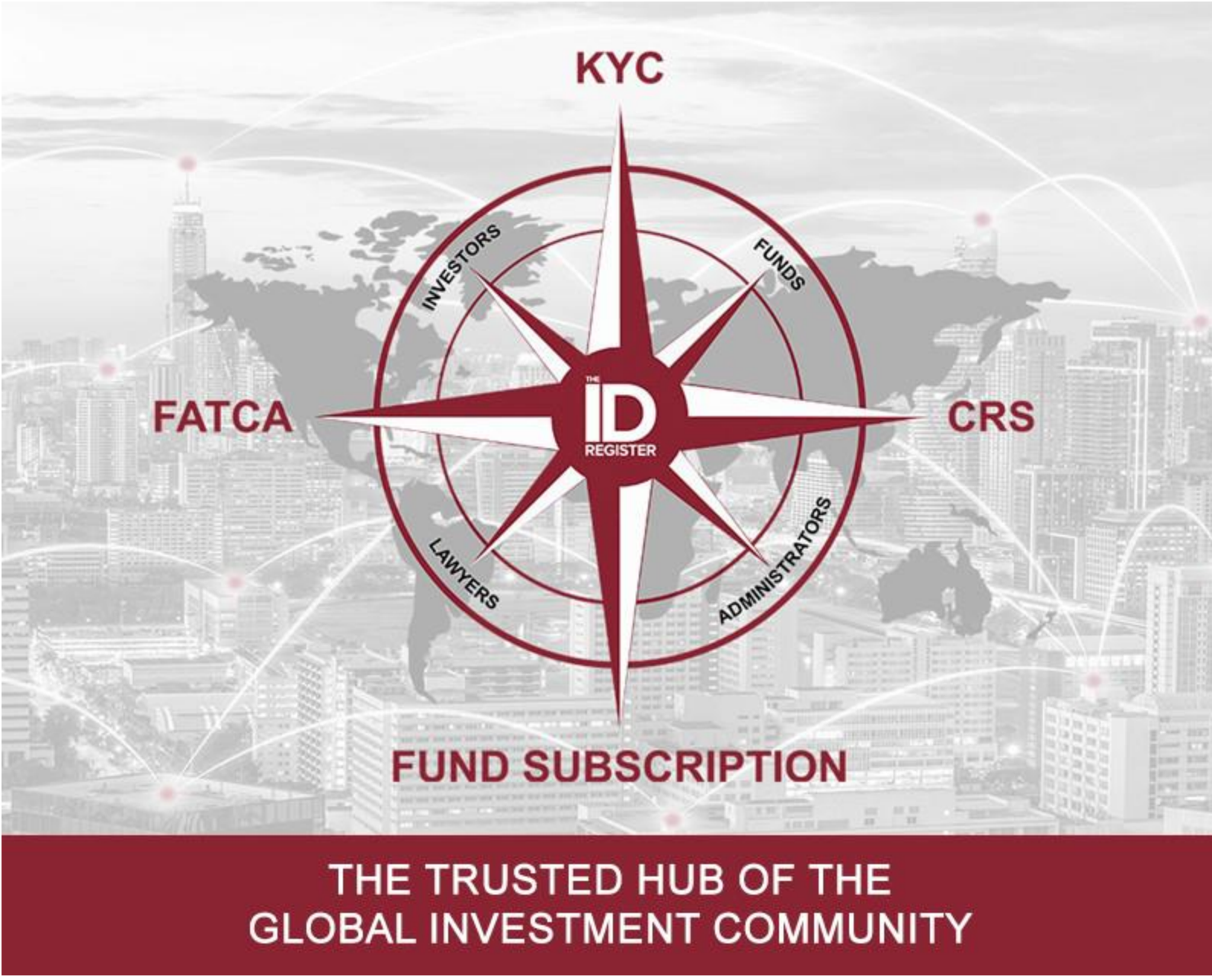


THE TRUSTED HUB OF THE
GLOBAL INVESTMENT COMMUNITY

THE ID REGISTER

Information Security

31 August 2021

Europe: +44 20 3787 4138
US: 1-800-392-1325

SUMMARY

The ID Register provide due diligence support to investors and funds, focused on sophisticated institutional investors making long-term investments into funds in multiple jurisdictions. They save investors from having to provide due diligence information multiple times by aggregating information and submitting it to funds automatically.

The ID Register is committed to maintaining and continually improving information security to meet our responsibilities to our clients and regulators and to reduce exposure to legal sanction, risk, and reputational damage.

We are committed to ensuring:

- The confidentiality of client information.
- The integrity of our information.
- The availability of our information.
- That regulatory and legal requirements are met.

FRAMEWORK

We have built our application with respect to the following standards and frameworks:

- NIST Cyber Security Framework
- ISO/IEC 27001
- SOC 2

NIST CYBERSECURITY FRAMEWORK

The **NIST Cybersecurity Framework** is drafted by the National Institute of Standards and Technology (NIST) to address cybersecurity and provides a uniform set of rules, guidelines, and standards for organisations to use across industries. The security controls in the framework are broken up into 5 key functions. These functions are: Identify, Protect, Detect, Respond, Recover.

Identify: The Identify function is focused on laying the groundwork for an effective cybersecurity program. This function assists in developing an organisational understanding to manage cybersecurity risk to systems, people, assets, data, and capabilities.

Protect: The Protect function outlines appropriate safeguards to ensure delivery of critical infrastructure services and supports the ability to limit or contain the impact of a potential cybersecurity event.

Detect: Detecting potential cybersecurity incidents is critical and this function defines the appropriate activities to identify the occurrence of a cybersecurity event in a timely manner.

Respond: The Respond function focuses on appropriate activities to take action in case of a detected cybersecurity incident and supports the ability to contain the impact of a potential cybersecurity incident.

Recover: The Recover function identifies appropriate activities to renew and maintain plans for resilience and to restore any capabilities or services that were impaired due to a cybersecurity incident. Timely recovery to normal operations is impressed upon, to reduce the impact from a cybersecurity incident.

ISO/IEC 27001

The ID Register is also looking to be certified ISO/IEC 27001 in the near future.

ISO/IEC 27001 requires that management:

- Systematically examine the organisation's information security risks, taking account of the threats, vulnerabilities, and impacts.
- Design and implement a coherent and comprehensive suite of information security controls and/or other forms of risk treatment (such as risk avoidance or risk transfer) to address those risks that are deemed unacceptable; and
- Adopt an overarching management process to ensure that the information security controls continue to meet the organisation's information security needs on an ongoing basis.

SOC 2

SOC 2 compliance is part of the American Institute of CPAs' Service Organisation Control reporting platform. Its intent is to ensure the safety and privacy of customers' data. It outlines five trust service principles of security, availability, processing integrity, confidentiality, and privacy of customer data as a framework for safeguarding data.

The five trust services criteria are detailed below:

- Security refers to the protection of information and systems from unauthorized access. This is through the use of IT security infrastructures such as firewalls, two-factor authentication, and other measures to keep data safe from unauthorized access.
- Availability is whether the infrastructure, software, or information is maintained and has controls for operation, monitoring, and maintenance. This criterion also gauges whether the organisation maintains minimal acceptable network performance levels and assesses and mitigates potential external threats.
- Processing integrity ensures that systems perform their functions as intended and are free from error, delay, omission, and unauthorized or inadvertent manipulation. This means that data processing operations work as they should and are authorized, complete, and accurate.
- Confidentiality addresses the organisation's ability to protect data that should be restricted to a specified set of persons or organisations. This includes client data intended only for company personnel, confidential company information such as business plans or intellectual property, or any other information required to be protected by law, regulations, contracts, or agreements.
- Privacy criteria speaks to an organisation's ability to safeguard personally identifiable information from unauthorized access. This information generally takes the form of name, social security, or address information or other identifiers such as race, ethnicity, or health

information.

As of August 2021, KPMG Guernsey is currently looking at our SOC 2 controls so that we can be certified SOC 2 Type 1 by November 2021.

GOVERNANCE

The board of directors and management, at all levels, demonstrate through their directives, actions, and behavior the importance of integrity and ethical values to support the functioning of the application.

The ID Register employs controls globally through enforcement of policies, standards, and guidelines covering information security and risk. Each policy document is controlled and maintained by a specific owner.

The ID Register policies include, but are not limited to:

- Defined information security responsibilities for employees, contractors, and 3rd parties.
- Testing to identify missing controls or control deficiencies.
- Acceptable usage policies for all users including but not limited to, email and internet usage.
- Defined criteria for access control, including need to know, least privilege principle, unique ID, password complexity, access approvals, recertification transfer and leavers processes, privileged access, and remote access controls.
- Software development life cycles for applications including code review, separation of duties, security reviews for web services.
- Change control and disaster recovery / business continuity planning requirements.
- Detailed instructions for encryption, secure data transmission and destruction.
- End User Environment policies, covering data extraction, non-IT managed data processing, secure storage destruction and remote working.
- Technical configuration and control settings for IT infrastructure, networks, and platforms.
- Physical security.

RISK MANAGEMENT

The ID Register utilises risk management to identify, report and manage risks across the organisation. Information security frameworks within The ID Register follow internationally recognised best practice standards.

Risk assessments are performed periodically to address changes in the organisation's information security requirements or risk appetite and when significant changes occur. The ID Register performs risk assessments on a variety of assets within the organisation. These may be physical assets, people, processes, software, and information.

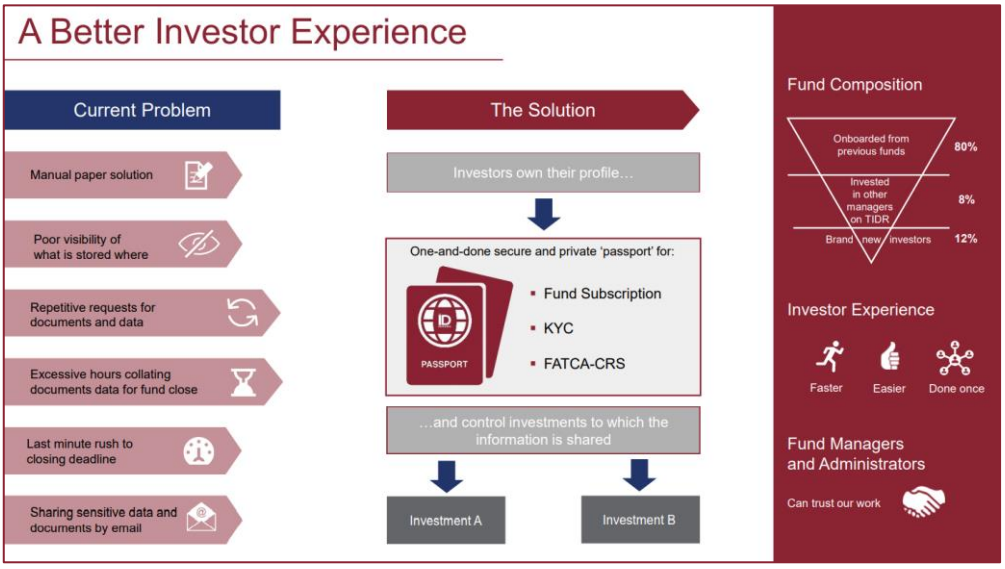
For example, regular information security risk assessments are performed upon application and infrastructure technologies to:

- Identify, quantify, and manage information security risks to achieve business objectives.
- Provide means to identify activities and factors which pose the greatest security risk to The ID Register.
- Ensure information security issues are managed according to their risk rating, and that controls are proportional to the level of risk discovered.

- Provide an enterprise view of information security risks and respective remediation plans to develop the information security strategy.
- Plan the deployment of resources to areas that provide the greatest reduction in risks to customer / corporate information.
- Assess all aspects of information security risks, threats, and vulnerabilities to our assets.

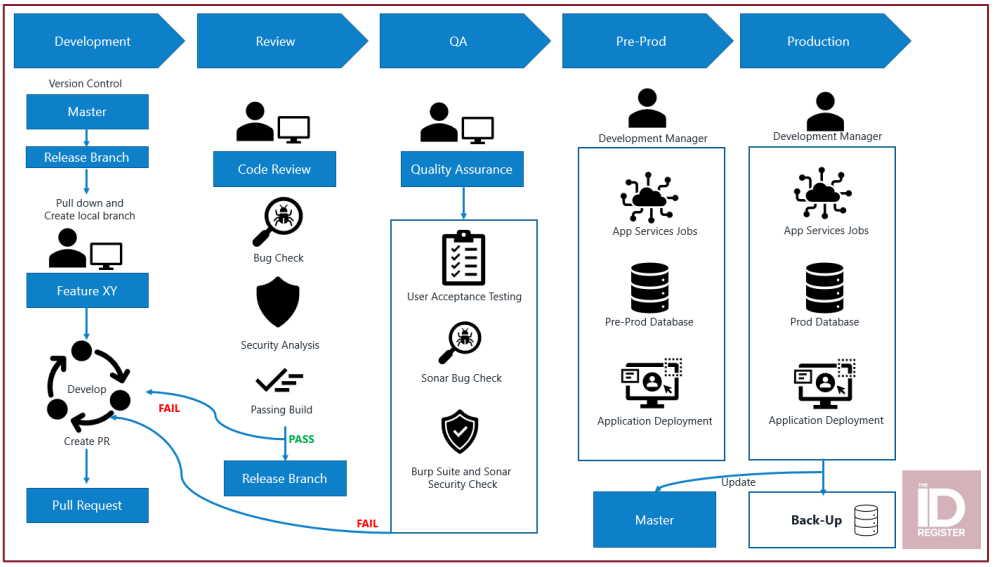
THE APPLICATION

APPLICATION OVERVIEW



DEVELOPMENT

The system is deployed to Microsoft Azure with the website and API hosted within App Services. Build automation is implemented via Azure DevOps, with deploy pipelines for code.



SECURITY CONTROLS

ACCESS MANAGEMENT AND MULTI-FACTOR AUTHENTICATION

Role Based Access Control (RBAC) is used via Active Directory security groups to apply appropriate permissions to the Azure subscription and environment specific resource groups. DevOps pipelines/scripts uses a dedicated service principal for each environment to ensure deployments are protected against misconfiguration.

The ID Register also uses Azure Multi-Factor Authentication that helps safeguard access to data, applications, and Azure resources. It provides additional security by requiring a second form of authentication and delivers strong authentication via a range of authentication methods.

Furthermore, the application has set of permission to apply the Role Based Access Control (RBAC) along with its own Multi-Factor authentication mechanism.

APPLICATION SECURITY

Web application security is the process of protecting websites and online services against different security threats that exploit vulnerabilities in an application's code. The code is tested against the OWASP Top 10 Application Security Risks.

At the ID Register we ensure that the application is secured using the following means:

- Static testing, which analyzes code at fixed points during its development. This is useful for developers to check their code as they are writing it to ensure that security issues are being introduced during development.
- Dynamic testing, which analyzes running code. This is more useful, as it can simulate attacks on production systems and reveal more complex attack patterns that use a combination of systems.
- Code obfuscation**:** Allow developer to protect their code from being attacked.
- Encryption: All data at rest and in transit are encrypted.
- Authorisation: We ensure that the correct person is assigned the right permission on the platform.

The Security team identify threats, controls and undertake testing to ensure risks within

- The ID Register application and systems are managed to an acceptable level.
- Technical and information security risk advice to businesses, functions' projects, or initiatives.
- Defining and testing application system controls relating to information security.
- Input to system build standards and procedures.
- Installation and monitoring of application-level controls.
- Development of minimum baseline security standards.
- Conduct security testing i.e., application penetration test (which includes vulnerabilities covered by the OWASP framework) and code reviews.

All Azure services are protected from distributed denial of service (DDoS) attacks using Azure's infrastructure DDoS.

AZURE INFRASTRUCTURE

All connection to the infrastructure goes through the Azure Landing Zone. The Azure Landing Zone is a secure and governed platform that our MS Partner has designed and deployed to current best practices based on Microsoft's Cloud Adoption Framework. The Cloud Adoption Framework enables repeatable scalability for Azure deployments whilst ensuring baseline identification, security and governance controls are in place.

Azure Security Centre is enabled to monitor and manage security for virtual machines, virtual networks, storage accounts and PaaS services such as SQL databases and Azure App Service. This provides security functionality including features such as regulatory compliance, advanced threat protection and vulnerability assessment capabilities. Azure Security Center is a security management system that provides tools to track and remediate the security of Azure resources through one interface. Within security center is Azure Defender, an additional plan that provides regulatory compliance, continuous security assessment, advanced threat protection, security incident alerting and proactive
recommendations for Azure resources by type.

VPN gateway in each region has also been configured to allow developers secure access to virtual machines and SQL databases. Authentication is provided by Azure AD using the Windows 10 Azure VPN client.

The connection also goes through a web application firewall (WAF). A web application firewall (WAF) is an independent resource that contains WAF rules and configuration to protect against common application attacks such as SQL injection. WAF policies can be applied at the global, per-site or per-URI scopes for supporting Azure resources and managed rules are offered via the OWASP core rule sets, with custom rules also available to meet specific requirements.
Furthermore, all resources are configured to send all diagnostics data to Azure Log Analytics where insights, queries and alerts can be subsequently viewed and configured via Azure monitor. This includes virtual machine and app service logs.

Secure key management is essential to protect data in the cloud. Azure Key Vault is used to encrypt keys and small secrets like passwords that use keys stored in hardware security modules (HSMs). With Key Vault, Microsoft does not have access to see or extract the keys, meaning The ID Register have full control over the keys and secrets held within the vault.

ENCRYPTION

Azure Disk Encryption leverages the Bitlocker Windows feature to encrypt OS and data disks, with an additional option to encrypt the temporary disk. The solution integrates with Azure Key Vault for the control and management of keys and secrets and reporting is integrated into Azure Security Center.

WORKSTATION AND MOBILE DEVICES

The ID Register laptops have anti-virus software incorporated into default operating builds, set to automatically check files as part of its regular full-time “on access” scanning and obtain updates as they become available.

- Laptops have a single, pre-installed customised build which limits users’ administrative access.
- Laptops are protected against data leakage from device loss using BitLocker and Microsoft InTune.
- No removable media is allowed to the personals.
- Internet access and network connectivity from The ID Register laptops is routed through the network. VPN software ensures that laptop users cannot connect directly to the public internet.
- The ID Register provided mobile devices are managed through a Unified Endpoint Management solution (UEM) enforcing policies and controls to limit information exposure.
- Limited number of bring your own device (BYOD) solutions protected using an industry standard mobile data management solution, enforcing a secure container under The ID Register’s control on the devices in the question.
- Mobile data management capabilities provide encryption for data in motion or at rest and capabilities to securely wipe data from lost or stolen devices.

SERVER

System security is built into our server platforms. Hardening measures and controls are incorporated into server builds; these include but are not limited to;

- Unnecessary and redundant services, devices, processes, protocols, system and network utilities, programs and accounts are disabled/removed.
- Operations/services are run with the minimum privileges required; appropriate file system security is applied.
- Strong user account and password controls are implemented for all users enforcing length, complexity, history, and lockouts. Automated password control with logging and auditing applied to privileged accounts.
- Additional monitoring capabilities are in place at the database level to protect sensitive data.
- Configuration settings are defined based on the ‘least privilege’ principle.
- Monitoring and reporting of any non-compliance.
- Audit trail management.

PATCH MANAGEMENT

SQL server virtual machine patching is already in place for the production SQL server with a schedule set at 2am every Sunday and a maintenance window of 60 minutes. The Security and Infrastructure Manager provide an update on the patch management to the senior management members.

MONITORING

Application insights has been enabled for the app services allowing the monitoring of key application performance indicators such as availability, failures, and performance.

All alerts are sent to the Security and Infrastructure Manager who will take the appropriate actions if required.

ENDPOINT PROTECTION

For Azure servers Microsoft provides an antimalware solution which is enabled via a virtual machine extension and will report back to Azure Security Center to show an overview of scans and detections. This integration also extends to Microsoft Defender for Endpoint, an enterprise security platform offering advanced analytics and threat intelligence.

REMOTE WORKING

The ID Register supports remote working capabilities where appropriate for its staff. Additional controls and guidance for staff working remotely include but are not limited to:

- Training and education on information security which must be completed within the 30 days.
- Full disk encryption on laptops.
- Secure mobility clients on laptops enforcing VPN use.
- Provision of managed mobile devices or support of 'Bring Your Own Device' via specialist applications offering secure containerisation.

INCIDENT MANAGEMENT

The ID Register's Incident Management & Response processes:

- Co-ordinate Cybersecurity incidents to ensure that all required tasks are completed and that duplicative or contradictory efforts are avoided
- Ensure that Cybersecurity incidents are investigated in a timely manner
- Ensure that the risk associated with an incident is appropriately identified, measured, and controlled
- Ensure that required internal notifications and external reporting is completed
- Ensure all Cybersecurity incidents are centrally tracked for trend analysis and consolidated reporting to management

VENDOR SECURITY MANAGEMENT

The ID Register has a Third-Party Risk Management policy to identify and control risks (including information security risks) associated with vendor relationships and contracts. The ID Register requires third parties to meet at least the same level of security as per The ID Register policies and standards, covering legal and regulatory requirements that apply to The ID Register information or systems accessed in the provision of service to The ID Register.

Furthermore, third parties with access to The ID Register's network or information are subjected to information security due diligence reviews based on their potential risk to the organisation. Specific information security clauses are included into terms and conditions of contracts with third parties. These may include the right to undertake audits of third-party premises, physical and logical security controls. Third parties' employees with access to our systems are subject to annual access recertification.

NON-DISCLOSURE AND CONFIDENTIALITY AGREEMENT

The ID Register only discloses information to 3rd parties if the appropriate controls have been considered and implemented (as applicable) to manage the 3rd party's access to, use and storage of The ID Register information. These controls may include:

- Agreeing confidentiality and information security obligations with the 3rd party.
- Making appropriate assessments of the information itself, how and why it is to be disclosed; and
- The transfer of information is secured using appropriate technical or process controls as required by The ID Register to meet our legal responsibilities, customer obligations and regulatory requirements

TRAINING AND RISK AWARENESS

The ID Register Staff vetting is a key defence against Insider and other risks. Minimum requirements for vetting are set out at The ID Register. All The ID Register employees, including contractors, service provider workers and contingent workers are subject to vetting prior to starting in role.

Key vetting objectives are to;

- Confirm the candidate's identity, employment history and relevant qualifications with respect to the post for which they are applying.
- Test their integrity in accordance with The ID Register values.
- Confirm that there are no legal or regulatory barriers to the organisation employing them

The ID Register has an ongoing security awareness programme employing various channels to engage staff including, intranet content, posters, e-mails, new employee education and annual mandatory information security awareness training for all staff. Completion of annual mandatory training is monitored and failure to complete training results in formal management action.

BUSINESS RESILIENCE

From a service perspective the current production deployment of the application offers the following SLAs:

- 99.95 app service plan standard tier
- 99.9% Single SQL server virtual machine with premium disks
- 99.9% Service bus standard
- 99.99% Storage account with RA-GRS

Delivering reliability in Azure is a shared responsibility starting first with a resilient foundation built into the platform. From there, the recovery point objective (RPO) and recovery time objective (RTO) are defined and met using a range of Azure services that compliment a well architected application.

The ID Register uses two Availability Zones mainly: North Europe (Ireland) and West Europe (Netherlands).

Azure Availability Zones are unique physical locations within an Azure region which have independent power, network, and cooling. Each availability zone consists of one or more physical data center buildings. Using availability zones for application and infrastructure resources provides tolerance for data center failures due to the redundancy and logical isolation of resources.

Azure Site Recovery allows The ID Register to replicate server data from on-premises servers to an Azure Recovery Services Vault. The servers in the cloud are stored as offline data and so compute charges are not incurred. When a failover is required, a click of a button can bring up all servers, or this could be automated. Azure Site Recovery also supports recovering to another data centre, or even between Azure regions.

HERE TO HELP

Please reach out to us if we can help you further or if you have any remaining questions.