Standards Assurance Tables

# Standards Assurance Tables

The Ministry of Justice (MoJ) Cyber Security team have developed a 'Standards Assurance Table' (SAT) in the form of a Google Sheet template.

The SAT measures technology systems (and surrounding information governance) against the [UK Cabinet Office](https://www.gov.uk/government/organisations/cabinet-office) [Minimum Cyber Security Standard (MCSS)](https://www.gov.uk/government/publications/the-minimum-cyber-security-standard) and [UK National Cyber Security Centre (NCSC)](https://www.ncsc.gov.uk/) [Cloud Security Principles (CSPs)](https://www.ncsc.gov.uk/collection/cloud-security?curPage=/collection/cloud-security/implementing-the-cloud-security-principles).

For transparency and open-working purposes, a [redacted copy of the Standards Assurance Table](https://docs.google.com/spreadsheets/d/1oO9RAZQ6ETsN2iHZb5zcFM0HROliw18MBv89oF-BPeg/edit?usp=sharing) has been published. Please note, this is not the functional template used within the MoJ.

## SAT Template

The SAT itself is written to be self-explanatory to a cyber security professional who is already aware of the MCSS/CSP and has a familiarity with information risk management concepts.

* Black labelled sheets describe the SAT and how it should be used
* Blue labelled sheets are the ones to complete
* Yellow labelled sheets are automatically calculated, providing reports based on the blue labelled sheet data
* Green labelled sheets offer help/guidance on SAT components

## Key SAT concepts

The SATs have measures including "Objectives", "Evidence", "Confidence", an overall "Delta" (which is the most pertinent SAT output) and "Further Evidence Required", with supporting commentary.

The primary SAT purpose is to help assess a system against the MCSS/CSP. It is used to determine confidence whether or not the evidence demonstrates the system is compliant (or not).

Evidence is analysed to determine confidence that the evidence demonstrates the system meets (or does not meet) the standards. It also indicates the 'gap' (delta) between the system's posture according to said evidence and the standards.

### Objectives

The MCSS/CSPs have been distilled into 39 objectives. The Assessor (normally a cyber security professional) completes the SAT by evaluating the target system against the objectives.

The [categories used within the MCSS](identify-protect-detect-respond-recover.html) are discussed seperately.

Objectives are templated. This means they can be added to but existing objectives must not be deleted or edit in-place.

### Evidence

To avoid assessments that are ultimately anecdotal, the assessor will only rely upon written evidence.

Evidence can come in the form of transcribed conversations, diagrams, documentation or other auditable information about a system.

Evidence might not be directly related to the system itself but form a part, for example, where there is a wider document that is not system orientated but which describes who is relevant role holders currently are.

Evidence is described as being 'Held', 'Partial', 'Not Held' or 'N/A' (where the Objective is not applicable to the system being assessed).

### Confidence

The assessor reviews the evidence and uses their professional opinion to indicate a Confidence Score.

The Confidence Score uses a scale from 0 (no confidence at all) to 14 (high level of confidence), or 'N/A' (where the Objective is not applicable to the system being assessed).

### Delta

The Delta Rating is the resulting 'distance' between the assessed system posture against an Objective and the confidence of the same.

Mathematically, the final Delta Rating is N/A (where the Objective is not applicable to the system being assessed) or 0 to 14 (inc).

A wide delta (higher numerical value) indicates that the Objective is not met. A narrow delta (lower numerical value) indicates that the Objective is closer to being met.

The Delta Rating is automatically calculated as '14 minus Confidence Score'.

### Further Evidence Required

The assessor indicates what further evidence *types* in their view are required based on the evidence they have thus far.

The [Further Evidence Required (Help) sheet](https://docs.google.com/spreadsheets/d/1oO9RAZQ6ETsN2iHZb5zcFM0HROliw18MBv89oF-BPeg/edit#gid=679100590) has a calculator which the assessor will use.

The data point is currently a unique number to assist with future automated analysis. The format and range of values for the data point is currently under active review and so subject to change without notice.

## Understanding the Objectives, gathering evidence for the assessor

Teams/individuals responsible for the design, creation, implementation, support and maintenance of systems should have viable written evidence (regardless of format) that should be made available to various teams on request, for example, security or to internal audit.

Using the [categories used within the MCSS](identify-protect-detect-respond-recover.html) as a basis, some indicative questions and documentation expectations are discussed below.

### IDENTIFY

#### Possible documentation

* Team organisation charts
* Data Privacy Impact Assessments (DPIAs)
* Information risk management documentation (for example, RMADS)
* Information flow diagrams

#### Thought questions

* Who is responsible and/or accountable for the the system whether from an operational or budgetary perspective?
* Who is responsible and/or accountable for the information held inside the system?
* What security-focused work has been conducted recently (within the last year) on any suppliers and supplier systems to ensure they are safe for use/integration?
* Where is the system technically hosted?
* In what services or geographical locations does the system *store* data?
* In what services, geographical, or legal locations does the system *process* data?
* What are the consequences if the system is unavailable to users or data has been lost/corrupted?
* How do the consequences of unavailability change over time? (For example, after one hour, one day, one week, one month... permanent.)
* What changes - if anything - regarding business continuity / disaster recovery processes or plans if the system is unavailable or data has been lost/corrupted?

### PROTECT

#### Possible documentation

* Data Privacy Impact Assessments (DPIAs)
* Information risk management documentation (for example, RMADS)
* Information flow diagrams
* Technical/system architecture documentation
* Penetration test / IT Health Check reports and remedial documentation
* Risk registers

#### Thought questions

* How does the system ensure only authorised people can use the system?
* How are system users managed for joiners, movers and leavers?
* How is the system's underlying software kept up to date for security software patching?
* How does the system protect itself appropriately and proportionately from attackers?
* What assurance is there that the system can protect itself from attackers over time, so it is secure now but also will remain secure in the future?
* How often has technical security testing been conducted? Where within the system?
* How does the system stay up to date using modern encryption to keep data safe?
* Does the system use multi-factor authentication (MFA, also known as 2FA)?
* For people who have access to the system, do they have all the right clearances in place? How is this assured?

### DETECT

#### Possible documentation

* Information risk management documentation (for example, RMADS)
* Technical/system architecture documentation
* Penetration test / IT Health Check reports and remedial documentation
* Risk registers

#### Thought questions

* How does the system, and accompanying operational support teams, know/detect when the system is under attack?
* How is access to the system (both authorsed and unauthorised) logged so retrospective investigations can take place to determine 'who did what when'?
* How is the required level of detail in logs determined? How long are log files retained?

### RESPOND

#### Possible documentation

* Information risk management documentation (for example, RMADS)
* Technical/system architecture documentation
* Operational/support documentation

#### Thought questions

* What plans, processes or procedures are in place to respond to a detected cyber attack?
* How are these plans kept up to date and relevant?
* Does everyone who needs to know about these plans know about them?
* Has the plan been tested in the last 12 months?
* How are stakeholder communications handled during a security incident?
* How are external communications handled during a security incident for external parties, such as supervisory bodies, the NCSC or Cabinet Office?

### RECOVER

#### Possible documentation

* Operational/support documentation
* Retrospective session notes

#### Thought questions

* What happens for business continuity / disaster recovery if the system is unavailable or data has been lost/corrupted?
* Have these measures been tested in the last 12 months?