AUREX SYSTEM DESCRIPTION AND SYSTEM BOUNDARY

Aurex Controlled Document - SOC 2 Evidence for the Product Features and System Boundary Control

THIS DOCUMENT IS CONFIDENTIAL AND INTENDED SOLELY FOR AUTHORIZED EMPLOYEES, CUSTOMERS, REVIEWERS AND AUDITORS.

Document ID	SDSB-AUREX-BEINEX-2026-001
Version	1.0
Effective / Last Reviewed Date	14-10-2026
Document Owner	Security Lead, Beinex
Author (Current Version)	Sachin Ullattil, Security Lead, Beinex
Reviewer	Divya Eipe, Risk Advisory & Compliance Lead, Aurex
Document Approver	Indumon Das, Managing Director, Aurex
Approval Date	See Section 16 - Document Approval & Sign Off.
Sign off Evidence	See Section 16 - Document Approval & Sign Off.
Classification	Confidential: Shared with customers and auditors on request. Do not share outside the organization without approval.
Applicable To	The Aurex GRC platform (web, application and database tiers) delivered under the Client On-Premise, Client Cloud Tenant and Aurex-Managed SaaS hosting models, and the processes performed by Beinex as subservice organization (inclusive method) under the Inter-Organization Service Agreement (IOSA-AUREX-BEINEX-2025-001).
Related Evidence	System Description - Aurex GRC Platform (SOC 2 Type 1); IOSA-AUREX-BEINEX-2025-001 v5.0; Policy Adoption Memo PAM-AUREX-BEINEX-2025-001 v3.0; Aurex Product Brochure; Aurex Internal Environments; Defined Data Input Types (DDIT-AUREX-BEINEX-2026-001); Supplier Security Policy (SSP-AUREX-BEINEX-2025-001); Backup and Restoration Procedure (BRP-AUREX-BEINEX-2025-001).

Note on scope: *This document (v1.0) defines the system boundary consistently with the Aurex GRC Platform System Description prepared for the SOC 2 Type 1 examination. Aurex Technologies Limited is the sole service organization; Beinex is presented as a subservice organization under the inclusive method. The hosting environment is described in provider-neutral terms because Aurex is delivered on-premise, in customer cloud tenants and as Aurex-managed SaaS on pre-approved cloud providers.*

Table of Contents

1. Purpose and Scope

2. Organization Overview and Entities in Scope

- 2.1 Aurex Technologies Limited
- 2.2 Beinex - Subservice Organization
- 2.3 Entities In and Out of Scope

3. Public Availability of Product Features

- 3.1 Product Website Evidence
- 3.2 What Is Published and What Is Not

4. Service Overview, Product Features and Service Commitments

- 4.1 Product Modules
- 4.2 Principal Service Commitments

5. Hosting Models and Responsibilities

- 5.1 Hosting Models
- 5.2 Infrastructure Ownership and Responsibility Matrix

6. In-Scope System Components

- 6.1 Infrastructure (Aurex-Managed SaaS)
- 6.2 Software
- 6.3 Environments
- 6.4 People and Governance
- 6.5 Processes, Policies and Procedures
- 6.6 Data

7. System Boundary Diagram

8. Interfaces and Integrations

- 8.1 Customer Source Systems

9. Data Flows

10. Subservice Organization and Third-Party Dependencies

11. Exclusions

12. Complementary User Entity Controls

13. Auditor Response Log

14. Document Review & Maintenance

15. Revision History

16. Document Approval & Sign Off

Annexure A - Product Website Screenshots

1. Purpose and Scope

1.1. This document defines the system boundary of the Aurex GRC platform for the SOC 2 Type 1 examination: the entities, hosting models, components, interfaces, data flows and third-party dependencies that are in scope, and what is excluded. It is consistent with the Aurex GRC Platform System Description.

1.2. The system boundary comprises the Aurex GRC application (web, application and database tiers) across the Staging and Production environments of each customer, and the processes, personnel and policies performed by Beinex Consulting Pvt Ltd and Beinex Solutions LLC on Aurex's behalf. Where a customer hosts the platform (Client On-Premise or Client Cloud Tenant), the customer-managed infrastructure is outside the boundary and addressed through Complementary User Entity Controls (Section 12). For the Aurex-Managed SaaS model, the cloud infrastructure is inside the boundary because it is managed by Beinex under contract to Aurex.

1.3. This document also responds to two comments from the external auditor (Crowe) on the control "product features and system boundaries are defined, maintained and accessible via the product website over the Internet":

- Show that product features and system boundary information are accessible over the Internet (Section 3).
- Document the system boundary, including third-party dependencies, data flows and exclusions (Sections 5 to 12).

2. Organization Overview and Entities in Scope

2.1 Aurex Technologies Limited

2.1.1. Aurex Technologies Limited ("Aurex"), headquartered in San Francisco, California, is the service organization and sole owner of the Aurex GRC platform. Aurex holds the platform's intellectual property, retains final governance authority over security, risk and operational decisions, and is the sole named service organization for the SOC 2 Type 1 examination.

2.1.2. Aurex's two regional affiliates, Aurex AI FZ-LLC (Ras Al Khaimah, UAE) and Aurex.AI Private Limited (Kottayam, Kerala, India), exist solely for regional commercial contracting and local regulatory compliance. They have no employees or IT infrastructure and are excluded from the boundary.

2.2 Beinex - Subservice Organization

2.2.1. Beinex delivers the platform for Aurex under the Inter-Organization Service Agreement (IOSA-AUREX-BEINEX-2025-001, v5.0, effective 17 June 2026), in two capacities: as a subservice organization performing technical and operational delivery, and as an authorized commercial agent executing regional customer subscription agreements on Aurex's behalf. Beinex personnel operate under Beinex corporate policies formally adopted for the Aurex GRC environment through the Policy Adoption Memo (PAM-AUREX-BEINEX-2025-001, v3.0).

2.2.2. Because Beinex's controls are fully integrated into Aurex's system of internal control, Beinex is presented under the inclusive method: its control activities are part of the boundary and are tested within the examination.

2.3 Entities In and Out of Scope

Entity	Location	Role	Boundary
Aurex Technologies Limited	San Francisco, USA	Service organization; platform owner; final governance and release authority	In scope

Entity	Location	Role	Boundary
Beinex Consulting Pvt Ltd	Kochi, Kerala, India	Principal operational entity: engineering, QA, DevOps, security operations, change, incident and release management, implementation, BC/DR, HR governance for assigned personnel	In scope (inclusive)
Beinex Solutions LLC	Dubai, UAE	Commercial delivery: account management, sales and marketing, customer support, commercial contracting as Aurex's authorized agent	In scope (inclusive)
Aurex AI FZ-LLC; Aurex.AI Private Limited	Ras Al Khaimah, UAE; Kottayam, India	Non-operational regional affiliates (commercial contracting, local compliance)	Excluded
Beinex Consulting DWC LLC; Beinex Information Technology Consulting LLC (Abu Dhabi); Beinex Advanced Information Technology LLC (Riyadh); Beinex Consulting WLL (Doha); Beinex Consulting Limited (Nairobi and London)	UAE, KSA, Qatar, Kenya, UK	Local regulatory and commercial presence only; no delivery functions	Excluded

3. Public Availability of Product Features

3.1 Product Website Evidence

3.1.1. Aurex product features are published on the public product website, www.aurex.ai, which anyone can reach over the Internet without logging in. Six full-screen screenshots taken on 13 October 2026 between 10:23 and 10:36 IST show the site live. Each shows the browser address bar and the Windows date and time, and they are attached as Annexure A.

Ref	Page	URL	What it shows	Captured (IST)
A-01	Home - banner	https://www.aurex.ai	Platform positioning and capability areas (Audit, Risk, Compliance, Governance, BCM, Incidents, Controls, Analytics, Data, AI/ML, Business Strategy)	13-10-2026 10:23
A-02	Home - Aurex Capabilities	https://www.aurex.ai	Risk & Controls and Governance & Compliance capability lists	13-10-2026 10:35
A-03	Home - Features	https://www.aurex.ai	Feature descriptions for Dashboards, Risk Management and Audit Management	13-10-2026 10:34
A-04	Solutions menu - Aurex Modules	https://www.aurex.ai	All seven modules: Risk Management, Business Continuity, Audit Management, Compliance & Policy Management, Analytics, Incident Reporting, Support Modules	13-10-2026 10:28
A-05	Site footer	https://www.aurex.ai	EULA, Privacy Policy and System Boundary	21-10-2026 12:32 PM

3.1.2. Each module named in A-04 also has its own public page linked from the Solutions menu, for example Risk Management and Audit Management.

3.2 What Is Published and What Is Not

3.2.1. Aurex publishes product features at module level, which is the standard set every customer starts from. Each deployment is then configured to the customer's requirements, and many are installed in the customer's own infrastructure. Those implementation details are therefore not published.

Information	Published on www.aurex.ai	How it is made available
Product modules and standard features	Yes	Public website (Section 3.1); product brochure on request
Terms, privacy, support and security commitments	Yes	Footer pages on the public website
Customer-specific configuration, workflows, source-system integrations and customisations	No	Agreed with each customer during due diligence and recorded in that customer's implementation documents
Module user manuals (e.g. Audit Management User Manual v1.0)	No	Provided to the customer's users at implementation
Hosting architecture and system boundary (this document)	No	Shared with customers and auditors on request, under confidentiality
Source code	No	Not shared outside Aurex and Beinex

3.2.2. Withholding these items does not affect the control. The control requires product features and system boundaries to be defined, maintained and accessible. Features are published at module level on the website. The boundary is defined in this controlled document and made available to the parties who rely on it.

4. Service Overview, Product Features and Service Commitments

4.1 Product Modules

4.1.1. Aurex GRC is a proprietary, AI-powered suite delivered as one web application, available in English and Arabic. All modules run inside the same application and share the in-scope components in Section 6.

Module	Key features (per brochure and website)
Digital Boardroom	End-to-end dashboard of the audit lifecycle; risk view across three lines of defence
Strategy & Performance Management	Strategy maps, goals and targets, KPI integration, links to risk, audit and compliance
Risk Management (Assessment, Aggregation, Controls)	Risk universe, scoring formulas and bands, likelihood/impact, risk controls hierarchy, self-assessment surveys
Audit Management (Planning, Reporting, Issue Tracker)	Risk-based audit plans, scheduling, budgets, timesheets, audit reports, issue and recommendation tracking
Analytics (Analytics Management, Advanced Analytics, Scenario Builder)	Exception scenarios, predictive analytics, no-code scenario builder with connectors to customer source systems

Module	Key features (per brochure and website)
Compliance & Policy Management	Compliance checklists, compliance scoring, obligation tracker; policy repository, drafting, review, approval and archiving
Business Continuity Management	Business impact analysis, continuity plans, BCM audits, RTO/RPO tracking
Incident Management	Incident logging, approval and notification workflows, dashboards
ESG	ESG goals, metrics and dashboards
Asset Management	Asset register and linkage of assets to risks and controls
AI Studio	AI-powered analytics and assistance across GRC modules
Expense, Project & Time Management	Budget allocation and utilisation, expense approval, resource allocation, timesheets
Platform features	Arabic/English switch, role-based access control, SSO, MFA, user activity (audit) log

4.2 Principal Service Commitments

4.2.1. Service levels are established under IOSA §7.1. Performance against these targets is reported weekly and reviewed by Aurex quarterly.

Commitment	Target
System availability (uptime)	99.9% monthly, excluding planned maintenance
Critical incident response (business hours)	15 minutes
High-priority incident response	1 hour
Critical CVE patch deployment	48 hours from patch availability
High CVE patch deployment	7 days from patch availability
Critical bug fix	24 hours from detection
Change request turnaround	2 business days

5. Hosting Models and Responsibilities

5.1 Hosting Models

5.1.1. Aurex GRC is deployed under one of three hosting models, selected at contracting. Data security is a shared responsibility between Aurex/Beinex and the customer in all three models.

Hosting model	Description	Infrastructure in boundary?
Client On-Premise	The customer owns, hosts and manages the infrastructure, operating systems and network. Beinex deploys, configures and releases the platform onto that infrastructure under contract to Aurex.	No - customer-managed (CUEC)
Client Cloud Tenant	The customer owns and manages a public cloud tenant in its own name. Beinex has the same platform-deployment responsibility within that tenant.	No - customer-managed (CUEC)

Hosting model	Description	Infrastructure in boundary?
Aurex-Managed SaaS	Beinex manages the full technology stack on Aurex-contracted cloud infrastructure from a pre-approved provider (IOSA §15.2): network, web, application and database tiers, monitoring, backup and security tooling.	Yes - managed by Beinex

5.2 Infrastructure Ownership and Responsibility Matrix

5.2.1. "Beinex" in this matrix means Beinex Consulting Pvt Ltd acting under contract to Aurex. Beinex Solutions LLC has no infrastructure-layer role.

Layer	Client On-Premise	Client Cloud Tenant	Aurex-Managed SaaS
Physical data center / facility	Customer	Cloud provider, under customer contract	Cloud provider, under Aurex contract
Network infrastructure	Customer	Customer (within tenant)	Beinex
Compute and OS (provisioning, patching)	Customer	Customer	Beinex
Web tier (NGINX) configuration	Shared	Shared	Beinex
Application tier (Angular, Django) deployment	Beinex	Beinex	Beinex
Database tier (MySQL, CockroachDB)	Beinex (host provided by customer)	Beinex (host provided by customer)	Beinex
Platform release and change management	Beinex	Beinex	Beinex
Backup and recovery	Customer (infrastructure); Beinex (application/database procedures)	Customer (infrastructure); Beinex (application/database procedures)	Beinex
Monitoring and logging - infrastructure	Customer	Customer	Beinex
Monitoring and logging - application	Beinex	Beinex	Beinex
Security tooling - network/endpoint	Customer	Customer	Beinex
Security tooling - application (SAST/DAST, WAF)	Beinex	Beinex	Beinex
IAM - infrastructure/OS accounts	Customer	Customer	Beinex
IAM - application accounts and roles	Shared	Shared	Shared
Data encryption in transit and at rest	Shared	Shared	Beinex
BC/DR execution	Shared	Shared	Beinex

5.2.2. In every hosting model, final production deployment authorization rests with the Aurex Technical Architect, and Beinex executes deployment only on that approval (IOSA §4.3).

6. In-Scope System Components

6.1 Infrastructure (Aurex-Managed SaaS)

6.1.1. For Aurex-Managed SaaS customers, the following infrastructure is inside the boundary. For customer-hosted models, the equivalent layers are run by the customer as shown in Section 5.2.

Component	Description
Hosting	Pre-approved public cloud provider contracted by Aurex (IOSA §15.2); a dedicated, logically isolated cloud account or subscription per customer, running Linux virtual machines
Hosting region	Agreed with each customer at contracting to meet data-residency requirements; a secondary region is used for disaster recovery
Network	Dedicated virtual network per customer; administrative access to production restricted to the Beinex DevOps group
DNS	Managed DNS service, used for normal routing and DR cut-over
Encryption at rest	Storage volumes encrypted with AES-256; keys held in the cloud provider's managed key service with access restricted to authorised users
Encryption in transit	HTTPS with TLS 1.2 or higher for user traffic and SSO exchanges
Backup	Daily (7-day retention) and weekly (30-day retention) backups of production instances, per the Backup and Restoration Procedure

6.2 Software

Layer	Technology
Web tier	NGINX (reverse proxy, TLS termination, request routing)
Application tier	Angular front end, Django (Python) back end, including AI-powered analytics and AI Studio
Data tier	MySQL (metadata) and CockroachDB (analytics)
Operating system	Linux
Identity	Application login with MFA; SAML 2.0 single sign-on with the customer's identity provider where configured
Build and release tooling	Source control and CI/CD tooling (including GitLab and Jenkins), code scanning (SAST and dependency scanning), monitoring and logging

6.3 Environments

6.3.1. Each customer has distinct Staging and Production environments. Beinex also maintains internal environments for development and testing.

Environment	Location	Customer data
Customer Production	Per-customer production instance in the agreed hosting model; app.aurex.ai for the internal Aurex tenant	Yes

Environment	Location	Customer data
Customer Staging	Per-customer staging instance, used by QA/DevOps for pre-release validation	No
Internal Staging	staging.beinex.in	No
Internal QA	qa.beinex.in	No
Development	Developer environment, segregated from production	No

6.4 People and Governance

6.4.1. Beinex Consulting Pvt Ltd personnel perform engineering, QA, DevOps, security operations, change and release management, incident management, implementation and BC/DR. Beinex Solutions LLC personnel perform account management, sales, marketing, customer support and commercial contracting. All Beinex personnel assigned to the engagement undergo background verification, sign confidentiality agreements before system access and complete annual security awareness training; access is revoked within 24 hours of separation.

Role	Entity	Core responsibility
Managing Director (Indumon Das)	Aurex	Ultimate executive authority; contract amendments; Level 3 escalation
Technical Architect	Aurex	Architecture and infrastructure approval; production deployment authorization
Product Manager	Aurex	Roadmap ownership; sprint acceptance; release governance
Project Manager	Aurex	Delivery timelines; milestone tracking
Risk Advisory & Compliance Lead (Divya Eipe)	Aurex	SOC 2 readiness; risk register; auditor liaison; risk exception approval
Founder & Executive Chairman	Beinex	Highest Beinex authority; Level 3 escalation counterpart
Engineering Lead (Ganesh Krishnan G)	Beinex	Product engineering, CI/CD, code delivery
QA Lead (Prince Kurian)	Beinex	Testing, defect tracking, release quality
Security Lead (Sachin Ullattil)	Beinex	Security controls, access management, incident response
DevOps Lead (Arun M A)	Beinex	Infrastructure, CI/CD, change/release management, BC/DR
Account Management & Sales Lead	Beinex	Customer relationships, renewals, sales, marketing

6.4.2. Functions reserved exclusively to Aurex (IOSA §3.2): final approval of security policies and exceptions; licensing and pricing; product roadmap and strategic direction; SOC 2 report ownership and distribution.

6.5 Processes, Policies and Procedures

6.5.1. The system is operated under Beinex corporate policies adopted for the Aurex GRC environment under the Policy Adoption Memo, including the Information Security Policy, SDLC Policy, Incident Management Policy, Privileged Access Policy, Supplier Security Policy, Backup and Restoration Procedure, BCM and DR Policy, and Data Retention and Secure Disposal Procedure.

6.5.2. Incidents follow a five-tier escalation structure (Level 1, 2A, 2B, 2C and 3). Security incidents affecting customer data require notification within 15 minutes; confirmed security incidents require verbal notice within 1 hour and a written report within 24 hours.

6.6 Data

6.6.1. In-scope data is customer-submitted GRC content (risks, controls, audits, policies, incidents, compliance records, uploaded evidence), platform metadata (MySQL), analytics data (CockroachDB), user account data (name, business email, role) and activity logs. Sensitive personal information is not collected, per the SPII Non-Collection and Customer Consent control. Data input types are catalogued in DDIT-AUREX-BEINEX-2026-001.

Data type	Owner	Beinex rights (IOSA §8.3)
Customer Data	Aurex / Customer	No ownership; processed only as instructed
Aurex GRC product code	Aurex	No ownership; access only for service delivery
Beinex internal data	Beinex	Full ownership
Audit evidence	Aurex (for SOC 2)	May retain copies for audit defense

6.6.2. Controls applied to customer data (IOSA §8.1) include encryption in transit (TLS 1.2+) and at rest (AES-256), mandatory MFA for privileged access, role-based access control, retention of access and activity logs for at least 90 days, quarterly access reviews, regular vulnerability scanning and annual penetration testing.

7. System Boundary Diagram

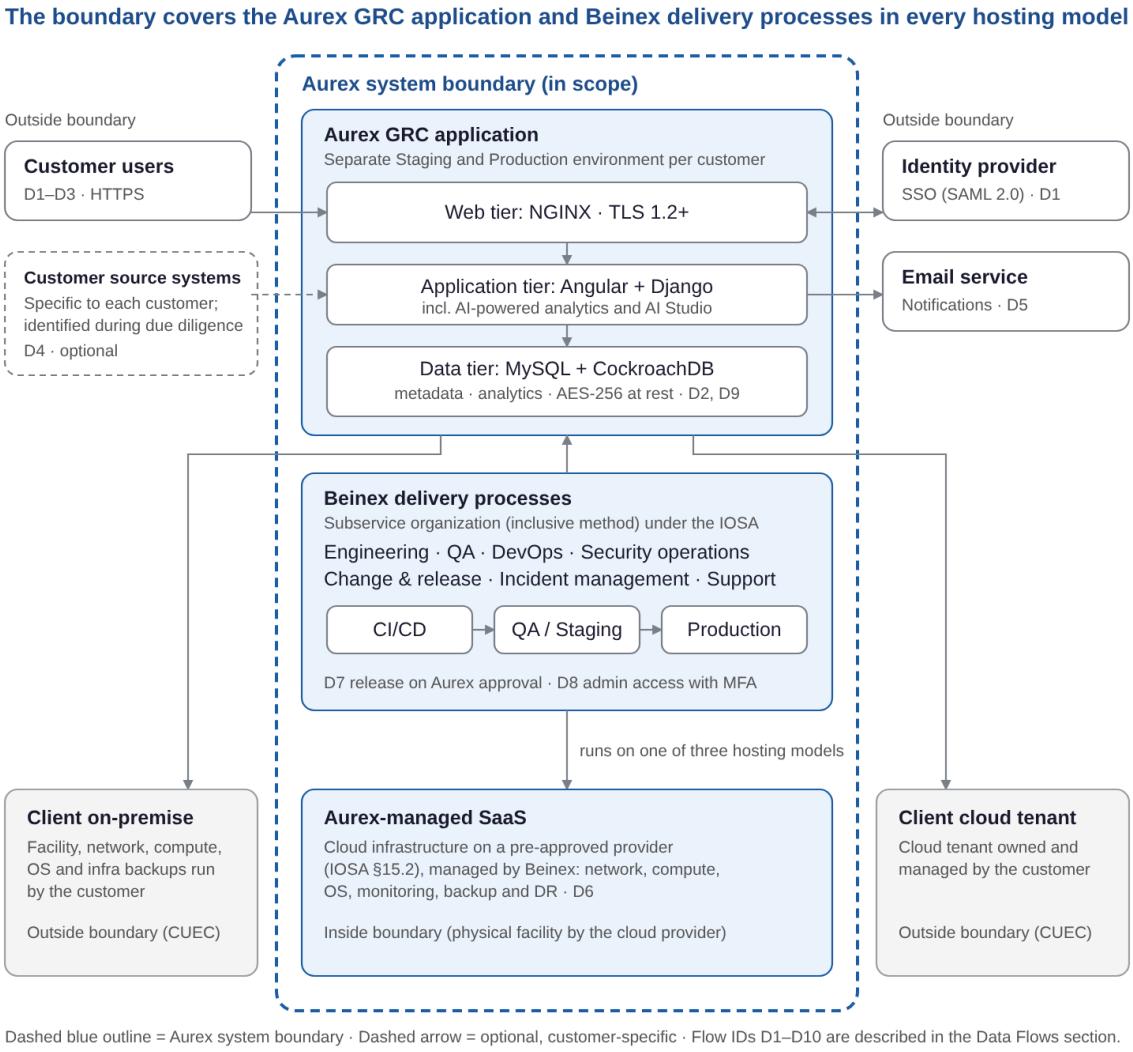


Figure 1 - Aurex system boundary across the three hosting models, with external parties and data flows D1 to D10

7.1. The application and Beinex delivery processes are inside the boundary in every hosting model. Infrastructure is inside the boundary only for Aurex-Managed SaaS. In a standard deployment only authentication (identity provider) and notifications (email) cross the boundary; customer source systems connect only where agreed for that customer.

8. Interfaces and Integrations

8.1. In a standard Aurex deployment the only third-party runtime integration is single sign-on with the customer's identity provider (for example Microsoft Entra ID). Any other integration exists only where a customer requests it, and then follows that customer's own security requirements.

Interface	Direction	Protocol / security	Standard or optional
End-user web access (browser, tablet, mobile)	Inbound	HTTPS, TLS 1.2+, via NGINX; MFA at login	Standard

Interface	Direction	Protocol / security	Standard or optional
Customer identity provider (SSO)	Inbound authentication assertion	SAML 2.0 over TLS, valid signing certificate	Standard where SSO is enabled
Email notifications (workflow alerts, follow-ups)	Outbound	SMTP over TLS	Standard
Customer source systems	Inbound data pull or upload	Defined per customer during due diligence (Section 8.1)	Optional, customer-specific
Customer directory (AD/LDAP)	Inbound authentication	LDAPS, per customer requirement	Optional, customer-hosted models only
Administrative access (Beinex DevOps)	Inbound	Cloud console and IAM with MFA; production application access via SSO (LDAP decommissioned 10 August 2026)	Standard

8.1 Customer Source Systems

8.1.1. Source systems differ for each customer and are not fixed in advance. They are identified only during the pre-implementation due diligence for that customer, together with the integration method (connector, scheduled extract or file upload), data scope, frequency and the security controls for the connection. The outcome is recorded in that customer's implementation documents (Ordering Document, Statement of Work or solution design) and approved before any connection is built.

8.1.2. The source systems themselves remain owned and operated by the customer and are outside the boundary. Data from them comes into scope once it enters the Aurex GRC application (flow D4).

9. Data Flows

9.1. Customer data enters through the browser or an agreed source-system connection, is stored encrypted in the customer's Aurex environment, and leaves only as user downloads, email notifications, or backups that stay within the hosting environment. Code moves the other way, from source control through QA and staging to production, and never carries customer data.

ID	Flow	From -> To	Data	Protection
D1	User sign-in	User browser -> NGINX -> Django; optional redirect to the customer identity provider and back	Credentials, MFA code or SAML assertion	TLS 1.2+; MFA; signed SAML 2.0 assertion
D2	Data entry and evidence upload	User browser -> application -> MySQL / CockroachDB	GRC records, attachments	TLS 1.2+ in transit; AES-256 at rest
D3	Reports and exports	Application -> user browser	Reports, dashboards, exports	TLS 1.2+; role-based access
D4	Customer source data (optional)	Customer source systems -> agreed connector or upload -> application	As defined for that customer during due diligence	Encrypted channel and controls agreed per customer

ID	Flow	From -> To	Data	Protection
D5	Notifications	Application -> email service -> users	Workflow alerts (record title, link, no attachments)	TLS on SMTP
D6	Backup and DR	Production instances -> backup storage in the hosting environment; DR copy to a secondary region (SaaS)	Instance and database backups	Encrypted backups; access restricted to DevOps
D7	Release of code	Source control -> QA -> staging -> production	Application code and configuration only	Aurex Technical Architect approval; no customer data in lower environments
D8	Administrative access	Beinex DevOps engineer -> cloud console/IAM (MFA) -> hosting network and instances	Operational access	MFA; DevOps group only
D9	Activity logging	Application -> audit log	User, time, action, affected record	Retained at least 90 days; read access restricted to administrators
D10	Deletion on exit or opt-out	Customer request -> Beinex DevOps -> database and backups	Customer records	Per Customer Opt-Out and Data Retention and Secure Disposal procedures

10. Subservice Organization and Third-Party Dependencies

10.1. Beinex is the only subservice organization and is presented under the inclusive method (Section 2.2). The vendors below support the service but do not perform controls on Aurex's behalf; they are managed under the Supplier Security Policy (SSP-AUREX-BEINEX-2025-001) and reviewed annually.

Party	Service used	Customer data?	Treatment	Assurance obtained
Beinex (Consulting Pvt Ltd; Solutions LLC)	Engineering, operations, security, support and commercial delivery	Yes - processed as instructed	Subservice organization, inclusive method	Controls tested within the examination; ISO 27001:2022 maintained by Beinex
Cloud hosting provider (Aurex-Managed SaaS only)	Physical facilities, virtual infrastructure, key management, backup storage, DNS	Hosts SaaS customer data	Pre-approved infrastructure provider (IOSA §15.2)	Provider's independent assurance reports (SOC 2 / ISO 27001), reviewed annually
Microsoft	Entra ID (SSO for internal production access), Microsoft 365 email	User identity attributes only	Supporting vendor	SOC 2 / ISO 27001, reviewed annually
GitLab	Source code repository, CI/CD	No	Supporting vendor	ISO 27001 certificate (vendor due diligence 23-09-2026)
Snyk	Dependency (SCA) scanning	No	Supporting vendor	ISO 27001 certificate

Party	Service used	Customer data?	Treatment	Assurance obtained
SonarSource	Static code analysis (SAST)	No	Supporting vendor	ISO 27001 certificate
Atlassian	Work tracking and documentation	No	Supporting vendor	ISO 27001 certificate
Figma	UI design	No	Supporting vendor	ISO 27001 certificate

10.2. For customer-hosted models, any cloud or infrastructure provider is contracted and managed by the customer and is outside the boundary.

11. Exclusions

11.1. The items below are outside the system boundary.

Excluded item	Reason	Responsible party
Customer-managed infrastructure in the Client On-Premise and Client Cloud Tenant models (facility, network, compute, OS, infrastructure backups and monitoring)	Owned and operated by the customer; addressed as Complementary User Entity Controls (Section 12)	Customer
Non-operational affiliates: Aurex AI FZ-LLC, Aurex.AI Private Limited and the five regional Beinex entities (Section 2.3)	No delivery personnel, infrastructure or control responsibilities relevant to the Trust Services Criteria	Aurex / Beinex
Customer source systems	Customer-specific, defined during due diligence and operated by the customer; data is in scope only once it enters Aurex (flow D4)	Customer
Customer identity providers and user provisioning decisions	Customer decides who gets access and manages its own directory	Customer
End-user devices and customer networks	Not owned or managed as part of the service	Customer
Public marketing website (www.aurex.ai) and partner portal	Publish product information only; no customer production data	Aurex marketing
Aurex Neo (next-generation version)	Under development and internal testing; not yet serving customers	Aurex (to be added when released)
Corporate systems not used to build or run Aurex (HR, finance) and advisory services	Not part of the Aurex GRC service	Beinex

12. Complementary User Entity Controls

12.1. The control environment assumes customers implement the following controls. Items marked "where applicable" apply mainly to the Client On-Premise and Client Cloud Tenant models.

- Maintain physical and environmental security of the data center or cloud tenant, where applicable.

- Provision, patch and secure operating systems, network devices, firewalls and cloud tenant configuration, where applicable.
- Maintain infrastructure-level backup, recovery and BC/DR capabilities for customer-managed layers, where applicable.
- Approve, provision, remove and periodically review their own users' access within their Aurex GRC tenant.
- Configure and secure their identity provider when using SSO, including MFA and account disablement on exit.
- Secure the source systems, credentials and channels used for any agreed source-system integration.
- Upload only the data types agreed for the service and do not enter sensitive personal information.
- Notify Aurex/Beinex promptly of any suspected security incident or unauthorized access.
- Use the platform in accordance with the Aurex EULA and applicable policies; raise deletion or opt-out requests through the agreed channel.

13. Auditor Response Log

#	Crowe comment	Response	Evidence
1	Provide the product website link or screenshots showing product features and system boundary information are accessible over the Internet.	Product features are published at https://www.aurex.ai, including the Solutions menu of seven modules and dedicated module pages; the EULA, Privacy Policy, System Boundary are linked from the footer. Because modules are configured to each customer's requirements and often installed in the customer's own infrastructure, customer-specific implementation details, user manuals and source code are not published; the detailed boundary is a controlled document shared with customers and auditors on request (Section 3.2).	Section 3; Annexure A (dated screenshots A-01 to A-06)
2	Provide the documented system boundary showing third-party dependencies, data flows and exclusions.	This document defines the entities in scope, the three hosting models and responsibility matrix, in-scope components, interfaces (including customer-specific source systems), ten data flows, a boundary diagram, the subservice organization and third-party dependencies, exclusions and customer responsibilities, consistent with the Aurex GRC Platform System Description.	Sections 2 and 5 to 12; SDSB-AUREX-BEINEX-2026-001 v1.0 with sign-off (Section 16)

14. Document Review & Maintenance

16.1. This document shall be reviewed:

- Annually, as part of the Beinex/Aurex management review process
- After any change to the System Description, the IOSA or the Policy Adoption Memo
- After any change to hosting models, pre-approved cloud providers or subservice arrangements
- After any change to supporting vendors or standard third-party integrations
- After a module or major product version (including Aurex Neo) enters customer production

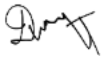
14.2. The Security Lead, Beinex is responsible for maintaining this document and coordinating its annual review with the Risk Advisory & Compliance Lead, Aurex. All revisions require approval by the Managing Director, Aurex.

15. Revision History

Version	Date	Author	Summary of Changes	Approver	Approval Date	Sign off Evidence
1.0	14-10-2026	Sachin Ullattil, Security Lead, Beinex Consulting Pvt. Ltd.	Initial document, issued in response to Crowe comments on the product features and system boundary control and aligned with the Aurex GRC Platform System Description. Includes dated website screenshots (Annexure A).	Indumon Das, Managing Director, Aurex Technologies		See Section 16 - Document Approval & Sign Off

16. Document Approval & Sign Off

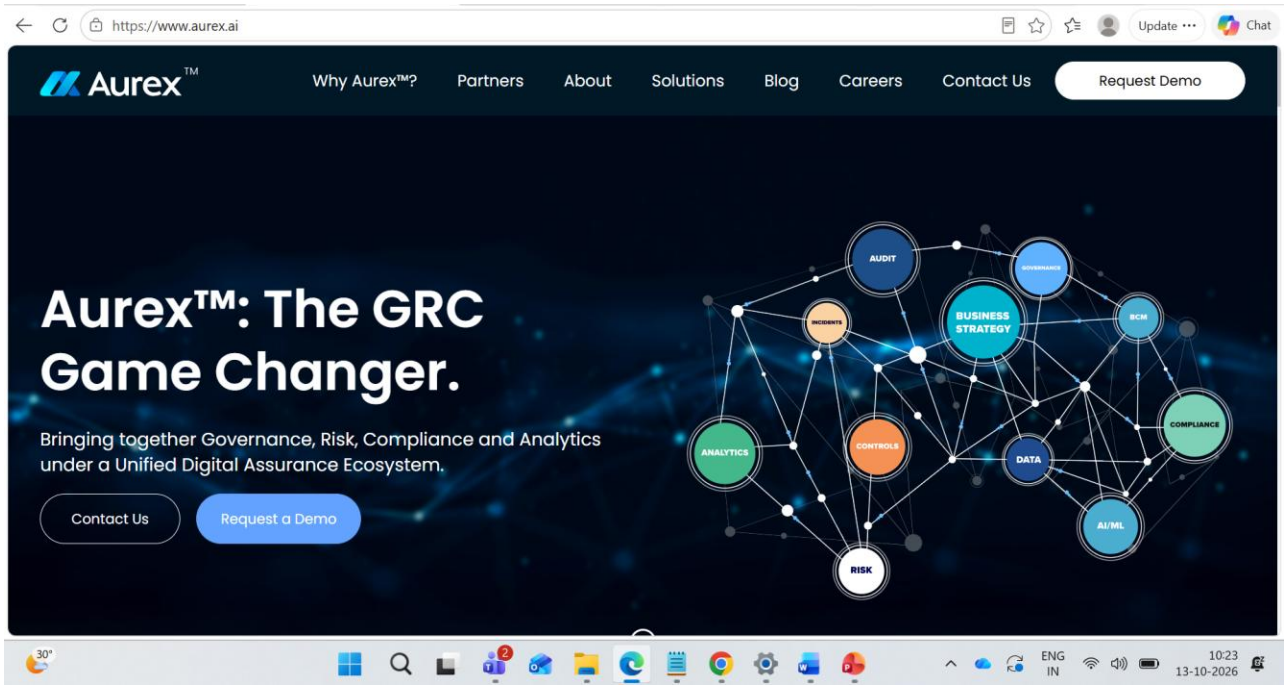
16.1. This document has been drafted, reviewed and approved in accordance with the roles, names and dates recorded below. Physical or digital signatures appended by each named individual as corroborating sign-off evidence.

Role	Name	Title/Organisation	Date	Signature
Author	Sachin Ullattil	Security Lead, Beinex Consulting Pvt. Ltd.	13-10-2026	
Reviewed & Recommended By	Divya Eipe	Risk Advisory & Compliance Lead, Aurex Technologies Limited	14-10-2026	
Approved By	Indumon Das	Managing Director, Aurex Technologies Limited	14-10-2026	

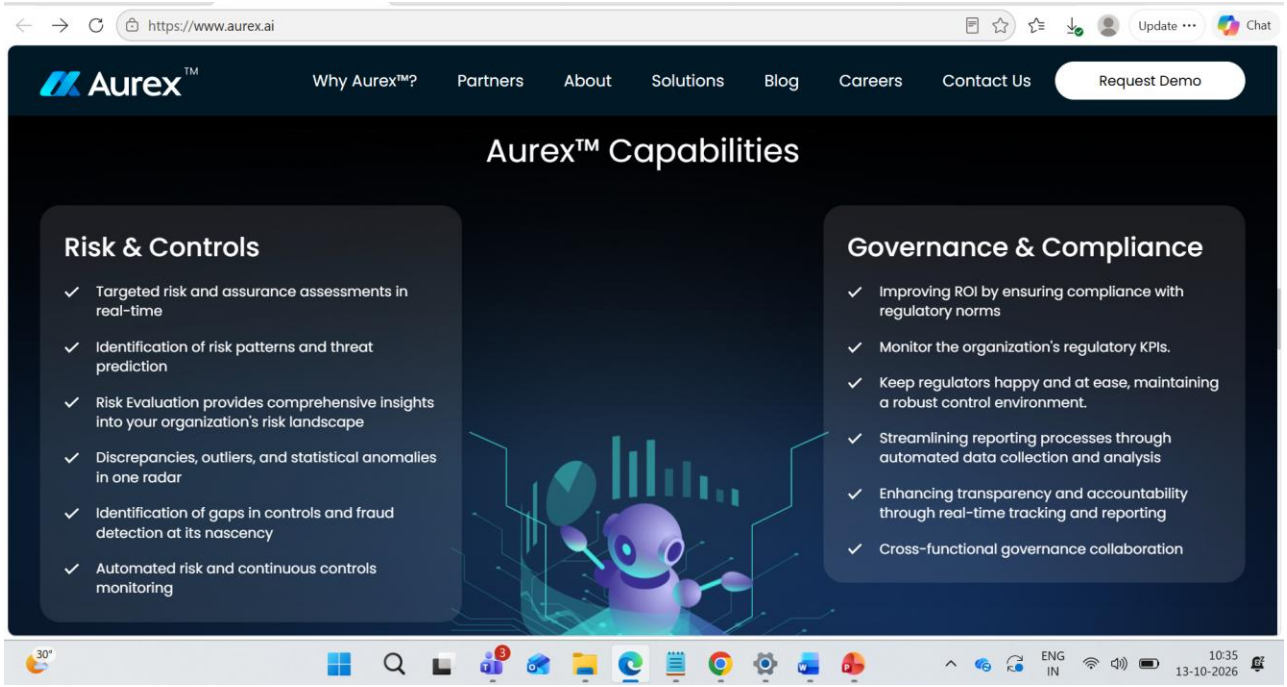
Annexure A - Product Website Screenshots

A.1. The screenshots below were captured by Sachin Ullattil on 13 October 2026 from the public website in Microsoft Edge on Windows. Each shows the browser address bar and the system date and time. A-04 is a photograph of the screen, because the Solutions menu closes when a screen-capture key is pressed.

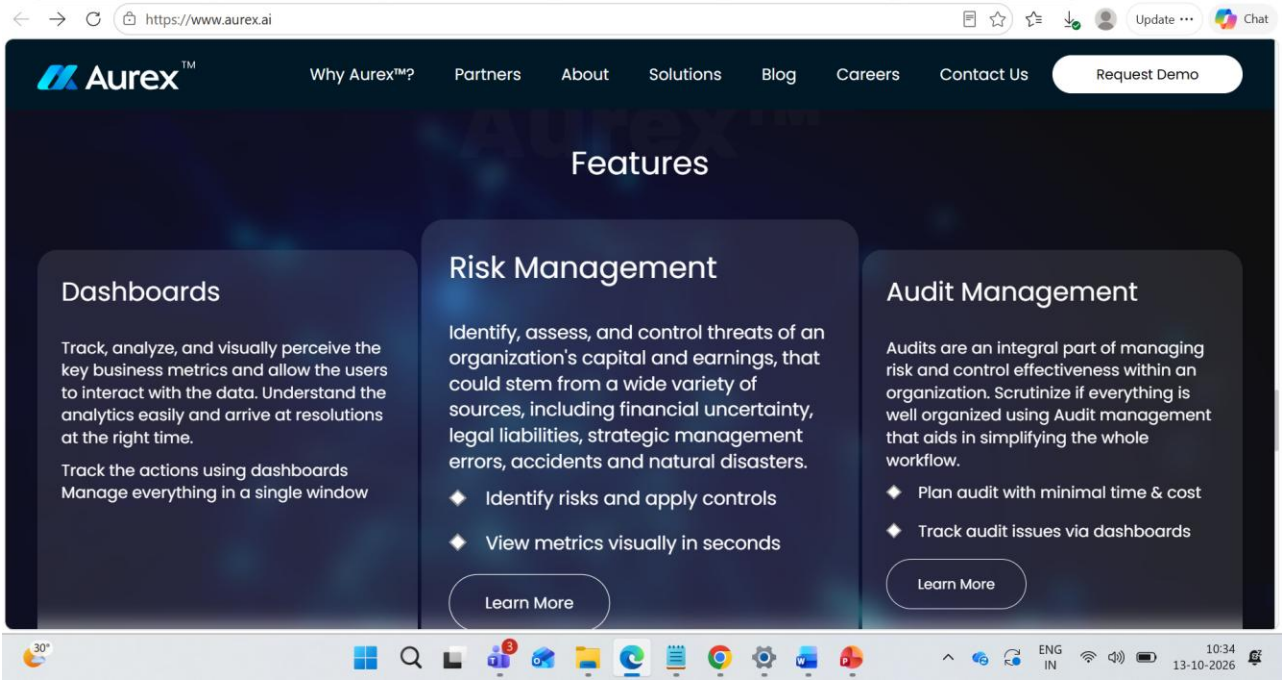
A-01 - Home page banner - https://www.aurex.ai - 13-10-2026 10:23 IST



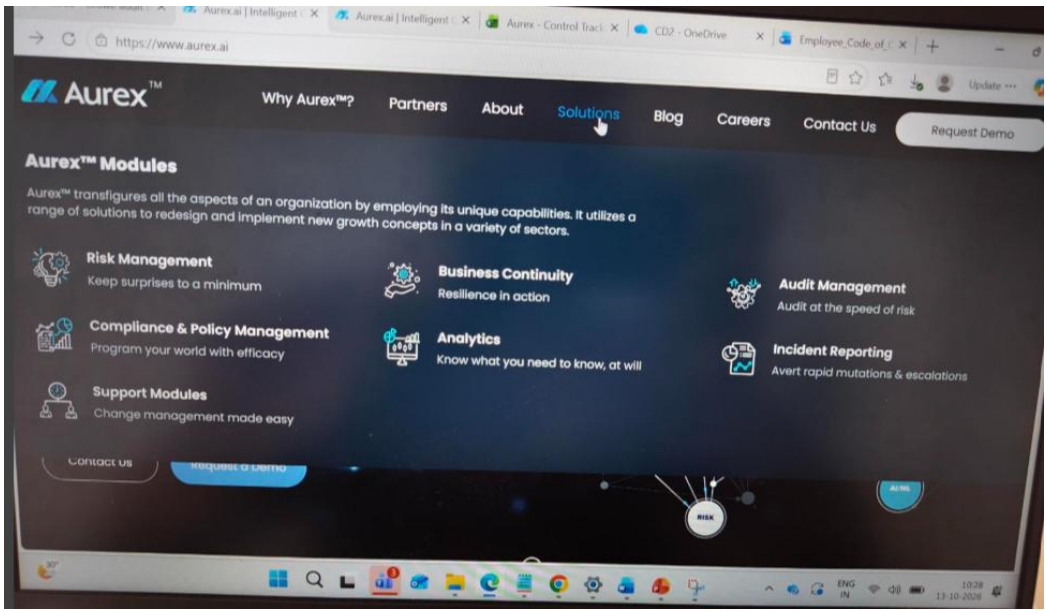
A-02 - Aurex Capabilities section - https://www.aurex.ai - 13-10-2026 10:35 IST



A-03 - Features section - https://www.aurex.ai - 13-10-2026 10:34 IST



A-04 - Solutions menu listing all Aurex modules - https://www.aurex.ai - 13-10-2026 10:28 IST



A-05 - Site footer with policy links - https://www.aurex.ai - 21-10-2026 12:32 PM

