 The risks from events that could interrupt business are identifed and evaluated e.g. fire, flood, major accident; pandemic, utility failure.

- ❑ Fully
- ❑ Largely
- ❑ Partly
- ❑ Not done

7.1.3 Continuity plans enable us to maintain operations following failure or damage to vital services and facilities.

- ❑ Fully
- ❑ Largely
- ❑ Partly
- ❑ Not done

7.1.4 Continuity plans are tested and updated regularly.

- ❑ Fully
- ❑ Largely
- ❑ Partly
- ❑ Not done

## 8. Misuse of proprietary software

8.1.1 We require staff to comply with software license conditions.

- ❑ Fully
- ❑ Largely
- ❑ Partly
- ❑ Not done

8.1.2 We maintain up-to-date registers of software licenses.

- ❑ Fully
- ❑ Largely
- ❑ Partly
- ❑ Not done

8.1.3 We conduct regular audits of software use.

- ❑ Fully
- ❑ Largely
- ❑ Partly
- ❑ Not done

## 9. Safeguarding enterprise data

9.1.1 Inventories of key enterprise data sources are maintained.

- ❑ Fully
- ❑ Largely
- ❑ Partly
- ❑ Not done

9.1.2 We have guidelines for retention, storing and disposal of data and records.

- ❑ Fully
- ❑ Largely
- ❑ Partly
- ❑ Not done

9.1.3 We have implemented measures to protect stored enterprise data from loss or corruption.

- ❑ Fully
- ❑ Largely
- ❑ Partly
- ❑ Not done

## 10. Personal data protection

10.1.1 We have a management structure and controls to comply with data protection legislation.

- ❑ Fully
- ❑ Largely
- ❑ Partly
- ❑ Not done

10.1.2 Data owners have responsibility to identify any personal information that is stored or proposed for storage.

- ❑ Fully
- ❑ Largely
- ❑ Partly
- ❑ Not done

10.1.3 We report the personal data being stored and the purposes for its use in accordance with applicable legislation e.g. Data Protection Act 1998.

- ❑ Fully
- ❑ Largely
- ❑ Partly
- ❑ Not done