IDENTIFY, PROTECT, DETECT, RESPOND, RECOVER

# IDENTIFY, PROTECT, DETECT, RESPOND, RECOVER

The Ministry of Justice (MoJ) is required to adhere (but prefers to exceed) to the [Minimum Cyber Security Standard (MCSS)](https://www.gov.uk/government/publications/the-minimum-cyber-security-standard).

## The Standard

The [UK HMG Security Policy Framework](https://www.gov.uk/government/publications/security-policy-framework) mandates protective security outcomes that the MoJ must achieve (and suppliers to MoJ, where they process MoJ data/information).

More information is available from <https://www.gov.uk/government/publications/the-minimum-cyber-security-standard.>

### IDENTIFY

IDENTIFY is a prerequisite standard that requires:

* appropriate information security governance processes;
* identification and cataloging of information held/processed; and
* identification and cataloging of key operational services provided.

### PROTECT

PROTECT is the core standard to provide fundamentally defences to information and requires:

* access to systems and information to be limited to identified, authenticated and authorised systems/users;
* systems to be proportionally protected against exploitation of known vulnerabilities; and
* highly privileged accounts (such as administrative level) to be protected from common attacks.

### DETECT

DETECT is the core standard to detect when attacks are taking, or have taken, place and requires:

* capture event information (and apply common threat intelligence sources, such as [CiSP](https://www.ncsc.gov.uk/cisp));
* based on PROTECT, define and direct monitoring tactics to detect when defence measures seem to have failed;
* detection of common attack techniques (such as commonly known applications or tooling); and
* implementation of transaction monitoring solutions where systems could be vulnerable to fraud attempts.

### RESPOND

RESPOND is the core standard to define the minimum of how organisations should respond to attacks and requires:

* development and maintenance of an incident response & management plan (including reporting, roles and responsibilities);
* development and maintenance of communication plans, particularly to relevant supervisory bodies, law enforcement and responsible organisations such as the NCSC;
* regular testing of the incident response & management plan;
* assessment and implementation of mitigating measures on discovery of an incident (successful attack); and
* post-incident reviews to ensure feedback into the iteration of the incident response & management plan.

### RECOVER

RECOVER is the core standard to define the minimum of how organisations should recover from an attack once it has been considered closed, and requires:

* identification and testing of contingency mechanisms to ensure the continuance of critical service delivery;
* timely restoration of the service to normal operation (a plan to do so, and testing of that plan);
* from DETECT & RESPOND, immediately implementing controls to ensure the same issue cannot arise in the same way again, ensuring systematic vulnerabilities are proportional remediated.