Australian Government
Australian Signals Directorate

ACSC Australian Cyber Security Centre

Essential Eight to ISM Mapping

First published: January 2019
Last updated: October 2021

Introduction

The Australian Cyber Security Centre (ACSC) has developed prioritised mitigation strategies, in the form of the *Strategies to Mitigate Cyber Security Incidents*, to help organisations protect themselves against various cyber threats. The most effective of these mitigation strategies are the Essential Eight.

The *Essential Eight Maturity Model*, first published in June 2017 and updated regularly, supports the implementation of the Essential Eight. It is based on the ACSC's experience in producing cyber threat intelligence, responding to cyber security incidents, conducting penetration testing and assisting organisations to implement the Essential Eight.

As the Essential Eight outlines a minimum set of preventative measures, organisations need to implement additional measures where it is warranted by their environment. Further, while the Essential Eight can help to mitigate the majority of cyber threats, it will not mitigate all cyber threats. As such, additional mitigation strategies and security controls need to be considered, including those from the *Strategies to Mitigate Cyber Security Incidents* and the *Information Security Manual* (ISM).

Mapping between the Essential Eight and the ISM

As Maturity Level Two is considered the baseline for non-corporate Commonwealth entities, a mapping between Maturity Level Two and Maturity Level Three of the *Essential Eight Maturity Model* and the ISM is outlined below. Changes between maturity levels are indicated via bolded text.

Mitigation Strategy	Maturity Level Two	Maturity Level Three
Application control	0843, 1490, 1657, 1660, 1661	0843, 1490, **1656**, 1657, **1658**, **1544**, **1659**, **1582**, 1660, 1661, **1662**, **1663**
Patch applications	1690, 1691, 1693, 1698, 1699, 1700, 1704	1690, 1691, **1692**, 1693, 1698, 1699, 1700, 1704, **0304**
Configure Microsoft Office macro settings	1671, 1488, 1672, 1673, 1489, 1677	1671, **1674**, **1487**, **1675**, **1676**, 1488, 1672, 1673, 1489, 1677, **1678**
User application hardening	1486, 1485, 1666, 1667, 1668, 1669, 1542, 1670, 1412, 1585, 1664	1486, 1485, **1654**, 1667, 1668, 1669, 1542, 1670, 1412, 1585, **1655**, **1621**, **1622**, 1664, **1665**

Restrict administrative privileges	1507, 1647, 1648, 1175, 1380, 1687, 1688, 1689, 1387, 1685, 1509, 1650	1507, 1647, 1648, **1508**, 1175, **1653**, 1380, 1687, 1688, 1689, **1649**, 1387, 1685, **1686**, 1509, **1651**, 1650, **1652**
Patch operating systems	1694, 1695, 1701, 1702, 1501	1694, 1695, **1696**, 1701, 1702, **1407**, 1501
Multi-factor authentication	1504, 1679, 1680, 1681, 1173, 1401, 1683	1504, 1679, 1680, 1681, 1173, **1505**, 1401, **1682**, 1683, **1684**
Regular backups	1511, 1515, 1705, 1707	1511, 1515, 1705, **1706**, 1707, **1708**

Further information

The *Information Security Manual* is a cyber security framework that organisations can apply to protect their systems and data from cyber threats. The advice in the *Strategies to Mitigate Cyber Security Incidents*, along with its Essential Eight, complements this framework.

Contact details

If you have any questions regarding this guidance you can write to us or call us on 1300 CYBER1 (1300 292 371).