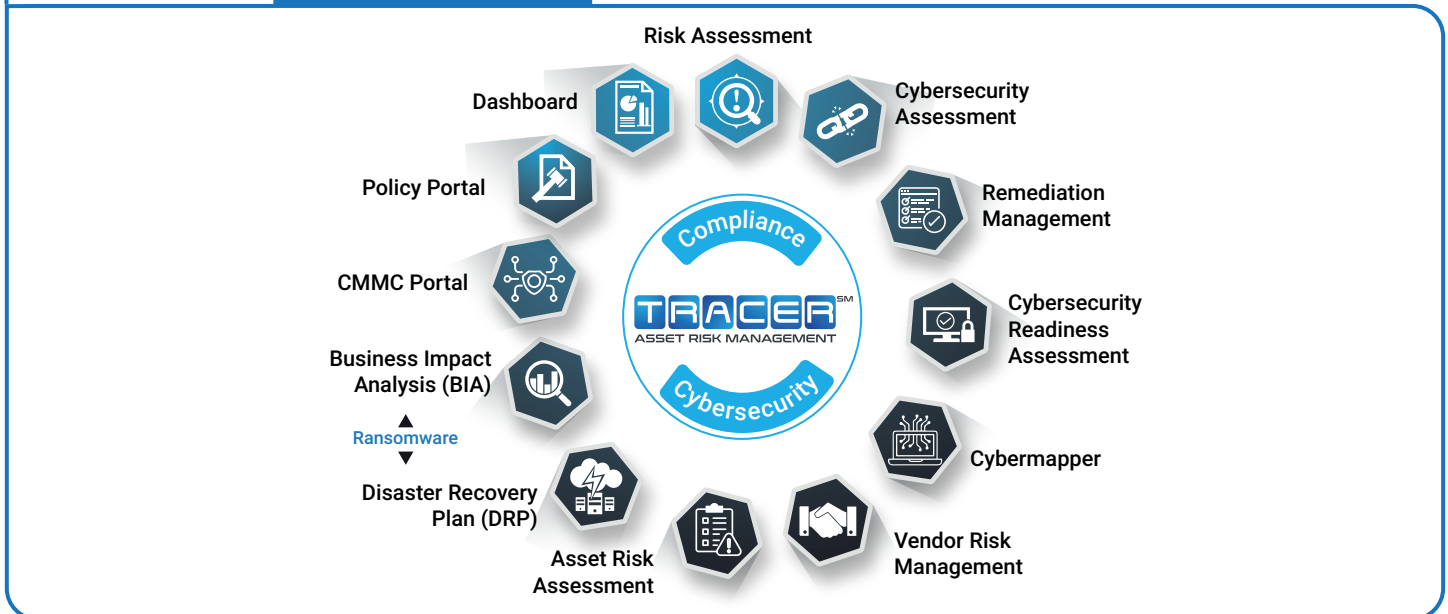




Features



Compliance

NIST SP 800-171

Search

TRACERSM

NIST DCF

Key Staff

Policy

Procedure

Evidence

Questionnaire

DRP

Security Controls

CMMC

Search

TRACERSM

CMMC Level 1 Self-Assessment

Phase 1 Planning

Phase 2 Self-Assessment

Phase 3 Confirmation

Phase 4 Generate Report

Reference

Dashboard

HIPAA

Search

TRACERSM

OCR Audit Protocol

OCR Policy

Service	Key Activity	Audit Inquiry	View to Policy
516.003(a)(1)	Prohibited uses and disclosures - Use and disclosure of health information for unauthorized purposes	Check for health plan use or disclosure for unauthorized purposes, Check for information on subject's 160-103 including family history	Select

Vendor (BA) Management

Search

TRACERSM

Vendor (BA) Management Portal

View

Vendor Name	Last Review Date	Type of Review	Point of Contact Name	Point of Contact Title	Point of Contact Email	Action
AT	Mar 1, 2021	Legal Services	J	J	J	View

Asset Risk Management

Search

TRACERSM

Asset Risk Management

Total # of Assets: 10

Pending Assets: 3

Total # of Assets: Assessment: 0

Asset List

APPLICATION NAME	USER NAME	EMAIL	ROLE	POC IT	DATE	ACTION
3M Clean Trace	Mary Johnson	mjohnson@3m.com	POC IT	mjohnson@ecfirst.com	Dec 28, 2021	View
3M Clean Trace	John Smith	jsmith@ecfirst.com	POC IT	jsmith@ecfirst.com	Dec 28, 2021	View

Policy Portal

Policy Dashboard

Client Login

Dashboard

Security Policy Library

Search

File Name	File Type	File Size	Action
Implement Subnetworks Policy	PDF	1.5 MB	View
Limit System Access to Types of Transaction Policy	DOCX	257.4 KB	View
Escort and Monitor Visitors Policy	DOCX	150 KB	View

NIST SP 800-171

Phase 1 Planning

Search..



Intake Form

100%



Roles

75%



SSP

50%



General

82.2%



Policy & Procedure

30%



Evidence

67%

Sample Report



Risk Assessment
NIST SP 800-171

October 24, 2022



Cyber Readiness



CMMC Portal

Search...



CMMC Level 1

Back

Home / Assessment / CMMC Level 1 Self-Assessment

Self-Assessment

Phase

1

Planning

Phase

2

Self-Assessment

Phase

3

Confirmation

Phase

4

Generate Report

Phase

5

POA&M

Reference

Dashboard

HIPAA Portal

Area Agency on Aging

HIPAA Risk Assessment Area Agency on Aging Back

[Home](#) / [Assessment](#) / [HIPAA Risk Assessment](#)

General Information

ID of Key Staff

Policy Questionnaire

100%

Procedure Questionnaire

100%

Security Control Information

70%

Applications / Evidence

97%

Walkthrough

32%

Vendor Risk Management Portal

Vendor Risk Management Portal ecfirst Back

[Home](#) / [Vendor Risk Management Portal](#)

Total # of Vendor(s) **3**

Pending Vendor(s) **2**

Total # of Vendor(s) Assessed **1**

Vendor(s) Status

30%

Vendor 1

50%

Vendor 2

13%

Vendor 3

Vendor Administration

Onboarding Vendor

Offboarding Vendor

Access Control

Awareness and Training

Audit and Accountability

Configuration Management

Identification and Authentication

Incident Response

Maintenance

Media Protection

Personnel Security

Physical Protection

Risk Assessment

Security Assessment

System and Communications Protection

System and Information Integrity

Approvals and Comments

© ECFIRST. ALL RIGHTS RESERVED. 2023

PAGE 3

Asset Risk Assessment

Asset Risk Management
ecfirst
Back

[Home / Asset Risk Management](#)

Total # of Asset(s) **10**

Pending Asset(s) **3**

Total # of Asset(s) Assessed **0**

Asset List

[Export to Excel](#)

APPLICATION NAME	↑↓ USER NAME	↑↓ EMAIL	↑↓ ROLE	↑↓ POC IT	↑↓ DATE	↑↓ ACTION
3M Clean Trace	Mary Johnson	maryjohnson@dib.org	POC IT	maryjohnson@assettracer.com	Dec 28, 2021	✎ 🗑
3M Clean Trace	John Smith	johnsmith@ventures.org	POC IT	johnsmith@assettracer.com	Dec 30, 2021	✎ 🗑

Asset Risk Administration

Department Master

Vendor Master

Application Master

User Master

Interview Schedule

Ransomware Readiness

Disaster Recovery Plan

10.0%

- Instructions
- In-scope Locations **100.0%**
- Roles and Responsibilities **0.0%**
- Data Center Operations **0.0%**

BIA

38.8%

- BIA-Data Collection Form **55.3%**
- BIA IT-Data Collection Form **22.2%**

IT Disaster Recovery Plan

Data Center Operations

Item	Primary Data Center	SECONDARY Data Center
Building Structure / Environment		
Building Location, Floor Number	<input type="text"/>	<input type="text"/>
Sq. Footage of Data Center	<input type="text"/>	<input type="text"/>
Structure Type	<input type="text"/>	<input type="text"/>

Policy Portal

Policy Dashboard



Dashboard

[Back](#)
[Home](#) / [Policy](#) / [Dashboard](#)

Security Policy Library

[Upload](#)
[Create](#)
[Index](#)

Search:

Show more

3



File Name	File Type	File Size	Action
Implement Subnetworks Policy	PDF	1.5 MB	Edit Download Delete
Limit System Access to Types of Transaction Policy	DOCX	257.4 KB	Edit Download Delete
Escort and Monitor Visitors Policy	DOCX	150 KB	Edit Download Delete

Privacy Policy Library

[Upload](#)
[Create](#)
[Index](#)

Other Policy Library

[Upload](#)
[Create](#)
[Index](#)

Create New Policy

Policy Library

Policy Set

CMMC Level 1



List of CMMC (Level 1) Policies

[View Policy Format](#)

Control Physical Access Policy



Edit ecfirst Sample Policy Content?

Yes



Mandatory Policy Information

Policy Title

Control Physical Access Policy

Policy

CMMC-0001-POL

Effective Date

January 1, 2022

Last Revised

January 1, 2022

Approved by

John Smith

Version

2.0

Reference

Manage Physical Access (PE.L1-3.10.5)

Policy

Domain 101: Physical Protection (PE)

[Save](#)

Procedure Portal

Procedure Dashboard



Dashboard

[Back](#)
[Home](#) / [Procedure](#) / [Dashboard](#)

Security Procedure Library

[Upload](#)
[Create](#)
[Index](#)

Search

Show more 3

File Name	File Type	File Size	Action
Limit System Access to Types of Transaction Procedure	PDF	1.5 MB	View Download Delete
Firewall Configuration Procedure	DOCX	257.4 KB	View Download Delete
Sanitize Information System Media Procedure	DOCX	150 KB	View Download Delete

Privacy Procedure Library

[Upload](#)
[Create](#)
[Index](#)

Other Procedure Library

[Upload](#)
[Create](#)
[Index](#)

Evidence Portal



Evidence Dashboard

[Back](#)
[Home](#) / [Evidence](#) / [Evidence Dashboard](#)

HIPAA

100%

15 Files

10 GB


NIST SP 800-171

52.7%

10 Files

7 GB


CMMC L1

80%

25 Files

18 GB


CMMC L2

30%

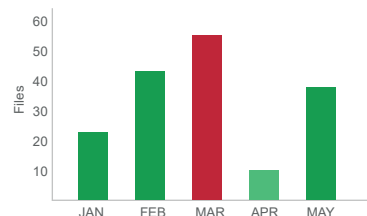
9 Files

8 GB

Favourites

Limit System Access to Types.pdf	1.5 MB
Jun 29, 2022 CMMC L1 AC.L1-3.1.1	
Firewall Configuration Evidence.docx	257.4 KB
Jun 29, 2022 NIST SP 800-171	
Sanitize Information System.docx	150 KB
May 5, 2022 CMMC L1 IA.L1-3.5.1	

Usage Stats



Recently Uploaded

- 5 Minutes ago**
 Limit System Access.pdf
 Jun 29, 2022 | CMMC L1 | AC.L1-3.1.1
- 3 Weeks ago**
 Firewall Configuration Evidence.docx
 Jun 29, 2022 | NIST SP 800-171
- 1 Month ago**
 Sanitize Information System.docx
 May 5, 2022 | CMMC L1 | IA.L1-3.5.1

Evidence Portal



HIPAA Evidence

[Back](#)
[Home](#) / [Evidence](#) / [HIPAA Dashboard](#) / [HIPAA Evidence](#)

#	HIPAA Standards & Implementation Specifications	Evidence List	Document Description	Evidence Description	Evidence Date
Security					
Administrative Safeguards					
1	§ 164.308(a)(1)(i) Security Management Process STD	Network Diagrams			<input type="checkbox"/> Evidence less than 90 days old <input type="checkbox"/> Evidence grater than 90 days old
2	§ 164.308(a)(1)(ii)(A) Risk Analysis (R) SPEC	Copies of previous assessment			
Organizational Safeguards					
1	§ 164.314(a)(1) Business Associate Contracts or Other Arrangements STD	List of BAA and other contracts			
2	§ 164.308(a)(1)(ii)(A) Risk Analysis (R) SPEC	Copies of previous assessment			



CMMC LI

[Back](#)
[Home](#) / [Evidence](#) / [Evidence Dashboard](#) / [CMMC LI](#)

#	Practice ID	Sample Evidences	Evidence Artifact	Evidence Description	Evidence Date
DOMAIN 1: Access Control (AC)					
1	AC.L1-3.1.1 Authorized Access control	▪ SSP	<input type="button" value="Choose File"/> <input type="button" value="Upload"/>	<input type="text" value="Please describe the evidence"/>	<input type="text" value=""/>
		▪ System design documentation	<input type="button" value="Choose File"/> <input type="button" value="Upload"/>	<input type="text" value="Please describe the evidence description..."/>	<input type="text" value=""/>
2	AC.L1-3.1.2 Transaction & Function Control	▪ Restricts access only to specific transactions and functions, SSP	<input type="button" value="Choose File"/> <input type="button" value="Upload"/>	<input type="text" value="Please describe the evidence description..."/>	<input type="text" value=""/>
DOMAIN 5: Identification & Authentication (IA)					
3	IA.L1-3.5.1 Identification	▪ Identify information system users, SSP	<input type="button" value="Choose File"/> <input type="button" value="Upload"/>	<input type="text" value="Please describe the evidence description..."/>	<input type="text" value=""/>

Cybermapper

Search...



Cybermapper View

Back

[Home](#) / Cybermapper View

What would you like to see the mapping table for?

HIPAA

ISO 27001:2013

Show



HIPAA to ISO 27001:2013

HIPAA Implementation Specification

ISO 27001:2013 Annex A. Control Objectives

164.308(a)(1)(i) Security Management Process

164.308(a)(1)(i) Security Management Process STD

A.6.1.5 Information Security in Project Management

164.308(a)(1)(ii)(A) Risk Analysis (R) SPEC

A.14.1.1 Information security requirements analysis and specification

A.18.2.1 Independent review of information security

Executive Dashboard

Executive Dashboard

Reports

Title	Updated on	View
RA Report	-	View
CA Report	-	N/A
RA CAP	-	N/A

Policy Status

Title	View
Privacy Policy	N/A
Security Policy	N/A

Quick Links

- [Remediation Portal](#)
- [Cybersecurity Readiness Assessment](#)
- [Cyber Mapper](#)

Risk Assessment Status

Title	Updated on	Status	View
DCF	-		
DCAF	-		
Compliance	-	N/A	

Cybersecurity Assessment Status

Title	Updated on	Status	View
DCF	-		
Compliance Status	-	N/A	

Business Associates

Title	View

Kris Laidley

Kris.Laidley@ecfirst.com

www.ecfirst.com

Reimagining Cyber Defense