Quality Management System

Table of Contents

1. Background

Summary information about Own products and services

At Own, our mission is to empower customers to own and protect their data on any SaaS platform.

What does Own do?

Own is a leading SaaS data protection platform that provides secure, automated, daily backups and rapid data restore tools of SaaS data. This service is delivered in the traditional software as a service (SaaS) model and is built with strict quality standards. Own helps more than 4,000 businesses across all industries worldwide, covering data loss and corruption caused by human errors, malicious intent, integration errors, and rogue applications. Our quality management system focuses on ensuring that our processes and best practices are followed when developing, delivering, and supporting our SaaS solution.

What are the features of Own products?

We live in an always on, digital-first world where data is the lifeblood of business. From small startups to the largest enterprises, data is the essential strategic asset that drives critical processes, delivers insights into performance, guides customer experiences, fuels innovation, and informs about emerging trends.

Own helps organizations better protect and manage their data with our comprehensive backup and recovery, security, archiving, and sandbox seeding products.

Own Recover eliminates data downtime, ensuring data incidents never impact business resiliency. Whether data is lost or corrupted by accident or malicious intent — or it's inaccessible due to forces of nature or an outage — the data you need to return to business as usual is ready and waiting. Learn more about Own Recover.

Own Secure enables customers to strengthen their security posture by helping them to understand data exposure risks and proactively take action to protect and secure their data. With Secure, customers can easily assess their current security implementation compared to their expected (required) policies around data classification, access controls, platform encryption (encryption at rest), data retention and compliance audits.

Own Archiver is an easy-to-use, flexible and effective automated data archiving solution for Salesforce customers. It enables administrators to effortlessly define, automate and manage custom data retention policies that include specific data to be archived, how frequently data archiving activities occur, and how long archived data is retained. Learn more about Own Archiver.

Own Enhanced Sandbox Seeding is an intuitive and powerful sandbox seeding solution for organizations that develop on the Salesforce platform. It enables administrators and developers to effortlessly define, finetune and automate the replication of precise subsets of data schemes from production environments or other sandboxes, then quickly seed them to Developer, Developer Pro or Partial Sandboxes with identical metadata. Learn more about Own Enhanced Sandbox Seeding.

How Own helps Life Sciences organizations

Own supports many life sciences operations across the globe, with clients including Novartis, Twist Bioscience and Athena health. During the pandemic, the shift to a remote workforce vastly accelerated transformation initiatives. SaaS platforms such as Salesforce and Microsoft Dynamics 365 became the bedrock of communication with all stakeholders as the world went virtual.

Own offers the most comprehensive platform to protect the critical customer, partner and operational data that life sciences customers rely on — and store — within Salesforce and Microsoft Dynamics 365. Own can help organizations :

- Safeguard 100% of data and metadata with automated backups
- Go back in time to identify and restore the exact data you need
- Seed sandboxes with ideal data sets for development, testing and training
- Archive records to align with data lifecycle management policies
- Maintain compliance with record management policies and regulations like GDPR/CCPA
- Deliver world-class account management, customer service and technical support resources

Own's commitment to quality

Own products are designed, developed and maintained using industry-leading infrastructure, processes, and tools. Own product development follows a well-defined Secure System Development Lifecycle which considers and documents user requirements, system standards, testing criteria, and test results.

As a data protection platform, we take security very seriously and determined that we require an approach to software and product security beyond what a traditional QMS could offer.

To help accomplish this goal, we've mapped our existing QMS and cybersecurity framework against the standards and regulations that Life Sciences organizations typically face, particularly 21 CFR Part 11 ("GxP") and, EudraLex Volume 4, Annex 11 ("GmP"). We also engaged an independent third-party audit firm to validate our mapping process. While Own's core function is not as a "computerized system" within the context of a Life Sciences organization, there are critical aspects that we can help our Life Science customers with through our QMS, cybersecurity framework, and the shared responsibility model.

The expanded QMS ensures that Own is able to consistently provide products and services that meet our customers' and regulators requirements on information security. It also provides the baseline for a shared responsibility model that can be applied across frameworks, and expands the scope to include information security best practices that help ensure confidentiality, integrity and availability are maintained within the environment.

While the Own QMS can be applied across multiple regulations, frameworks, and standards, this specific view focuses on our Life Sciences customers. Within this industry, we find a majority of users require additional validation beyond our leading practice certifications and audit reports.Below is a listing of the frameworks, certifications, and audit reports Own maintains:

- A well-established information security program based on industry leading practices
- An annual SOC 2, Type II assessment covering all Trust Service Criteria (Security, Confidentiality, Privacy, Processing Integrity, and Availability).
- A certified ISMS and ISPMS program in accordance with ISO 27001/27701;
- FIPS 140-2 validated cryptographic mechanisms
- More information about the Own security controls can be accessed here: (https://www.owndata.com/resources/ebook/own-security-controls-overview)

How can Own's QMS support Life Science Organizations

The Own QMS focuses on describing the processes that support our core capabilities to help ensure our products are designed, developed, and delivered at the highest levels of quality and in a manner that ensures stability, reliability and security of the environment and our customer's data.

Because Own is not a Life Sciences company, we do not directly enable organizations to perform processes specifically related to scoped activities under 21 CFR Part 11 ("GxP") and, EudraLex Volume 4, Annex 11 ("GmP"). While Own provides a reliable solution to backup and recover your electronic records and signatures, we do not provide a mechanism for replacing paper records with a computerized system. This would more commonly be applicable for systems that directly facilitate electronic signatures, tracking tools for drug makers, medical device manufacturers, biotech companies and other FDA-regulation uses.

Own does not facilitate the design, implementation or ongoing maintenance of a regulatory program Life Science organizations would use to provide assurance over their GxP or GmP program. Our products are not designed as a platform for electronic signatures or records, nor do we facilitate the manufacturing of medical devices (such as blood glucose meters), or provide any detailed tracking or metrics for critical manufacturing processes such as pharmaceuticals, which require precise and accurate measurements throughout the process.

Because of this, the Own QMS addresses only the applicable requirements of the 21 CFR Part 11 (“GxP”) and EudraLex Volume 4, Annex 11 (“GmP”) requirements, and only tests against the relevant use cases, which does not include the performance validation activities commonly associated with these regulations. These relevant validations include select controls for IQ/OQ/PQ explained as follows: The Installation Qualification (IQ) validation is relevant in ensuring equipment that supports a regulated activity is installed correctly to ensure accurate and precise measurement or documentation. The Operating Qualification (OQ) validation is intended to ensure that, once installed correctly, the equipment used maintains precision and accuracy over time while operating. The Performance Qualification (PQ) validation is intended to ensure that the process maintains precision and accuracy over time.

While our products do not directly facilitate the regulated activities described above, we are committed to providing the highest level of support to the Life Sciences industry. We have mapped the controls within this Quality Management System to both 21 CFR Part 11 (“GxP”) and EudraLex Volume 4, Annex 11 (“GmP”). As noted above, because we are not facilitating regulated activities, there are specific subparts (“GxP”) or sections (“GmP”) that are not applicable to the Own products and must be facilitated within your system of record. To help eliminate audit effort and redundant requests, the relevant subparts and sections of the regulations are mapped to externally validated controls within our ISO 27001 certification and SOC 2, Type II report.

2. Shared Responsibility Model

A high-level overview of the shared responsibility model

As a cloud services provider, Own maintains a leading-class product built utilizing quality, security and compliance concepts. Our products are also classified as Software as a Service (SaaS), so we designed them such that you can configure how you use them according to your individual business needs and use cases. Given this flexibility, overall information security and compliance with regulatory standards can only be accomplished through a shared responsibility model.

As the users of our SaaS systems, you must understand what aspects we are able to accomplish through the proper configuration and use of our systems, and how to align these configuration and processes with your internal processes to maintain the appropriate level of security and compliance based on your organization’s requirements.

Own maintains all product upgrades, updates, improvements, and innovation. Own is also responsible for providing always-available application services that are hosted on a resilient infrastructure and maintaining data copies to withstand infrastructure failures or product outages.

Our customers are responsible for policies and rules governing data management, including access management, usage, development testing, security, compliance, data protection, backup, and data lifecycle management.

Definition of Own products in relation to shared responsibility model

Within the concept of a shared responsibility model, Own is responsible for the security configuration and management of the cloud Infrastructure as a Service (IaaS) to host and deliver our products and services. For example, for Amazon Elastic Compute Cloud (Amazon EC2), Own performs management activities such as updates and security patches, maintains AWS security configuration, and implements other leading practice tools required to protect the product and data. For other services such as Amazon Simple Storage Solution(S3), Own inherits the security configuration provided by the IaaS providers while maintaining the responsibility of implementing security and privacy controls in managing data, particularly data encryption and access controls.

Examples of this shared responsibility include:

- Patch Management – IaaS is responsible for patching and fixing vulnerabilities within the infrastructure, while Own is responsible for patching any unmanaged services such as non-containerized operating systems under its control and Own developed applications.
- Configuration Management – IaaS maintains the configuration of its infrastructure devices, while Own is responsible for configuring unmanaged services (operating systems, databases), and Own developed applications.

Own-specific controls which Own is solely responsible for implementing such as:

- Service and Communications Protection or Zone Security may require Own to route or zone data within specific security environments and perform the review of security groups for its VPCs.
- Awareness & Training – While Own independently validates that the IaaS trains its employees in accordance with our company's standards, we also conduct security and privacy training for our own internal users and administrators.

Customer obligations under the shared responsibility model

Although the cloud security providers (IaaS and the SaaS providers) are responsible for maintenance of the platform and products, there are customer-specific controls related to the access, configuration, and use of the products.such as

- Salesforce permissions and data access
- User access identity, application role-based access (RBAC) configuration and permissions
- Configuration of backup and archive services, and retention policies

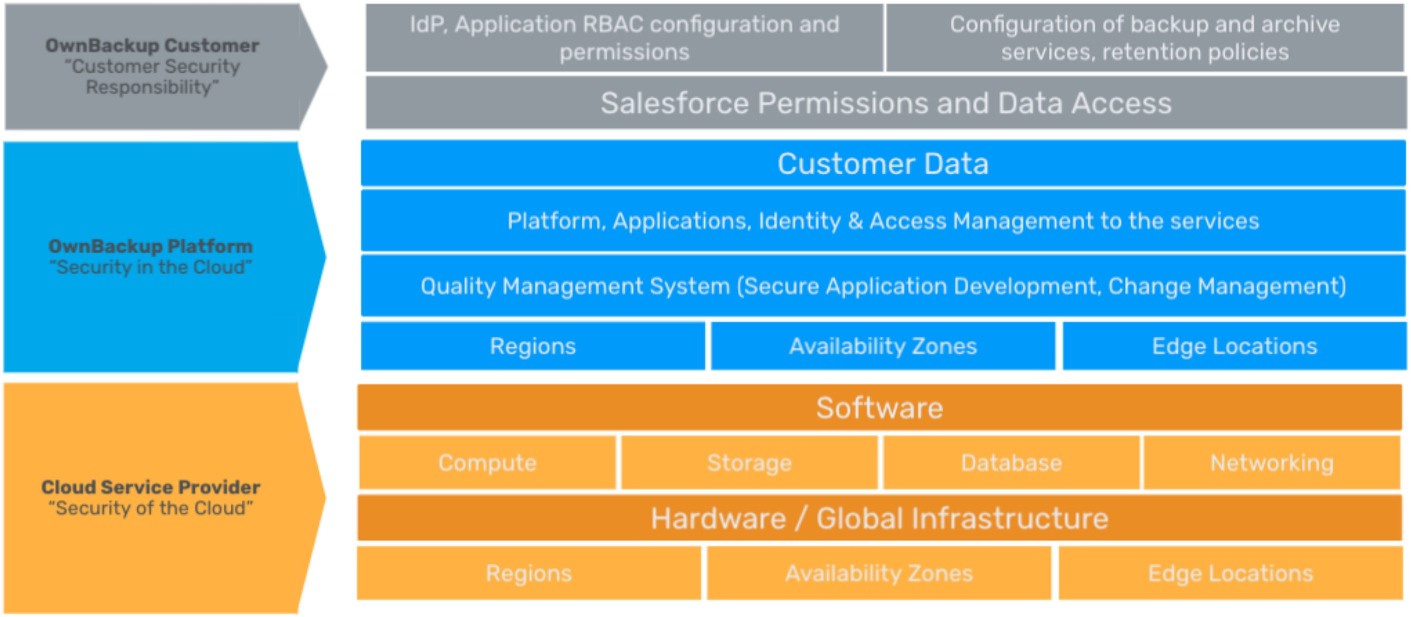
Putting it all together (Where does Own play a role?)

Own is a Software as a Service (SaaS) provider with products designed for multi-tenancy that are developed and delivered with the highest quality standards in mind to maintain security, stability and high availability for all user entities across industries utilizing the platform. Similar to other commercial IT products such as database engines, operating systems, and consumer mobile platforms, Own products are not inherently developed for use in specific “GxP” or “GmP” systems, rather, they are developed according to current quality and security standards for commercial IT product providers, including specific cybersecurity considerations.

Own Products are user-configurable, general-purpose in nature, and delivered to commercial IT quality and security standards such as ISO 27001 and SOC2, and others. This is similar to other general-purpose IT products and services such as database engines, operating systems, programming languages, consumer mobile platforms, etc.

Own provides the tools to help customers be compliant from a data archiving , backup, and recovery perspective. We support the record and log requirements by maintaining the integrity and availability of the records throughout the company's retention period needs. We also provide solutions to enable customers to support their compliance program and meet the following requirements:

a. Availability and business continuity plan;
b. Accurate and complete records;
c. Ability to retrieve records;
d. Backup restoration protocols;



OwnBackup Customer
"Customer Security Responsibility"

IdP, Application RBAC configuration and permissions

Configuration of backup and archive services, retention policies

Salesforce Permissions and Data Access

OwnBackup Platform
"Security in the Cloud"

Customer Data

Platform, Applications, Identity & Access Management to the services

Quality Management System (Secure Application Development, Change Management)

Regions | Availability Zones | Edge Locations

Cloud Service Provider
"Security of the Cloud"

Software

Compute | Storage | Database | Networking

Hardware / Global Infrastructure

Regions | Availability Zones | Edge Locations

The shared responsibility extends to the controls

The Own shared responsibility model also extends to IT controls. Just as the responsibility to operate the IT environment is shared between end users and Own, so is the management, operation and verification of IT controls shared.

Own provides a baseline of control that can be leveraged by our customers to reduce the burden of compliance and control operation. However, as each customer uses and configures Own differently, there are aspects that our customers will have to own and perform.

The Own control and compliance documentation (including this whitepaper and our shared responsibility model) can serve as a tool in helping you reduce your burden and develop the appropriate controls that, in collaboration with Own's environment, can help you maintain compliance

For Life Sciences entities looking to comply with GxP and GmP, Own has mapped our control environment to specific subparts and sections of the regulation. We have included the aspects inherited from AWS and Azure and the considerations our users should make when building a compliant environment within the Life Sciences industry utilizing Own Products.

3. Details of the Own Quality Management System

Own implements an internally developed Quality Management System that was developed using industry-leading cybersecurity frameworks, particularly SOC2 and ISO 27001, and were mapped against the applicable control requirements of GxP and GMP. Although Own does not inherently serve as a “GxP” or “GmP” system, nor does it perform any specific “GxP” or “GmP” scoped activity, we mapped our QMS against applicable GxP and GmP controls to support the compliance program of our Life Sciences clients.

Own’s Information Security team is responsible for implementing the information security-related policies within the organization. Own has aligned its information security function with the company’s core business, particularly when it comes to product security and enterprise security. There is strong leadership and management involvement in information security and privacy to provide visible support for security and privacy initiatives.

The Own QMS defines a group of information security principles and controls that are integral to the design of our products and services, taking into account the legal and regulatory requirements, contractual obligations, and industry best practices related to the confidentiality, integrity, and availability of the information within the Own systems.

(Product) Secure software development

Own designs all new products and services- and makes any significant changes to current products and services- through an intensive review and evaluation as part of the product development lifecycle. This t includes project management with participation from the product design, development, and product security teams.

The software development component of the QMS covers the following requirements to enforce the controls that form part of the Secure Software Development Lifecycle (SDLC):

(a) software development methodology;

(b) programming standards;

(c) source code reviews;

(d) development testing;

(e) software specifications: user requirements and functional requirements;

(f) software design specifications;

(g) development of user manuals; and

(h) vulnerability / penetration testing.

Own develops custom code for its products and services and uses open source software that includes binary or machine-executable code from third-parties that are reviewed and approved by the development team prior to implementation. No third-party software components or code can be used unless the prior open source review is completed. Own technology is built on top of IaaS providers such as Amazon Web Services and Microsoft Azure, and uses software components such as APIs and microservices to support the operation and configuration of the underlying infrastructure for use by Own.

Own implements controls to ensure that the code are developed and managed consistently through the software development process, such as:

- The implementation of a code management system to assemble a code package;
- Internal source code repository;
- The hosting system in which the Own code is staged;
- The tools used to automate the testing, approval, deployment, and continuous monitoring of codes;
- Change management tools to capture the details of change information including the detection and monitoring of unauthorized changes to code or configuration settings in the production environment;
- The mechanism for the reporting and escalation of non-compliance with the secure software development processes;

Code management

The code management within the SDLC follows these steps regardless of any newly developed codes or a change to an existing code in the repository:

1. A developer creates the code in the authorized development environment that was approved by the engineering team. This is where the initial build and functional testing of the codes are performed.
2. A developer stores the code (check -in) to the authorized internal source code repository.
3. The code is reviewed by an additional person who approves it. Approvals are tracked, logged and retained to maintain the integrity of code updates.
4. The approved code is converted into the appropriate deployable code package using the tool that was approved by the engineering and security team.
5. After the codes are built, the integration test is performed to evaluate code performance against specific functional requirements. Once the code passes the integration testing, it gets pushed to the production environment.

6. The code package is tested using automated integration and verification testing in the pre-production environment, and if successful is moved to production.

Every step in the code management process is recorded in the change management solution. Any software components such as open source codes are still subject to the code review outlined above, and are tracked for dependencies.

Testing

Own performs different stages of controlled code testing and continuous approval to ensure safe code deployment to the production environment. These quality tests (e.g., unit test, integration test, functional test, acceptance test, performance test) in non-production environments ensure code is performing as designed. If the code fails any of the tests, or is found to have deviated from the secure coding standards, the release of the code to production is stopped, and the team is notified of the need to review and remediate the cause of the failure or non-compliance.

The development team maintains separate development and test environments that are configured similar to the production environment. The objective is to simulate how the code will perform in the production environment without the risk of unauthorized access or change to the production environment and live data. The development team also uses automation to perform these tests and to move the code across environments to maintain consistency and efficiency.

Change and configuration management

The QMS implements Change and Configuration Management (CCM), which is a set of processes and procedures to manage the effect of change-related incidents, including preparation, review and approval.. This includes documents, software, release management, bug fixes, patches and upgrades. The CCM is designed to maintain the integrity of the products and services and to avoid inadvertent service disruption or unauthorized code in the production environment.

CCM processes are observed for every type of the change (e.g. routine, emergency) and include the authorization, logging, testing and documentation of changes. Any change to the code used in Own products and services is thoroughly reviewed, tested, approved and communicated. T

CCM processes include:

1. **Preparation:** This includes the scheduling and identifying of resources such as APIs, microservices or open source codes, preparation of notification lists, and component dependencies with the objective of minimizing the impact of changes to the existing production code base.
2. **Change request:** This includes the documentation of change requests, including the use of a change management tool to capture information related to potential impact, recording of code review results,

planned activities for promotion and production, and rollback procedures.

3. **Change review:** This covers the inspection of proposed changes by peers and the change control body of the technical aspect of the change. This provides appropriate oversight and ensures the changes satisfy the intended business requirement while minimizing security risks. The change control body usually includes key organization personnel and Own subject-matter experts who own key functions or processes that will be impacted by the proposed changes.
4. **Testing:** All proposed changes are tested to validate that the proposed changes perform as expected and do not adversely impact the performance of the business function.
5. **Communication and monitoring:** This includes the notification of stakeholders before and after the implemented change, communication and management of timelines, monitoring of the results of the change, creation of the metrics if applicable, the close-out of the change, or a rollback in case of failure.

Own implements and maintains baseline configuration of its systems, following the guidance of leading industry frameworks as well as recommendations from infrastructure service providers. Changes to the systems that fall under the QMS are supported by change tickets that contain information about impact analysis, security components, timelines, test results, implementation steps, rollback procedures, and approvals.

Testing is a critical component of CCM. To perform testing, the changes are pushed to the non-production environments where the performance and behavior of the changes are observed. When the testing criteria are met, the changes are approved or rejected. The decisions for change requests are recorded in the change management system, including a schedule of when changes will be implemented.

Change tickets contain the rollback procedure that will be implemented to restore the system to its state prior to the change in the event that the desired system performance is not achieved in the production environment. CCM also includes communication steps to alert and notify personnel of changes relevant to their respective processes or when a change was made that does not comply with CCM processes.

Exceptions to the CCM are not allowed except in cases involving emergency changes to the production that present high risk if not addressed immediately. While emergency changes are expedient in nature, all emergency changes are logged and still require appropriate approvals. The exceptions are reviewed to identify the root cause and take actions to remediate any issue — or perform a rollback if necessary. A periodic review of the emergency changes is also performed to determine whether the emergency change is being abused to bypass CCM processes.

Access controls

Own implements appropriate physical and logical access restrictions to help enforce controls soonly authorized individuals may access the Own computerized systems. These restrictions maintain and validate the integrity of the data contained therein — including an audit trail that tracks system access usage and edits — and imposes access controls on data entry and any edits. The access controls also implement security measures in relation to system administration, including segregation of duties, logical security, planned maintenance, unplanned maintenance, user management, incident/problem management, backup and restore, and help desk.

Information and communication protection

Own implements information security and privacy controls to protect the confidentiality, integrity, availability and quality of the data that's processed under the QMS from manipulation or loss, whether intentional or unintentional. These controls are enforced using the combination of reasonable and appropriate systems, processes and controls to minimize human errors that can lead to data integrity issues as well as mechanisms to evaluate the effectiveness of these controls.

Documented information

Own maintains formal, documented policies and procedures of its operations and information security as part of the QMS. The documentation provides guidance on the implementation of the information security and privacy controls including change control and management within Own products and services. The policies and processes cover the purpose, scope, roles and responsibilities to maintain the confidentiality, integrity and availability of customer data maintained and operated by Own. Own maintains information and records as required by the contractual and regulatory obligations and will protect these information and records under the QMS.

Compliance management

To maintain the continuous effectiveness of the QMS, the Own Information Security Team monitors the implementation and maintenance of the QMS through its internal and external audit programs. The team performs regular verification activities as part of risk assessments to monitor compliance and effectiveness of the QMS.

Own maintains a documented audit schedule of different information security and privacy audits, such as SOC2 and ISO 27001/27701. Additional assessments are also performed to support:

- Internal assessments coming from the Information Security, product security, and relevant administrative and corporate teams
- External auditors and certifying agents for other certifications such as FedRAMP, France HDS, and Australia's IRAP Cloud Services and Authorization
- Own customers, including current customers (audits) and potential customers (sales)

Own's QMS is based on SOC2 Trust Services Criteria and ISO 27001 ISMS with mapping against the GxP and GmP control requirements. To keep up with evolving criteria, periodic revalidation and quality controls checks measure the effectiveness of the QMS and are performed along with the SOC2 Audit based on an

Agreed Upon Procedure (AUP) with an independent external auditor.

Own takes appropriate corrective actions from critical findings identified as a result of the compliance assessments and audits and closes these corrective actions in a timely manner as defined in the SLA under the Risk Assessment Policy.

The remediation steps of these nonconformities within the scope of the QMS include:

1. Identification of non-conformities within its QMS
2. Analyzing potential causes of non-conformities
3. Reviewing and developing appropriate remediation action to prevent recurrence of nonconformities
4. Implementing planned corrective action
5. Monitoring and reporting results of corrective action taken
6. Evaluation of the effectiveness of corrective action
7. Identification of applicable preventative action or control
8. Implementation of preventative action or control
9. Monitoring and reporting of preventative action results
10. Review of the preventative action for continuous improvement

Backup

Systems falling under the QMS are periodically backed up with suitable backup system(s) as defined by the product owner to support disaster recovery and business continuity and meet customer, data owner, compliance, or legal requirements. The integrity and accuracy of backup and the ability to restore the information are tested and documented during validation and monitored periodically. Own also implements adequate mechanisms to protect backups to ensure they are recoverable throughout the retention period.

Own encrypts all backup storage containing confidential customer information using AES-265 or other encryption methods approved by the office of the CISO.

Own uses cloud storage provided by cloud service providers (CSPs). Own is responsible for properly configuring and using these backup services and taking appropriate steps to maintain the security of backups containing confidential customer information.

The backups of confidential customer information are maintained across multiple isolated locations or availability zones provided by the CSP and managed by Own. Distributing applications across multiple availability zones provides resiliency in the face of most failure modes, including natural disasters or system failures. Each availability zone is designed to operate independently with high reliability. Backups are monitored for successful replication across multiple availability zones using the functionality and tools provided by CSPs.

Own is responsible for implementation of appropriate security configurations for CSP environments to protect data integrity as well as ensure data and resources are only retrieved with appropriate permission. Access to backups as well as the encryption keys used in the backups are restricted to a limited number of authorized personnel and are subject to access recertification requirements.

To ensure that backups are operating effectively, Own performs testing exercises to determine whether functions are operating as intended. During and after testing, Own documents the test results, including personnel responsibility, process performance, corrective actions, and lessons learned for continuous improvement.

Own will dispose of backups by means of secure overwrite, process recommendations from CSPs, or encryption key destruction.

Business continuity and disaster recovery

Own has a business continuity policy and plan in place that is clearly defined, management-approved, and periodically tested. The business continuity plan is documented and outlines the strategy for the continued operations of the business, products, services and systems covered by the QMS. The business continuity policy is included as part of the Information Management System (ISMS) that all Own personnel must comply with.

Own conducts risk assessments and a business impact analysis at least annually to identify critical systems and information assets and assess potential loss scenarios resulting from disruption or security incidents. The impact of interruption or failure of a critical third-party provider is also included in the risk assessment. These analyses help Own identify and evaluate the risk level of tolerance that can be used to establish metrics for the recovery of business operations and prioritize the timeframe for recovery based on business impact. The assessment result is also used as a basis for investments in prevention, mitigation and recovery strategies.

The results of the risk assessments and business impact analysis help establish the appropriate Recovery Point Objectives and Recovery Time Objectives of the information systems and processes covered by the QMS. This ensures the timely recovery of organizational operations. As preventative and mitigating controls, Own maintains multiple redundancy zones offered by the CSP.

Training and preparedness

As a part of the organization’s business continuity plan, the organization requires all relevant personnel participate in a tabletop exercise to test the design and operational effectiveness of the plan. At the conclusion of the test(s), the organization will complete a "Lessons Learned" exercise, and if inefficiencies or errors are identified, the plan is updated and/or additional training is provided as appropriate.

The business continuity plan is regularly reviewed and updated to maintain the effectiveness in meeting the reasonable and expected challenges, including disasters and interruptions that can have a negative impact on products and services provided to customers and other information systems covered by the QMS. Relevant personnel from impacted business areas participate in the review and testing (or tabletop exercises) to simulate different scenarios and gauge the company's responsiveness in implementing the business continuity plans. Lessons learned during and after the testing, including corrective actions, are recorded for the purpose of continuous improvement.

Personnel security

Own implements formal, documented policies that address the purpose, scope, roles, responsibilities, and management commitment in ensuring that personnel have the adequate experience, training and qualifications to maintain the confidentiality, integrity and availability of company's systems and information while performing their job functions.

Own performs background checks on all candidates in accordance with relevant laws and regulations of the jurisdiction where the candidate is a subject, taking into account all the relevant privacy and protection of personally identifiable information. Background checks include character references, confirmation of academic and professional qualifications, criminal records, and employment authorization documents.

Individuals hired for information security-related roles who are required to perform privileged-user activities are subject to detailed screening to make sure candidates have the necessary competence to perform the security role and can be trusted, given the criticality of the activities to be performance for the organization.

Own job candidates are informed of their information security roles and responsibilities during the pre-employment process. These security obligations are codified in the Acceptable Use Policy, Code of Conduct, and Employee Handbook that job candidates must review, agree and acknowledge as important terms and conditions their employment with Own. These documents outline the information security expectations in order to protect and maintain the confidentiality, integrity and availability of information systems and data assets. These responsibilities continue for a defined period after the end of the employment as allowed by the relevant laws.

Own requires all employees and contractors perform the information security obligations as defined with the established company policies and procedures. Information security personnel and those who perform privileged-user functions are required to continue to have the appropriate skills and qualifications through continuous learning. Employees and contractors are also provided with mechanisms to anonymously report any suspected violations of information security policies and procedures.

Training and awareness

Developers and personnel involved in the development or maintenance of Own products and services are required to receive appropriate training to maintain the confidentiality, integrity and availability of data in Own systems. Own conducts the training and awareness based on the following principles:

1. Training includes the personnel's responsibility in implementing the controls covered by the QMS as well as the privacy and information security obligations.

2. The record of training is kept and maintained to monitor compliance.

3. Training materials are regularly updated to cover the every changing privacy and information landscape and threat vectors.

Own provides specialized training for developers and personnel directly involved in the development, maintenance and support of Own products and services based on the roles and responsibilities.

Training includes::

- Candidate background screening
- Workplace conduct standards
- Clean desk policy and procedures
- Phishing, social engineering and malware
- Data classification, handling and protection
- Compliance responsibilities
- How to report information security and/or privacy incidents, concerns and other complaints to appropriate personnel
- How to recognize insider threats in the form of suspicious communications and behavior
- Announcements and other communications to reinforce training objectives

Records of training and relevant certifications are maintained to verify individuals have appropriate training.

Third-party management

Own maintains a third-party risk management program to manage vendor relationships and monitor the performance of third-party providers. Own creates and maintains written agreement with third parties based on the nature of the product or services provided and implements appropriate guardrails to protect Own using a risk-based approach in qualifying, monitoring and enforcing the contractual obligations.

Own recognizes the industry-accepted assurances and industry certifications on the implementation of information security and privacy controls by its vendors, such as the AICPA Trust Service Criteria SOC2 and ISO 27001 Information Security Management. Without these assurances and certifications, Own performs an in-depth assessment of the security controls of the third-party providers that includes at least the following:

1. Information security governance
2. Software development
3. Change and release management
4. Configuration management
5. Vulnerability management
6. Third-Party Management;
7. Physical and environment security
8. Training and awareness

Final thoughts

If you are a Life Sciences company, you have specific GxP or GmP obligations, including accountability to regulators of how you use Own services for backup, recovery, archiving and testing of your data. You can use the information we provided here regarding our Quality Management System within the context of your processes and business operations as a component of your GxP or GmP regulated systems.

For more information about our products and services, including how we implement Own's QMS, please connect with us for a quick demo of our products.

4. Appendix: Product Features

Own Recover

Protect data and metadata with comprehensive, automated backups and rapid, stress-free recovery.

Automated daily backups: Configure backups for any number of production orgs or sandboxes, regardless of their size or complexity. Capture complete copies of data and metadata including standard and custom objects, chatter feeds, knowledge articles, person accounts, attachments, files and more.

Backup on demand: Instantly back up an entire org or specific objects. Capture data immediately before and after projects like deployments or mass record updates, then compare changes to identify accidental deletions or corruptions that may have occurred.

High-frequency backups: Reduce your RPO. Options include targeted backups of highly transactional, frequently changing objects, as well full org backups that run on a schedule throughout the day.

Manage backups: Drill into the details of any org for a complete view of all of your backup activities. Access the latest backup, monitor backup history, and manage alerts and notifications.

Configure Smart Alerts: Configure thresholds to identify statistical outliers from normal business activities. Customize alerts to uncover significant changes to specific objects and the number of records added, removed or modified.

Receive instant notifications: Be the first to know about data incidents. Monitor data in production orgs and sandboxes and receive alerts when anomalies are detected in backups, then take immediate action.

Data compare: Compare two backups to identify changes to records and fields. Select any two snapshots from your history to locate data that was added, deleted or changed between the backups. Download and review the affected data to restore it to its former state in minutes.

Metadata compare: Isolate precise metadata changes between two backups. Choose any two snapshots of the same service or different orgs to generate side-by-side, before-and-after comparison.

Compare the difference: Visualize abnormal data behavior and when it occurred. Graphs illustrate how your data and metadata changed over any period in your backup history. Diagnose problems in seconds by identifying the precise number of additions, deletions and changes that took place during select time periods.

Isolate data incidents: Understand the scope of changes, identify what data was impacted, and pinpoint precisely when issues occurred. Drill down into specific objects to isolate unwanted modifications, deletions and additions from intentional updates performed as part of normal business activity.

Restore with precision: Recover the exact data you need from any backup in your history without affecting valid data added since the backup occurred. Data relationships remain intact regardless how many levels deep they go. In no time, your org will look like the problem never happened.

Easily find records: Quickly locate records in your backups to recover deleted or corrupted data and simplify compliance, audit and legal requests. Streamline Data Subject Requests such as Right To Be Forgotten to ensure backups are compliant with GDPR, CCPA, HIPAA, SEC17a-4 and others.

Manage data policies: Customize backup timing, frequency and details for all services across your enterprise. By default, Own Recover includes 99 years of retention but offers you the flexibility to tailor daily, weekly, monthly and yearly backup retention by org. You can also manage API consumption by backup and exclude data you don’t need to preserve.

Simplify regulatory compliance: Maintain compliance with internal data retention policies, industry regulations, and government mandates. Plus, streamline Data Subject Requests such as Right To Be Forgotten with granular anonymization to ensure backups are compliant with GDPR, CCPA, HIPAA, SEC 17a-4 and others.

Export data: Export backup data with or without attachments to a CSV file, SQL file, or a MySQL Endpoint. Options include the ability to export manually or automate export via APIs.

Multi-org manager: Access your backups for any number of production orgs or sandboxes from a single convenient console. Control permissions to manage and monitor backups for business units across the enterprise, and instantly add backup protection to additional services with just a few clicks.

Learn more about Own Recover for Salesforce and Microsoft Dynamics 365.

Own Secure

Fortify data security: Strengthen security posture by understanding data exposure risks and proactively taking action to protect and secure your data — all within the Salesforce platform.

Identify security risks with confidence: Easily assess your current Salesforce security implementation compared to your expected (required) policies around data classification, access controls, Platform Encryption (encryption at rest), data retention and compliance audits.

Classify sensitive information with ease: Isolate exactly where sensitive information exists in Salesforce and easily apply classification categories without leaving Salesforce.

Meticulously control access rights: Stop Salesforce configuration creep with granular “Who Sees What” lenses and trace individual, group or guest access rights down to the record level.

Blueprint to remediate: Know with certainty the path forward to proactively remediate security vulnerabilities and encryption blindspots with detailed action plans and real time alerts.

Prove compliance with industry regulations: Deliver real time evidence-based reports and audits to satisfy internal policies and external regulations in highly regulated industries.

Accelerate Salesforce Shield implementation: Implement and report on Shield encryption while providing evidence-based compliance reports.

Analyze security posture across multiple Salesforce orgs: Identify exposure trends over time with six critical risk lenses across multiple Salesforce orgs to fully assess enterprise security posture.

Own Sandbox Seeding

Propagate data to sandboxes for faster innovation and ideal training environments.

Seed from production or sandboxes: Seed perfectly sized, relevant data sets to Developer, Developer Pro or Partial Copy sandboxes from production orgs or other sandboxes.

Seed with precision: Create the ideal development and testing environment with subsets of data from production orgs or other sandboxes.

Seed only what you need: Control what data is seeded for initial and subsequent projects with options to add all records, delete existing records and replace with new, or only update incremental changes since previous seed. You can instantly view a sample of the data that will be seeded to verify filters are creating the desired data set.

Reuse seed templates: Configure and recycle templates and built-in filters to isolate perfect data sets to repeatedly seed to any sandbox with an identical data structure. That way, rather than having to start from scratch each time you want to seed, you can start with only the specific data you need and then add more data as you need it.

Anonymize sensitive data: Because sandbox data is a subset of production data, it's likely to contain confidential information that could be accessed by many people during development, testing and training. With Enhanced Sandbox Seeding, you can apply custom templates to mask sensitive information before it is seeded to its destination.

Continuously update data: Update template filters in seconds to add or remove data based on new requirements, then reseed to update the destination's records.

Manage seed size: Real-time counters keep track of the number of records included for each object type selected, and filters provide options to further refine the ideal data set and size. At any point, a single click produces a report to show a sample of records defined by the custom parameters.

Learn more about Own Enhanced Sandbox Seeding.

Own Archiver

Preserve data with customizable retention policies and simplified compliance.

Automatically archive: Securely store immutable replicas of specified Salesforce records attachments, and safeguard data needed for compliance regulations and audits.

Customize policies: Configure, test and manage custom archiving policies that define what data to store, how often, retention timeframe, who can restore and more.

Improve systems performance: Reduce data volume to speed backups and overcome Salesforce performance issues for search, reporting, calculations and more.

Improve compliance: Meet industry and government regulations and internal policies that require secure, immutable archives and/or retention limits.

Programmatically delete: Schedule automatic removal of obsolete data and data that must be purged from archives per industry/government regulations and internal policies.

Manage archiving activities: Dashboards provide a single source of truth to review, edit and manage all archiving activities and permissions used to govern data.

Monitor storage limits: Monitor Salesforce data usage against prescribed limits and archive data to stay within thresholds.

Restore with ease: Restore records one-at-time or in bulk, designate users to view archived data and files directly within Salesforce, and set privileges to allow specific users to recover records for archives.

Learn more about Own Archiver.