|  |  |
| --- | --- |
|  | |
|  | Security Impact Assessment (SIA) Form  (Elastic Cloud)  The document needs to be filled out for all proposed new projects to assess the security risk that they may pose to the Agency.   |  |  |  |  | | --- | --- | --- | --- | | Version | Date | Author | Comments | | 2.0 | Aug 18 | InfoSec | Format changes | | 3.0 | Aug 21 | InfoSec | Added in Business Consequences section | |

**Contents**

[1 About the project 2](#_Toc39055656)

[2 Details of data/information affected by this project 2](#_Toc39055657)

[3 Risk assessment 4](#_Toc39055658)

[4 Additional Questions 5](#_Toc39055659)

[5 Information Security Assessment 6](#_Toc39055660)

[6 Appendix A - Impact & Likelihood Matrix 6](#_Toc39055661)

[7 Appendix B - SIA Risk Matrix & Scoring 7](#_Toc39055662)

# About the project

## General Information

|  |  |  |  |
| --- | --- | --- | --- |
| Requested by | Department | Project name | Ref number |
| Sandeep Verma | TD3, Engineering | DevOps | DevOps- Elastic Cloud |

## Project details

|  |
| --- |
| Description of project |
| We are migrating from the current DevOps platform that Accenture provides as a managed service, to a new platform. Elastic cloud enables you to quickly and easily find information, gain insights, and protect your technology investment whether you run on Amazon Web Services, Microsoft Azure, or Google Cloud. |

## Project delivery

|  |  |  |  |
| --- | --- | --- | --- |
| Expected delivery date | Estimated size of the project | Current project stage gate | Project’s remit: Divisional, department or agency |
| 31st March (project is scheduled to end) |  |  | DevOps will be managed by TD3 Engineering with interest from Delivery, Application Management, DKIM and vendors. |

## Primary reason for privacy and security impact assessment

|  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- |
| New project? | Change to an existing project? | Developing or procuring a new technology? | Implementing a new application, system or technology? | New or updated business process? | Updating a system that results in new privacy risks? |
| Yes | No | Yes | Yes | Updated | No |

(Please answer Yes or No)

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| Project Owner | Information Asset Owner (IAO) | Information Custodian (IC) | Division | Name or ref # of asset(s) in question |
| Engineering |  |  | TD3 |  |

# Details of data/information affected by this project

## Security classification of the data

|  |  |  |  |
| --- | --- | --- | --- |
| Official | Secret | Top secret | Is or will this data be in the public domain? |
| Yes | No | No | No |

## Type of data

Which of the following categories best describe the type of data affected by this project or change?

Against each applicable type please describe how the data will be used or processed. These descriptors might help you: (collected; stored; shared internally/externally)

|  |  |  |
| --- | --- | --- |
| Data types | Indicate which data types apply | How will you use this data? |
| Personal data | No |  |
| Special category personal data | No |  |
| Personal / special category personal data processed for law enforcement purposes | No |  |
| Credit card information | No |  |
| Other financial data | No |  |
| Intellectual Property | No |  |
| Commercially sensitive information | Yes | Beats will be used to ship logfile data to Elastic Cloud where it will be indexed and made available to Kibana for visualisation.  The data is about metrics. |
| Other data type (please specify) | n/a |  |

## Data Protection considerations

If you will be processing information about living individuals (personal data) have you consulted [dataprotection@mhra.gov.uk](mailto:dataprotection@mhra.gov.uk) to consider whether you need to do any of the following?

|  |  |
| --- | --- |
| **Data Protection consideration** | **Yes/No** |
| Undertake a Data Protection Impact Assessment | n/a |
| Write or amend a cookie policy | n/a |
| Update a Privacy Notice | n/a |
| Update the Asset register | n/a |
| Update our Record of Personal Data Processing (Article 30 register) | n/a |

## Data location and retention

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| Where geographically will the data be at rest (UK/ EU/ USA/ Other) | Where geographically will the data be accessible from (UK/ EU/ USA/ Other) | What is the data retention requirement for this data | Can the project satisfy data retention and any other specific handling/storage requirements | \*if ‘no’, please describe corrective action |
| UK | UK | No time limits | Yes | n/a |

# Risk assessment

Please use the risk matrices in Appendix A and B to assess the inherent and residual risks

## Impact

**Confidentiality:** This is the about ensuring that the data is only available to those that are authorised to see it. It concerns preventing sensitive information being accessed by the ‘wrong’ person.

**Integrity:** This is the maintaining the accuracy of data. Preventing it being tampered with to maintain its trustworthiness.

**Availability:** This is about ensuring the data is available to those whenever it’s needed.

### **Business Consequences**

|  |  |
| --- | --- |
| Please use this section to articulate the business consequences of a breach in the Confidentiality, Integrity or Availability of the system. | |
| What will be the business consequences of unintended or unauthorised disclosure of information (worst case scenario) | Outsiders may have access to dashboard, visualisations of metrics.  This means that they will be able to analyse the performance metrics of our legacy AO applications but not be able to make any changes. |
| What will be the business consequences of errors in information or of deliberate manipulation of information (worst case scenario) | Outsiders can create new charts and modify appearance of dashboards but they can’t change any data.  Note: Check elastic cloud and see if outsiders can manipulate the data in Kibana.    Ans: If a user’s account has been compromised and outsiders gain access to a user’s account, outsiders can manipulate the data in Kibana. |
| What will be the business consequences of prolonged outage (worst case scenario) | The DevOps team will not be able to monitor performance or availability of AO applications. Automated alerts will not be functioning so the DevOps team will not be able to respond.  This means we can’t monitor spikes in usage, but the AO applications will continue to run.  We will still have access to logfiles so we can manually trace through the logs to identify any abnormal usage patterns.  As a backup we can setup Azure Monitor to offer a redundant monitoring service.  Note: Can we continue to use Beats to ship data into Azure Monitor. Can Beats be used to replace log analytics in Azure. How can we set up Azure monitoring easy to move away from elastic cloud.  Ans: Elastic cloud is now running in Azure Cloud as a third-party software solution and can be deployed from Azure marketplace. |

### **Impact Rating**

|  |  |  |
| --- | --- | --- |
| Assuming that no controls are in place please estimate the level of impact to the Agency or customers if there was a breach in Confidentiality | Assuming that no controls are in place please estimate the level of impact to the Agency or customers if there was a breach in Integrity | Assuming that no controls are in place please estimate the level of impact to the Agency or its customers if there was a loss of Availability |
| Insignificant | Low | Low |

Please respond: Critical / High / Medium / Low / Insignificant

## Controls and residual risks

|  |
| --- |
| Residual risk: Confidentiality |
| Now, please describe the controls already in place, or to be included in the solution design, that will reduce the impacts described above and the likelihood of the impact occurring against Confidentiality |
| Research: can we use SAML Azure AD on elastic cloud, check in elastic cloud free trial version.  Ans: We are able to use SAML AAD SSO for Elasticsearch and this can be done by creating in Azure portal Enterprise application 🡪 Configure Enterprise Application for Single Sign-on 🡪  https://www.elastic.co/blog/saml-based-single-sign-on-with-elasticsearch-and-azure-active-directory  Users will need an account to access Elastic Cloud which is tied to Azure AD.    Read-only, read-write permissions can be granted to individuals for access to specific metrics, dashboards and visualisations. This way we can reduce who has visibility to specific dashboards, metrics and visualisations in Elastic Cloud. |

|  |
| --- |
| Residual risk: Integrity |
| Now, please describe the controls already in place, or to be included in the solution design, that will reduce the impacts described above and the likelihood of the impact occurring against Integrity |
| Users will need an account to access Elastic Cloud which is tied to Azure AD.    Read-only, read-write permissions can be granted to individuals for access to specific metrics, dashboards and visualisations. This way we can reduce who has visibility to specific dashboards, metrics and visualisations in Elastic Cloud. |

|  |
| --- |
| Residual risk: Availability |
| Now, please describe the controls already in place, or to be included in the solution design, that will reduce the impacts described above and the likelihood of the impact occurring against Availability |
| If Elastic Cloud went down then we just loose observability of the performance of the AO applications. We will have 2 DevOps engineers in the target operating model. With the limited time, they will only be accessing Elastic cloud a few times a day to a few times a week. If we lost a day’s worth of access, the consequences would be negligible.  We will still have access to logfiles so we can manually trace through the logs to identify any abnormal usage patterns.  As a backup we can setup Azure Monitor to offer a redundant monitoring service.  We will have two nodes so if one goes down |

# Additional Questions

|  |  |
| --- | --- |
| What is the number of admin accounts/basic user accounts? | 2 Admin accounts within DevOps Engineering team and basic user accounts. |
| Are access control restrictions in place, including user privileges? | Yes |
| Is the information that is being used backed up? |  |
| Is the software patched/up to date? |  |
| Is the data at rest or in transit encrypted? |  |
| Does the company hold any security accreditations? (e.g. ISO27001, ISO27002 or alignment to these…) | Elastic Cloud is a service that enables you to quickly and easily find information, gain insights, and protect your technology investment. It is compliant with SOC 2, ISO 27001, ISO 27017 and ISO 27018, CSA STAR, HIPAA, FedRAMP, SOC 3, ISAE 3000. |
| Do any third parties have access to the systems/information? If so how is access defined? | Yes |
| If applicable, please provide a description of the software along with details of the provider | It enables you to quickly and easily find information, gain insights, and protect your technology investment.  <https://www.elastic.co/> |

# Information Security Assessment

**\*\*To Be Completed by Information Security Only\*\***

## Information Security General Information

|  |  |  |  |
| --- | --- | --- | --- |
| Information Security Impact Assessment Matrix | | | |
| CIA | Impact | Likelihood | Risk rating score (Impact x Likelihood) |
| Confidentiality |  |  |  |
| Integrity |  |  |  |
| Availability |  |  |  |

**Impact:** 5(Critical) 4(High) 3(Medium) 2(Low) 1(Insignificant)

**Likelihood:** 5(Almost Certain) 4(Likely) 3(Possible) 2(Unlikely) 1(Remote)

## Overall security rating

|  |  |  |
| --- | --- | --- |
| Information Security team overall risk assessment | What action is recommended because of this assessment? | Are further controls necessary to mitigate the likelihood or impact of C, I or A. If so what? |
|  |  |  |

# Appendix A - Impact & Likelihood Matrix

**Impact:**

|  |  |  |
| --- | --- | --- |
| Scale | | Impact |
| 5 | Critical | Prevents achievement of The Agency objectives or has highly damaging impact on Agency operational effectiveness or reputation. . |
| 4 | High | Significant detrimental effect on achievement of Agency corporate objectives in the longer term. National media criticism. |
| 3 | Medium | Impacts at local level on elements of efficiency, output and quality which impacts on the outcome of long-term Agency corporate objectives. Potential for negative local media coverage |
| 2 | Low | Impact at local level on short term goals within their objectives without affecting long term achievement of Agency corporate objectives. |
| 1 | Insignificant | Minor and containable impact on achievement of local (establishment / business area) objectives. |

**Likelihood:**

|  |  |  |
| --- | --- | --- |
| Scale | | Likelihood |
| 5 | Almost certain | As a result of the controls that are in place/not in place the likelihood of the event occurring is almost certain to occur. |
| 4 | Likely | As a result of the controls that are in place/not in place the likelihood of the event occurring is likely to occur. |
| 3 | Possible | As a result of the controls that are in place/not in place the likelihood of the event occurring is possible. |
| 2 | Unlikely | As a result of the controls that are in place/not in place the likelihood of the event occurring is unlikely. |
| 1 | Remote | As a result of the controls that are in place/not in place the likelihood of the event occurring is remote. |

# Appendix B - SIA Risk Matrix & Scoring

[Please use the above matrix to help you arrive at a rating in **Section 3**]

|  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- |
|  |  | **Likelihood** | | | | |
|  |  | **1 Remote** | **2**  **Unlikely** | **3**  **Possible** | **4**  **Likely** | **5**  **Almost certain** |
| **Impact** | **5**  **Critical** | 5 | 10 | 15 | 20 | 25 |
| **4**  **High** | 4 | 8 | 12 | 16 | 20 |
| **3**  **Medium** | 3 | 6 | 9 | 12 | 15 |
| **2**  **Low** | 2 | 4 | 6 | 8 | 10 |
| **1**  **Insignificant** | 1 | 2 | 3 | 4 | 5 |

|  |  |  |
| --- | --- | --- |
| Guide to overall risk assessments and impact on project and change. | | |
| 5 | Critical | Serious issues with this project or change which must be addressed before progressing further. . |
| 4 | High | Significant security issues with this project or change that need to be corrected and agreed at the next stage gate. |
| 3 | Medium | There are security issues with this project or change that need to be mitigated before go-live. Explore options for mitigating impact. |
| 2 | Low | Project or change can proceed, provided the security team are updated throughout the project lifecycle till go-live. Certain risks can be accepted if the SIRO wishes but these need to be noted. |
| 1 | Insignificant | Minor and containable security risks to be noted. |