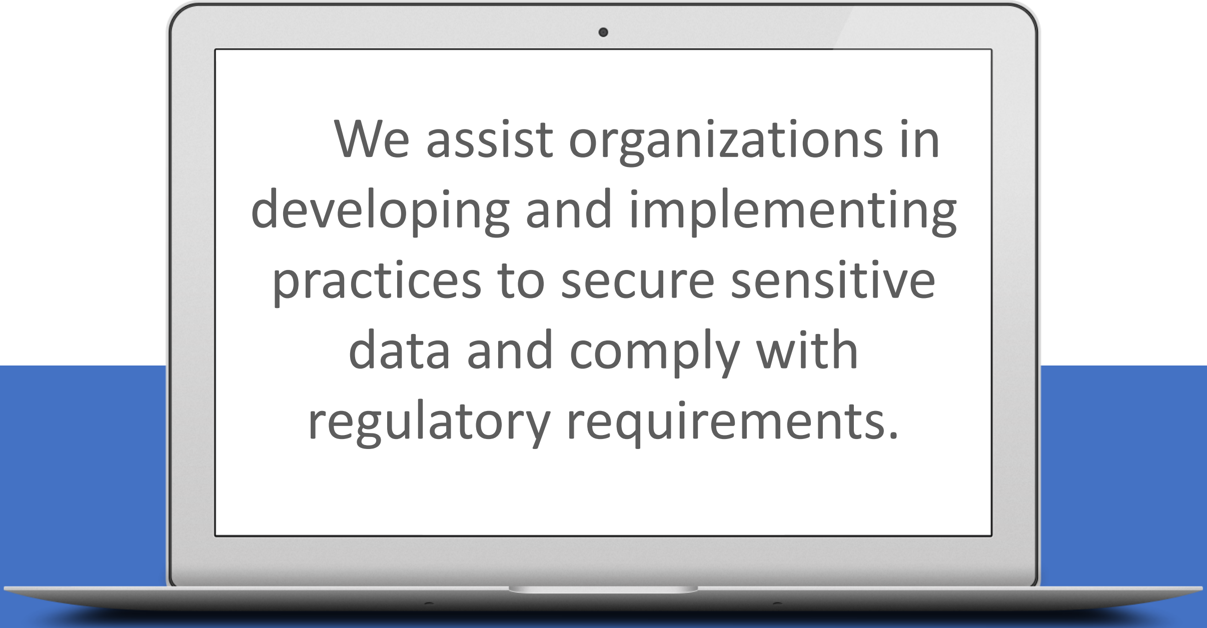
ISO 27001 Information Security Management System

Implementation and Certification Process

databrackets
info@databrackets.COM
866-276-8309

{databrackets}
cybersecurity • audit • compliance

About Us



We assist organizations in developing and implementing practices to secure sensitive data and comply with regulatory requirements.

DIY TOOLKIT

DIY assessment, training, customized policies & procedures and much more …

CONSULTING

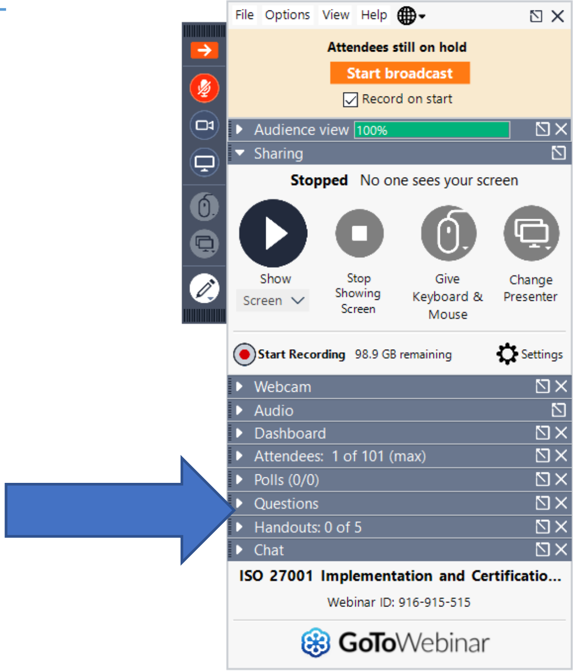
Professional services to help you with your Compliance needs

MANAGED SERVICES

Managed compliance and security services to focus on your key business outcome.

Webinar Logistics

- Submit your questions via GTW Chat/Question Panel (thanks to those who have already submitted your questions)
- Presentation deck available for download under the handout section
- Recording links will be emailed within the next 24 hrs.
- Please participate ☺



Disclaimer

Consult your attorney

This webinar has been provided for educational and informational purposes only and is not intended and should not be construed to constitute legal advice.

Please consult your attorneys in connection with any fact-specific situation under federal law and the applicable state or local laws that may impose additional obligations on you and your company.

Agenda

{databrackets}
cybersecurity • audit • compliance

1 Background

2 Overview of ISO 27001:2013

3 Risk-based Approach

4 Certification Process Flow

5 Families and Controls

6 Cross Mapping

7 Portal Demo

8 Questions & Answers

Always available via email to answer any questions

Srini's Background

Srini Kolathur

CISSP, CISA, CISM, MBA

Director, databrackets

- Security and Compliance
- Cisco IT Infrastructure
- HIPAA, PCI, Sarbanes-Oxley and ISO 27k Series
- Proud Rotarian
- Interests: Running, healthy living and giving back

{databrackets}
cybersecurity • audit • compliance

Benefits of ISO 27001 Certification

- ✓ Differentiator from your peers/competition: **Demonstrate Compliance**!
- ✓ Builds trust with consumers which can boost revenues – larger customers/ satisfy RFP requirements
- ✓ May result in opportunities for improvements to existing control environment
- ✓ “Easy” response to audit requests from customers and their auditors with consistent approach
- ✓ Evaluate sub-service providers (Use this excuse)
- ✓ Always certified by an accredited third-party

One of the fastest growing information security certifications for businesses

Certification Background

- Based on the Information Security Management System (ISMS) certification examination in conformity with defined requirements of ISO/IEC 27001:2013 standards
- Standards is prepared by Joint Technical Committee ISO/IEC JTC 1, Information technology, Subcommittee SC 27, IT Security techniques
- This International Standard has been prepared to provide requirements for establishing, implementing, maintaining and continually improving an information security management system

Certification Background … Cont'd

- The information security management system preserves the **confidentiality, integrity and availability** of information by applying a risk management process and gives confidence to interested parties that risks are adequately managed
- This International Standard specifies the requirements for **establishing, implementing, maintaining and continually improving an information security management system** within the context of the organization

Certification & Implementation - Overview

- Certification and implementation/consulting engagements to be separate (Impartiality and conflict)
- Readiness/Preparation
- Stage 1 and Stage 2 Audit
  - Stage 1 – Readiness
  - Stage 2 – Certification Audit
- Surveillance Audit
- Re-certification Audit
- Cross Mapping with Other Standards (NIST, SOC 2, etc.,)

Certification & Implementation – Timeline*

- Majority of time spent in readiness
- Point-in-time Audit
- Readiness – Approximately 8 to 12 weeks
- Certification Audit – 3 to 6 weeks
- Surveillance Audit – Every year
- Re-certification (full) audit – Every 3 years

Timeline varies based on the size, sites and complexity of the business

Certification & Implementation – Cost*

- Cost is based on # of Staff, Sites and Complexity
- Scope of the engagement
- Other certifications/attestation
- Suppliers/outsourcing activities
- Starts from $15k
- Travel costs for onsite audit

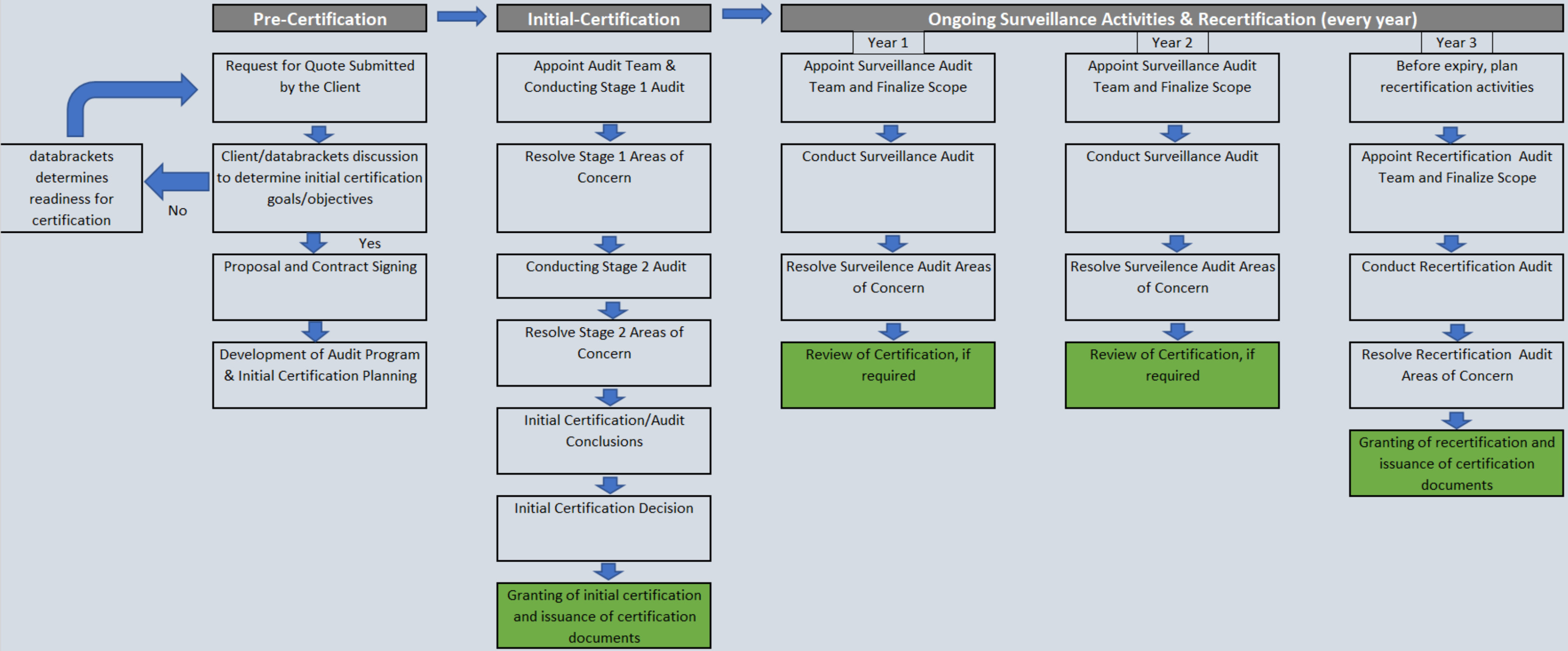
Cost varies based on the size, sites and complexity of the business

ISO 27001 Key Controls

4. Context of the organization	A.8 Asset management
5. Leadership	A.9 Access control
6. Planning	A.10 Cryptography
	A.11 Physical and environmental security
7. Support	A.12 Operations security
8. Operation	A.13 Communications security
9. Performance evaluation	A.14 System acquisition, development and maintenance
10. Improvement	A.15 Supplier relationships
A.5 Information security policies	A.16 Information security incident management
A.6 Organization of information security	A.17 Information security aspects of business continuity management
A.7 Human resource security	A.18 Compliance

150+ individual controls based on Statement of Applicability

ISO 27001 Audit and Certification Process Flow Chart



Pre-Certification

Request for Quote Submitted by the Client

Client/databrackets discussion to determine initial certification goals/objectives

No

databrackets determines readiness for certification

Yes

Proposal and Contract Signing

Development of Audit Program & Initial Certification Planning

Initial-Certification

Appoint Audit Team & Conducting Stage 1 Audit

Resolve Stage 1 Areas of Concern

Conducting Stage 2 Audit

Resolve Stage 2 Areas of Concern

Initial Certification/Audit Conclusions

Initial Certification Decision

Granting of initial certification and issuance of certification documents

Ongoing Surveillance Activities & Recertification (every year)

Year 1

Appoint Surveillance Audit Team and Finalize Scope

Conduct Surveillance Audit

Resolve Surveilence Audit Areas of Concern

Review of Certification, if required

Year 2

Appoint Surveillance Audit Team and Finalize Scope

Conduct Surveillance Audit

Resolve Surveilence Audit Areas of Concern

Review of Certification, if required

Year 3

Before expiry, plan recertification activities

Appoint Recertification Audit Team and Finalize Scope

Conduct Recertification Audit

Resolve Recertification Audit Areas of Concern

Granting of recertification and issuance of certification documents

Certification Objectives

- ✓Assess the readiness of the Org. against applicable ISO 27001:2013 requirements
- ✓Identify systems collecting/using/storing/processing information by various business processes and IT systems in the organization
- ✓ Identify specific gaps within business processes and IT systems against requirements
- ✓Identify and report the common security gaps across the organization
- ✓ Provide certification, as applicable, and high-level guidance to help address the gaps to meet ISO 27001 obligations

Annual recertification is required

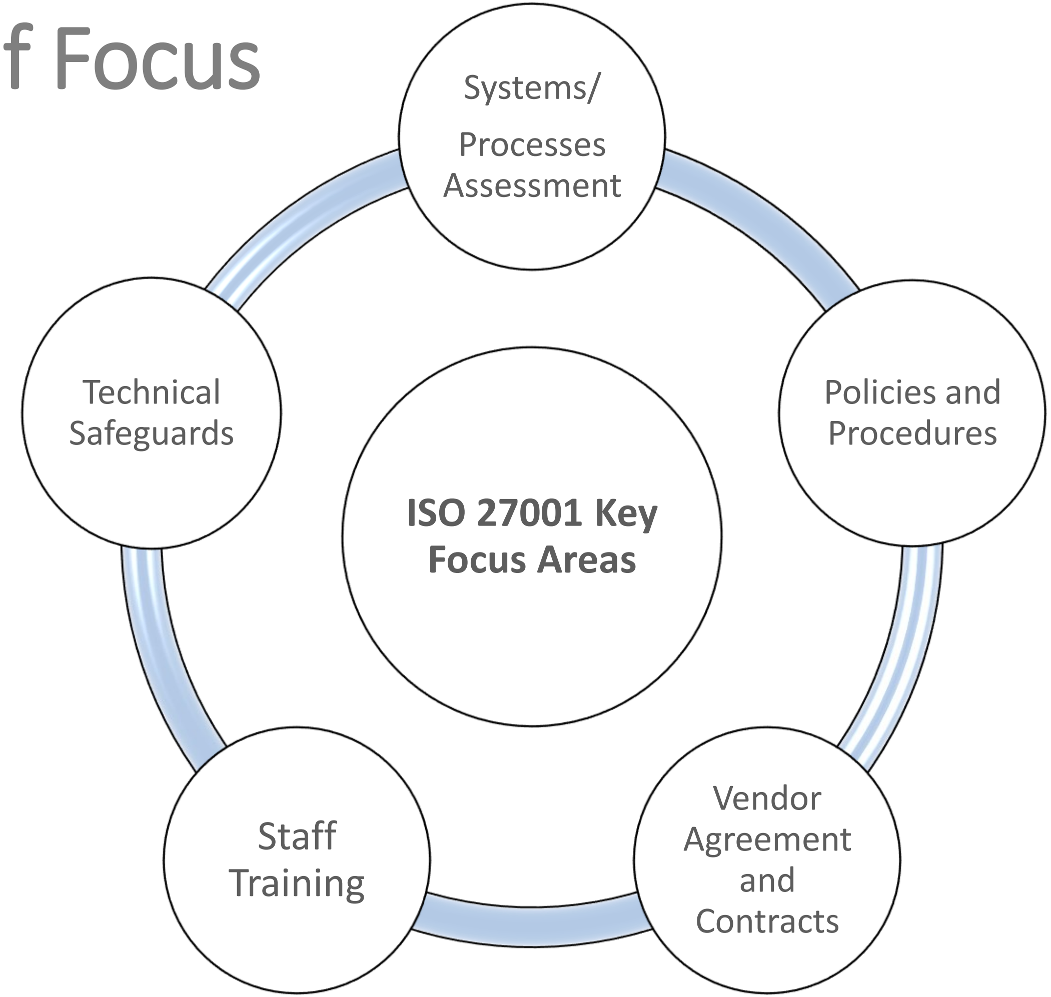
Scope

Any device that electronically stores or transmits information

- Core systems, File servers, E-mail, etc.,
- Computers
- Storage Devices (HD, FD, CD, DVD)
- Networking Devices (Routers, Switches, & Wireless)
- Smart-Phones, Tablets
- Cloud-Based Services
- Any other interfaces
- Third-party Contractors

ℹ Up to date data inventory sheet to be maintained

Top 5 Areas of Focus



ISO 27001 Key Focus Areas
Systems/ Processes Assessment
Policies and Procedures
Vendor Agreement and Contracts
Staff Training
Technical Safeguards

Documentation is to be maintained for 6 years

Data Security Programs

{databrackets} cybersecurity • audit • compliance

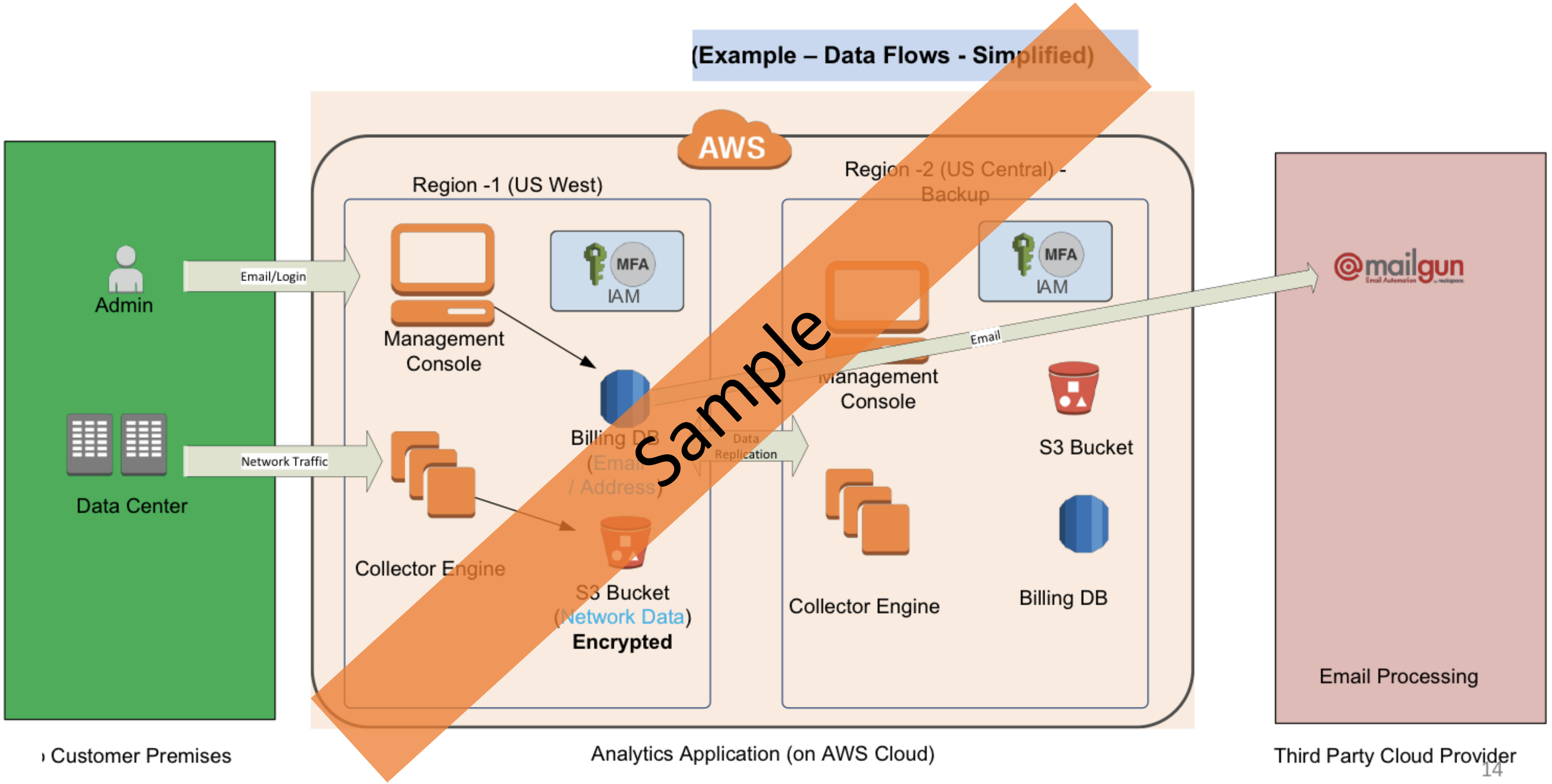
1. Security Program	Roles & Responsibilities External Parties
2. Security Policy	Policies and Procedures
3. Training & Awareness	Sanction, awareness training and reminders
4. Personnel Security	Background Checks, T&C, Termination Checklist
5. Physical Security	Secure Area
6. Operations Management	AV, Security Monitoring, Media Handling, Disposal, SOD
7. Incident Management	Process and Procedures
8. Business Continuity	Emergency access, Backup and DRs

Policies and Procedures

- □ **Physical Security Policy**
  - □ Maintenance record
  - □ Disposal
  - □ Access
- □ **Information Security Policy**
  - □ Access Policy
  - □ Sanction Policy
- □ **Contingency Plan Policy**
- □ **Security Incident Procedure/Breach**

- Master Security Policy
- Master Breach Policy

Sample Data Flows

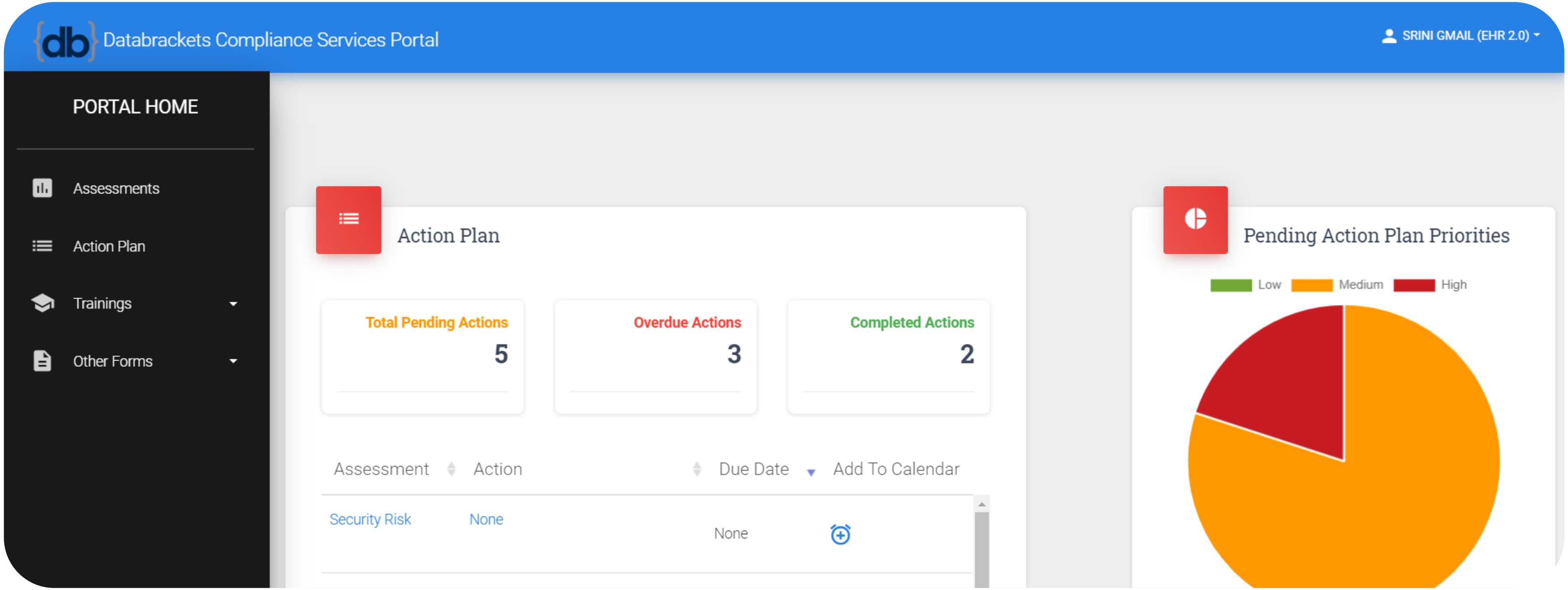


Deliverables

- ✓ISO 27001 Standards Assessment Report
  - ✓Scoping and Profiling
- ✓ISO 27001 Digital Certificate (finalized by the grant committee)
- ✓Portal Access to Track & Manage Control Deficiencies

Usually ISO 27001 certification audit is done after pre-audit/consulting by a third-party

databrackets online portal



Action Plan

Total Pending Actions	Overdue Actions	Completed Actions
5	3	2

Assessment	Action	Due Date	Add To Calendar
Security Risk	None	None	

Pending Action Plan Priorities

What is Expected from your Team

{databrackets} cybersecurity • audit • compliance

- ❑ Security Officer – The Point-Of-Contact
- ❑ IT Support Team – Network, End Device and Architecture
- ❑ List of Stakeholders and/or Owners of Business Processes
- ❑ Management Team (To review the final audit report)
- ❑ About 4 to 8 hours/week of your staff time is required to complete the project

ⓘ Annual recertification is required

Next Steps

{databrackets}
cybersecurity • audit • compliance

1. Signed Service Contract
2. Scoping, profiling and preparation of assessment plans – 3 to 4 weeks
3. ISO 27001 Certification Audit - 6 to 8 weeks
4. Audit Results/Certification Decision – 2 weeks

We provide audit support/guarantee for all our consulting customers

UPCOMING EVENTS

Feb’ 11 @ 1 p.m. ET: GDPR Compliance Readiness

Register now >> https://databrackets.com/events/

Find Us

CALL US
866-276 8309

SERVICE
info@databrackets.com

LOCATION
150, Cornerstone Dr.
Ste.#202, Cary, NC

SOCIALIZE
Facebook
Twitter

Twitter: @databrackets

Facebook: databrackets

Questions

Please don't hesitate to ask

Thank You

for your attention!

{databrackets}
cybersecurity • audit • compliance