The assessment of each system should be documented in a system information management plan template. This plan:

Template for system information management plan

National Archives of Australia

* will link to your systems register and other information governance documents
* should cover all relevant information about the system including software, business owners, how it will be managed over its life and details about its assessment against the framework, and
* may extend to systems and technology hosted in the cloud, or via social media and mobile devices.

|  |  |  |
| --- | --- | --- |
| **Full system detail** | **Your system** | **Plan or Action** |
| System name and full product name |  |  |
| System common name or abbreviation |  |  |
| Business owner (Division, Branch, Section) |  |  |
| Business processes supported by system |  |  |
| External or internal use only? |  |  |
| Security classification |  |  |
| Access controls – Can user roles be defined? |  |  |

|  |  |  |
| --- | --- | --- |
| **Technical detail** | **Your system** | **Plan or Action** |
| System version |  |  |
| System type eg database |  |  |
| Software, OS requirements |  |  |
| Age of system, date acquired |  |  |
| Upgrade due date |  |  |
| Server location (physical) |  |  |
| Current size of data holdings |  |  |

|  |  |  |
| --- | --- | --- |
| **System administration and support** | **Your system** | **Plan or Action** |
| System administrator |  |  |
| Number of administrators |  |  |
| Is there a maintenance agreement with vendor? |  |  |
| Where is the source code kept? |  |  |
| Where is system information kept? eg TRIM location |  |  |
| Where is the configuration, customisation documentation kept? eg TRIM location |  |  |
| Cost of system (initial procurement) |  |  |
| Ongoing costs (eg licensing and support) |  |  |
| Is there a related legacy system? |  |  |
| Is the legacy data managed? |  |  |
| Identify systems that use data from this system |  |  |
| Identify systems that this system uses data from |  |  |

|  |  |  |
| --- | --- | --- |
| **PHASE 1 – Risk assessment** | **Yes – Document details** | **No – Document details** |
| System name / full product name |  |  |
| 1.1 Does or will the system hold unique information or data (that is not duplicated elsewhere)? |  |  |
| 1.2 Is or will the information or data:  . be the authoritative source of truth,  . relied on to create the authoritative record, or  . feed into a system that holds the authoritative source of information or data? |  |  |
| 1.3 Is the risk or value of the information high enough to warrant additional controls to ensure that it is trustworthy? |  |  |
| 1.4 Is there sufficient business benefit for managing disposal within the system before decommissioning? |  |  |
| 1.5 Are you likely to access the information or data beyond the expected life of the system? |  |  |
| 1.6 Do or will you need to keep the information or data for longer than the expected life of the system? |  |  |

|  |  |  |
| --- | --- | --- |
| **PHASE 2 – Assessment of information management functionality**  **Module 1:  Information is trusted** | **Yes – Document details** | **No – Where a risk or gap was identified in Phase 2 – indicated by a 'No' response – document the solution to address the risk or functionality gap identified.** |
| 2.1.1  Can or will you be able to prove the information or data is authentic? |  |  |
| 2.1.2  Can or will you be able to identify or prevent unauthorised changes to the information or data? |  |  |
| 2.1.3 When you access information or data, can or will you be able to access all relevant parts of it? |  |  |
| 2.1.4 Does or will the system meet the Archives' minimum metadata requirements? |  |  |

|  |  |  |
| --- | --- | --- |
| **Module 2: Disposal is accountable** | **Yes – Document details** | **No – Where a risk or gap was identified in Phase 2 – indicated by a 'No' response – document the solution to address the risk or functionality gap identified.** |
| 2.2.1 Is or will disposal be controlled, systematic and recorded? |  |  |
| 2.2.2 Where there is more than one disposal class, can or will you be able to manage the different disposal classes? |  |  |
| 2.2.3 Can or will you be able to manage the system's control records in line with your accountability needs? |  |  |
| 2.2.4 Is or will destruction be in line with the Information Security Manual and other relevant policies? |  |  |

|  |  |  |
| --- | --- | --- |
| **Module 3: Export – import** | **Yes – Document details** | **No – Where a risk or gap was identified in Phase 2 – indicated by a 'No' response – document the solution to address the risk or functionality gap identified.** |
| 2.3.1 Are you or will you be able to export the information or data in a usable format? |  |  |
| 2.3.2 Are you or will you be able to import information or data into the system? |  |  |

|  |  |  |
| --- | --- | --- |
| **Module 4: Reporting** | **Yes – Document details** | **No – Where a risk or gap was identified in Phase 2 – indicated by a 'No' response – document the solution to address the risk or functionality gap identified.** |
| 2.4.1 Can or will the system generate reports on your information or data management processes? |  |  |
| 2.4.2 Can or will the system create automatic alerts in response to specific triggers? |  |  |