

**TECHNOLOGY RISK - PROJECT & PROGRAMME RISK ASSUANCE**

**IT Control Set (ITCS)’s**

Compliance Requirements Report for: INVP 5917E Master Data Platform/Tool

.

|  |  |
| --- | --- |
| **Document Control** | |
| Data Classification: | **INTERNAL** |
| Author: | Jasbir Singh Randhawa |
| Date: | Apr 05, 2021. |
| Version | 1.0 |

Introduction

Technology Risk Programme Risk Assurance (TRPA) have completed an assessment of the IT Control Set (ITCS) based on detail obtained and have documented within this report the controls that are required and should be delivered as part of the solution.

TRPA support project teams in understanding the ***“what”***: what is required to mitigate risks and satisfy the Global IT Control Set, but not the ***“how”***. The how or design of the controls is the responsibility of projects and programmes in collaboration with key stakeholders.

Various aspects of the project have been considered to determine the project risk classification;

* Data sensitivity/classification
* Regulatory requirements
* System architecture (e.g. SaaS, PaaS, on NG network)
* Internet facing
* Support model
* User base
* Wireless
* Operational Criticality

Ongoing engagement with TRPA is based on the classification and will differ:

**Low** – available should the project require any advice.

**Medium** – regular 1-2-1 (monthly) with the PM to monitor progress / assist with any risk and control related queries (consultancy), provide a risk assurance opinion and go live decision.

**High** – involvement in project meetings, change boards, project management board’s etc, monitor progress through each stage providing consultancy, provide risk assurance opinion and go live decision.

***The level of involvement with the project and any additional TRPA costs will be discussed and agreed in advance with project stakeholders.***

**Changes to project scope/architecture:** Should changes to the project scope or planned architecture occur, you should re-engage with TRPA to ensure controls applicability is reassessed.

Project Overview

|  |  |
| --- | --- |
| Project ID | INVP 5917E |
| Project Name | INVP 5917E\_Master Data Platform Tool |
| **Project Risk Classification** | **HIGH** |
|  |  |
| Project Description | As per the “Fixing Data” paper presented in April 2020 to executives by Chief Data Officer Charles Zentay, unless we “Fix Data” our security, major programs, and financial and operational performance are at risk. In addition, clean, organized Data is like a common language and underpins Business Analytics and Digital Transformation. To overcome our data problems, the key components are (i) building upon the progress of Data BMS to improve capabilities of Data Governance & Stewardship; (ii) implementing standardized Data Tools & Platforms; and (iii) driving Master Data Solutions in each major domain (Employee, Customer, Asset, Product, Vendor, and Finance). To ensure rapid action and coordination, it is imperative to agree on a “Hub-and-Spoke” operating model, an owner to drive Master Data for each major domain, and a holistic funding model. |
| Project Go Live Date | TBD |
| Region | US / UK |
| Business Area / Org | Group Function |
| Business Partner | *Ed*  *Brodsky* |
| Program Manager | *Ed*  *Brodsky* |
| Project Manager | TBD |
| Development Dir/Mgr. |  |
| IT Solution Delivery Type | **Medium & Large Scale (Unknown or Net-New Technology)** |
| Data Security Classifications | **Confidential** |
| Data Business Criticality | Critical |
| Data Type | Financial, Operational |
| External Information Recipient | TBD |
| Cloud Based Solution | TBD |
| System Accessibility Type | Intranet |
| Use of Third Party & Supplier Services | Yes |
| Third Party & Supplier Types | Vendor |
| Critical National Infrastructure Impact | No |

# 

# Impacted External Regulations

The ITPRC responses identified which external regulatory requirements are applicable to the project. The results of which are shown below:

K**ey:** In-scope = ****Not in-scope = 

**GDPR / Data Privacy:** If the proposed technology solution includes processing, storing and/or transmitting (customer) privacy data, TRPA strongly recommend that the project team engage with Data Privacy and Records Management (Deborah Tamborski for the US and Glen Truman for the UK) to determine if a Privacy Impact Assessment is needed and ensure compliance with all relevant data privacy legislation.

|  |  |  |
| --- | --- | --- |
| Regulation | In-scope | Rationale |
| US Privacy Law |  | The solution will process or store Personally Identifiable Information. |
| GDPR | **** | The solution will process or store Personally Identifiable Information, of UK or EU subjects. |
| HIPPA |  | The solution will not process or store protected health information (PHI) for subjects/residents. |
| NERC-CIP |  | The solution does not relate to Bulk Electricity Systems for electrical transmission and generation in North America. |
| NIS-D\* |  | Disruption to the solution would impact National Grid’s ability to operate essential services in the UK. |
| PCI-DSS |  | The solution will not store, process, and/or transmit payment cardholder data. |
| Sarbanes-Oxley  (SOX) | **** | The solution will not impact financial systems or applications determined to be in scope or moving into scope for SOX. |

**3rd Parties/Vendors:** If a 3rd Party/Vendor is involved in the delivery or the ongoing support of the proposed technology solution TRPA strongly recommend that the project team engage and obtain the relevant assurance report(s) (SOC 1 and/or 2) to determine if any user complimentary controls (National Grid controls) are required.

# Impacted Global IT Control Categories

The following recommendations have been determined by taking-into-account external regulatory requirements, risks associated with the solution architecture, the data being processed and/or business activities supported by the solution.

| Category | Applicable? | Indicative Risk | Total Controls in Category | Controls in Scope |
| --- | --- | --- | --- | --- |
| **CYBER SECURITY** | | |  |  |
| Account Access Control | **** | Unauthorized persistent or privileged access to company information systems and networks could increase the likelihood of inappropriate use or loss of data that impacts the confidentiality, integrity and availability of data used in critical business processes. | **34** | 18 |
| Awareness and Training | **** | The lack of security awareness and proper training of personnel resulting in preventable cyber and physical security failures leading to the disruption of critical business processes. | **6** | 1 |
| Continuous Monitoring | **** | Undetected and monitored malicious activity present on information systems and networks could result in cyber security failures leading to the disruption of critical business processes. | **19** | 9 |
| Cyber Security Management |  | Unapproved and inconsistent configurations of information systems being installed could introduce cyber and physical security issues, and system failures resulting in a disruption to critical business processes. | **7** | 0 |
| Identification & Authentication | **** | Ineffective identification and authentication controls could lead to the repudiation of unauthorized account access usage resulting in the inappropriate use or loss of data and therefore impact the confidentiality, integrity and availability of data used in critical business processes. | **9** | 7 |
| Incident Response |  | The inability to appropriately handle cyber security incidents could result in cascading, forensics, or reporting failures leading to the disruption of critical business processes. | **14** | 0 |
| Network Security | **** | Weak security controls over network hardware and logical parameters including network capacity could result in the unavailability of essential communication between information systems leading to the disruption of critical business processes. | **14** | 5 |
| Risk Management |  | The inability to identify, analyse and implement IT risk decisions in a prioritized manner could result in cyber security failures leading to the disruption of critical business processes. | **10** | 0 |
| Security Architecture |  | Ineffective design and implementation of system environments could result in cyber security incidents and system failures leading to the disruption of critical business processes. | **3** | 0 |
| System Logging | **** | The lack of an audit trail could result in the inability to ensure users are accountable for their actions, are adhering to security policies, and in the event that information systems are misused, or a breach occurs, to conduct forensic investigations. | **8** | 5 |
| Threat and Vulnerability Management | **** | Unmanaged or remediated zero-day vulnerabilities discovered in information systems could result in the exploitation of system control weakness, security breaches, and information system outages leading to the disruption of critical business processes. | **17** | 4 |
| **Data Management** | | |  |  |
| Data Security | **** | The lack of designed or implemented safeguards to ensure secure, controlled collection, storage, transmission, and disposal of information throughout the data lifecycle could result in the breach of sensitive personal data, or non-public financial information leading to the disruption of critical business processes. | **11** | 4 |
| **IT Operations & Performance Management** | | |  |  |
| Asset Management | **** | Not understanding the full scope of information systems present within the environment and not having a process to manage the systems could result in cyber security, and system failures leading to the disruption of critical business processes. | **14** | 3 |
| Capacity, Availability, & Performance Management | **** | Not understanding the capacity, availability and performance requirements of systems could impact the operation of information systems leading to the disruption of critical business processes. | **8** | 5 |
| Configuration Management | **** | Unapproved and inconsistent configurations of information systems being installed could introduce system failures resulting in a disruption to critical business processes. | **11** | 6 |
| Change Management | **** | Unauthorized changes made to information systems or through unrestricted inappropriate access to production environments could result in system failures leading to the disruption of critical business processes. | **13** | 6 |
| Patch Management | **** | Known identified information systems vulnerabilities not patched in a timely manner could result in cyber security breaches and other systems failures leading to the disruption of critical business processes. | **11** | 4 |
| Problem Management |  | System incidents, outages and other problems impacting information systems could go undetected and unresolved which could result in the prolonged disruption of critical business processes and increased likelihood of future disruption if no root cause analysis is performed. | **4** | 0 |
| **IT Resilience** | | |  |  |
| Backups | **** | Data and system backups are not available to enable timely, complete and accurate restoration of data leading to the disruption of critical business processes. | **6** | **5** |
| Business Continuity | **** | The absence of a formalized and approved business continuity plan that is tested on a periodic basis could lead to a system failure/degradation, cybersecurity breach, or site failure resulting in delayed or inability to effectively obtain critical business operations. | **8** | **2** |
| Disaster Recovery | **** | The absence of a formalized and approved disaster recovery plan that is tested on a periodic basis could lead to a system failure/degradation, cybersecurity breach, or site failure resulting in delayed or inability to effectively obtain critical business operations. | **10** | **2** |
| |  |  |  | | --- | --- | --- | | **Physical Security** |  |  | | | | | |
| Facility Security |  | The lack or failure of facility environmental protection controls could result in the damage or destruction of information systems and other company owned equipment leading to the disruption of critical business processes. | **5** | 0 |
| People Security |  | Malicious activity is performed by personnel hired by the company or personnel present within company facilities resulting in cyber and physical security failures. | **9** | 0 |
| Physical Security |  | Inappropriate access or the lack of protective measures to physical locations could result in the abuse or tampering of facilities, equipment, or other information system assets leading to the disruption of critical business processes. | **22** | 0 |
| |  | | --- | | **Supply Change Management** | | | |  |  |
| Service Level Agreements |  | The absence of a comprehensive strategy to manage supplier (3rd and 4th party) sourcing, selection, control setting and assurance requirements (including technology and security), and contractual enforcement could result in the operational and regulatory risk exposure for the company leading to the disruption of critical business processes or regulatory scrutiny, sanctions and fines. | **3** | **0** |
| System and Services Acquisition | **** | The absence of a comprehensive strategy to manage supplier (3rd and 4th party) sourcing, selection, control setting and assurance requirements (including technology and security), and contractual enforcement could result in the operational and regulatory risk exposure for the company leading to the disruption of critical business processes or regulatory scrutiny, sanctions and fines. | **7** | **2** |

# Required Controls Matrix

The matrix provides detail of the Controls that are required to be delivered as part of the solution.



## **Appendix A - Glossary of Terms**

|  |  |  |
| --- | --- | --- |
|  | Term | Definition |
| **IT**  **Solution**  **Delivery** | Application Maintenance Event | Under the SDF, these are projects that are delivering small changes to current technology solutions leveraged by National Grid's DEV/QA/PROD environments. |
| Example(s): Enhancements, Infrastructure Upgrades, and Patches. |
| Medium & Large Scale (Known/Existing Technology) | Under the SDF, these are projects that are introducing medium to large scale changes to current technology solutions leveraged by National Grid's DEV/QA/PROD environments. |
| Example(s): Infrastructure changes, hosting changes, and/or licensing of modules or functionality for current tools such as SAP, GBE, Salesforce, among others |
| Medium & Large Scale (Unknown or Net-New Technology) | Under the SDF, these are projects that are introducing medium to large scale changes into the National Grid DEV/QA/PROD environments via new technology solutions not used in the past. |
| Example(s): Infrastructure changes, hosting changes, and/or licensing of modules or functionality for new applications and/or hosting providers |
| **Data**  **Security**  **Classifications** | Publicly Available | Information approved for publication outside of the company. Unauthorised disclosure will not cause any harm to National Grid businesses, employees or customers. |
| Example(s): information published on external websites and social media. |
| Internal Use Only | Information for National Grid staff and authorised contractors. The disclosure or loss of such information would be inappropriate and could have a negative impact on National Grid. |
| Example(s): information published on Infonets, in internal policies or in procedures. |
| Confidential | Information that is commercially or operationally sensitive, where disclosure or loss could have an impact on National Grid businesses, not limited to financial or reputational damage. This could also include information about individuals where a duty of confidentiality is owed. |
| Example(s): staff performance and reward records, commercial contract/tender information. |
| Strictly Confidential | This refers to information that is commercially or operationally sensitive and where disclosure would have a significant impact on National Grid, its assets or its individuals. Information is to be addressed to named groups or individuals only. |
| Example(s): critical electricity or gas networks and related computer system operational details, possible acquisition of commercial information, Executive Board discussions. |
| **Business**  **Data**  **Criticality Types** | Business Critical Data | Information that is considered both "Operationally Critical" and "Critical" as Business Data Criticality Types. |
| Data Type | None |
| IT Operational |
| OT operational |
| Commercial |
| Personal Identifiable Information (PII) |
| Health & Medical |
| Financial |
| Payment Card Information (PCI) |
| Other - Please explain |
| Operationally Critical | Data/information that is deemed essential to the continuance and delivery of a set of activities/processes that are deemed essential to delivering the primary objective of the day-to-day operation and control of the gas and electricity networks. |
| Critical | Data/information that is deemed essential to the continuance and delivery of activities/processes that are deemed critical to maintaining legal, regulatory, commercial and business responsibilities. |
| Core | Any data/information that is deemed essential to the continuance and delivery of any activity/process that is central to National Grid’s normal day-to-day activities. Such data would affect the ability of the company to manage its businesses effectively with consequential impacts on business profitability and reputation. |
| Efficiency and Performance | Data that if incomplete, inaccurate or missing is unlikely to have a significant impact upon the public or the business in the short to medium term but may impact on the efficiency and performance of National Grid over time. |
| **Information Recipients** | External Organizations | Regulators, Auditing Entities, Trading Partners, Third Parties, Suppliers, among others. |
| **Cloud** | Private Cloud | Data separated both logically and physically. |
| Example(s): Dedicated infrastructure and logical space. |
| Hybrid Cloud | Data logically separated but not physically |
| Example(s): Same infrastructure to other clients, but separate logical space. |
| **System**  **Accessibility**  **Types** | Public Cloud | Data not logically or Physically separated |
| Example(s): Same infrastructure and logical space to other clients. |
| Local Access | The solution requires an individual to be physically present to access it. |
| Example(s): Current production environments such as GMS, EMS, direct server access, among others |
| Intranet Access | The solution enables an individual to only access it through the corporate VPN environment. |
| Example(s): Current production environments such as SAP, GBE, Salesforce, among others |
| Internet Access | The solution enables an individual to access it publicly from outside the corporate VPN environment. |
| Example(s): Current production environments such as nationalgrid.com |
| **Use of Third Party**  **& Supplier Services** | Delivery Services | Service offering(s) that revolve around the Design, Development & Implementation of an IT Solution or Product. |
| Continued Management Services | Service offering(s) that revolve around the Post-Production Operations, Administration, and/or Maintenance Support of an IT Solution or Product. |
| **Third Party**  **& Supplier Types** | Ecosystem Partner | A Third Party who is contracted at the enterprise level as a preferred vendor, to provide pre-defined IT services long term across multiple systems and projects. |
| Example(s): ADAM Partners |
| Vendor | A Third Party who is not considered an Ecosystem Partner, who is performing short term work for National Grid under a direct contractual business relationship. |
| Example(s): Non-ADAM Partner, an entity providing SaaS Solution being contracted |
| Sub-Contractor/Processor | A Third party performing work for National Grid without a direct contractual business relationship (i.e. A vendor's third party partner). |
| Example(s): An entity providing infrastructure services to a SaaS solution provided by a vendor being contracted by National Grid. |

* End