GRC: Compliance Audit for Skyler Inc.

Robert Russell

Overview

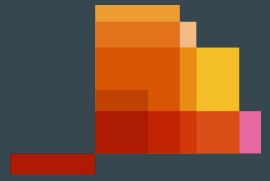
Cybersecurity Compliance Audit

- GRC: Frameworks
  - NIST CSF V1.1 (2.0?)
    - Policy vs Control
      - Risk Appetite
        - Gapps Platform Tool
          - Demonstration
            - Summary

Goal

Perform an IT compliance audit on a simulated tech company using the web-platform Gapps

What is a Cybersecurity Compliance Audit?



pwc

Deloitte.

The Fun Police

CyberSecurity Auditors come from Third-Party companies to check for regulatory compliance to a framework

EY

Governance, Risk, and Compliance Frameworks

International Organization for Standardization
ISO
27001

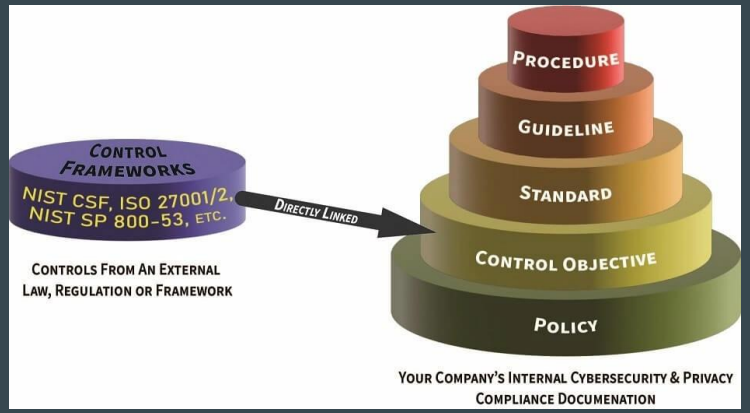
SOC 2
TYPE 2
AICPA
SOC

PCI
DSS
COMPLIANT

NERC
NORTH AMERICAN ELECTRIC RELIABILITY CORPORATION
CRITICAL INFRASTRUCTURE PROTECTION

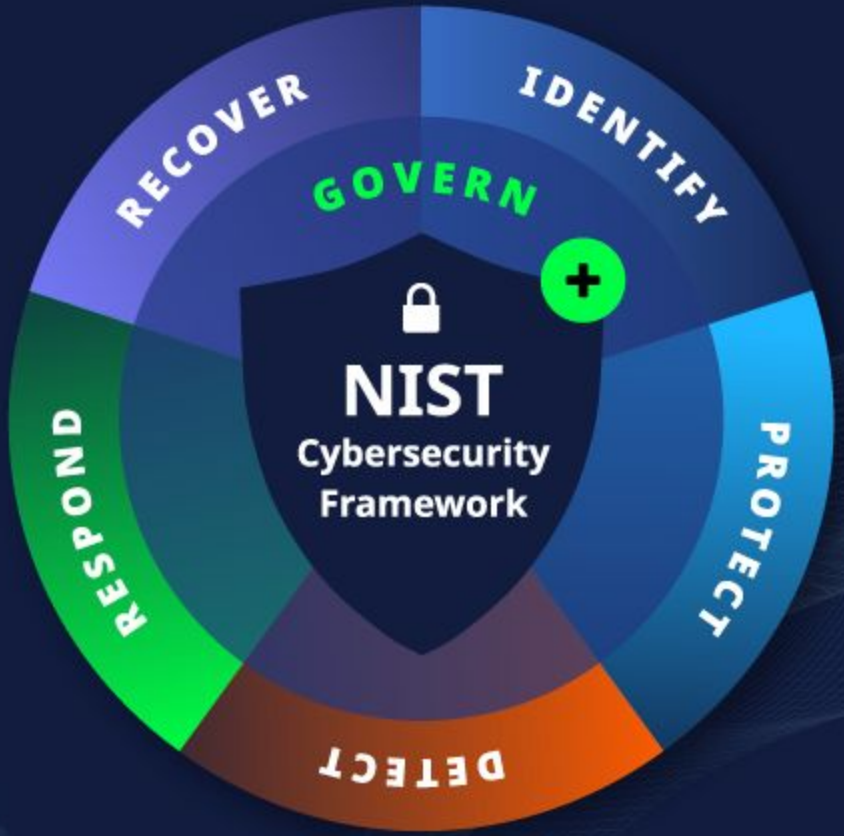
CIS Center for Internet Security
CIS Controls®

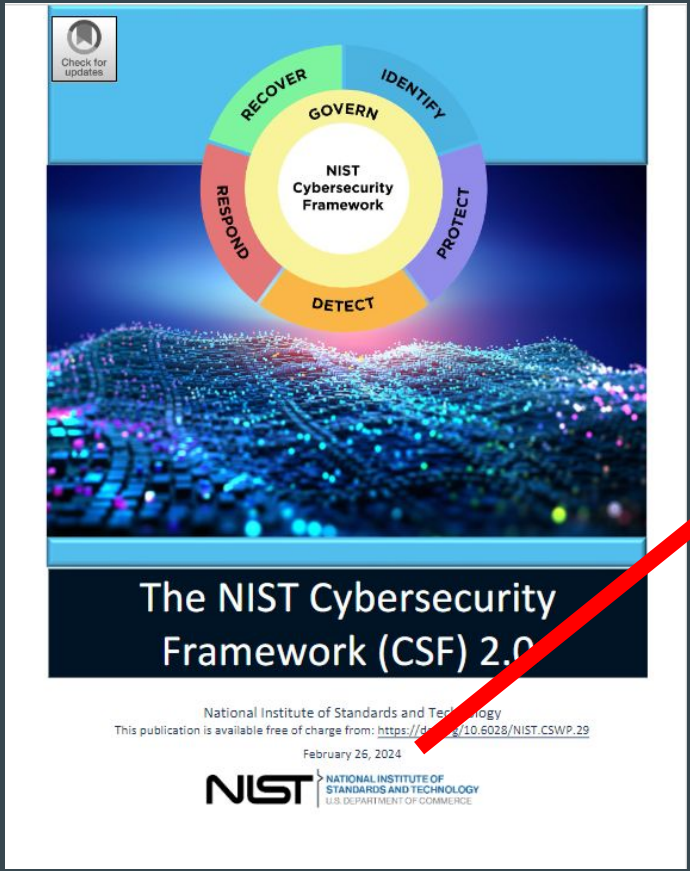
Governance, Risk, and Compliance Frameworks



The Cover

Frameworks drive policy implementation by outlining the guide to meet the company's goals

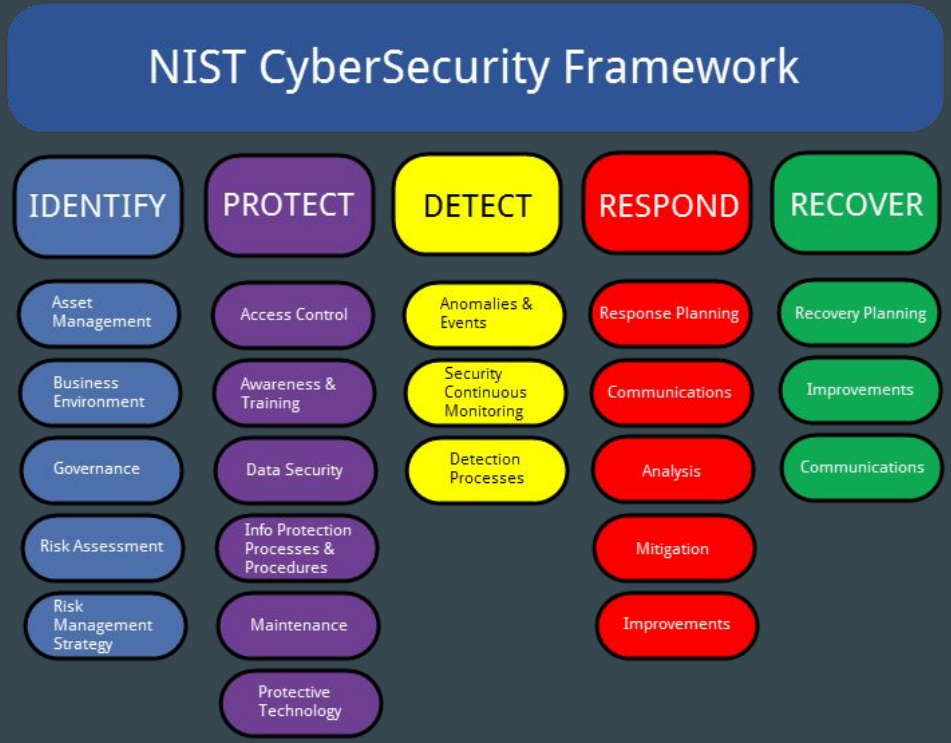

RECOVER
IDENTIFY
GOVERN
NIST
Cybersecurity
Framework
RESPOND
PROTECT
DETECT

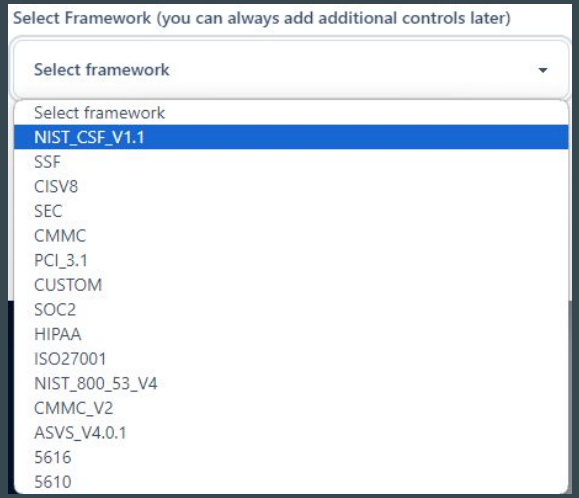

Check for updates
RECOVER
IDENTIFY
GOVERN
NIST Cybersecurity Framework
RESPOND
PROTECT
DETECT
The NIST Cybersecurity Framework (CSF) 2.0
National Institute of Standards and Technology
This publication is available free of charge from: https://doi.org/10.6028/NIST.CSWP.29
February 26, 2024
NIST
NATIONAL INSTITUTE OF STANDARDS AND TECHNOLOGY
U.S. DEPARTMENT OF COMMERCE


National Institute of Standards and Technology
This publication is available free of charge from: https://doi.org/10.6028/NIST.CSWP.29
February 26, 2024
NIST
NATIONAL INSTITUTE OF STANDARDS AND TECHNOLOGY
U.S. DEPARTMENT OF COMMERCE

NIST CSF 2.0

NIST CSF V1.1 ca. 2018





23 Controls

100+ Subcontrols

REF CODE	CONTROL NAME	#SUB CONTROLS
RS.AN	Analysis	5
DE.AE	Anomalies & Events	5
ID.AM	Asset Management	6
PR.AT	Awareness & Training	5
ID.BE	Business Environment	5
RC.CO	Communications	3
RS.CO	Communications	5
PR.DS	Data Security	8
DE.DP	Detection Process	5
ID.GV	Governance	4
PR.AC	IAM	7

REF CODE	CONTROL NAME	#SUB CONTROLS
RC.IM	Improvements	2
RS.IM	Improvements	2
PR.IP	IPPP	12
PR.MA	Maintenance	2
RS.MI	Mitigation	3
PR.PT	Protective Technology	5
RC.RP	Recovery Planning	1
RS.RP	Response Planning	1
ID.RA	Risk Assessment	6
ID.RM	Risk Management Strategy	3
DE.CM	Security Continuous Monitoring	8
ID.SC	Supply Chain Risk Management	8

Policy vs Control

Policy

General statement from executive leadership to guide action and decisions for a desired outcome.

"We are willing to have a high risk appetite. Modify assessment thresholds and controls accordingly."

Control

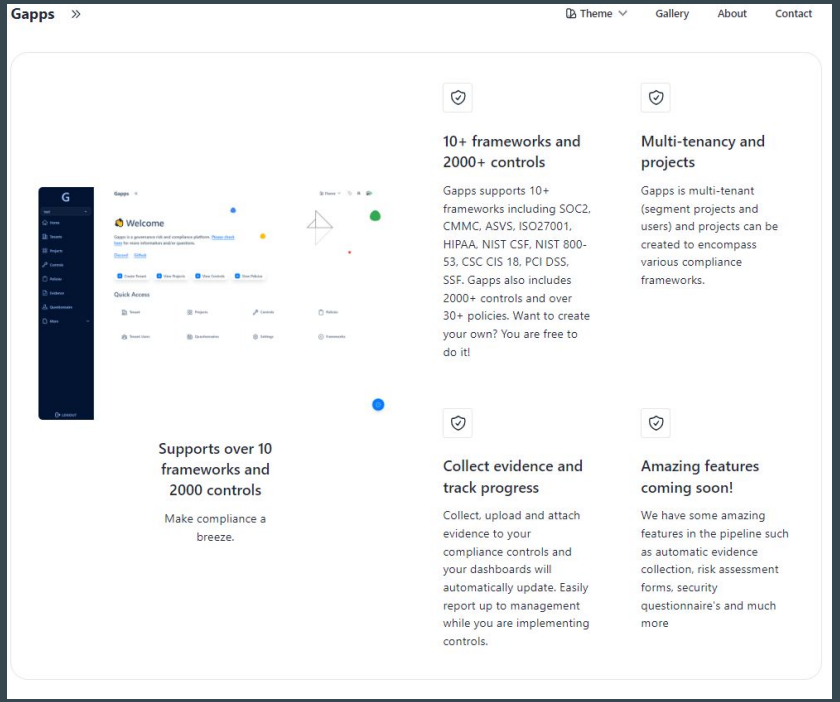
Technical/administrative/physical safeguards to mitigate the exploitation of a vulnerability.

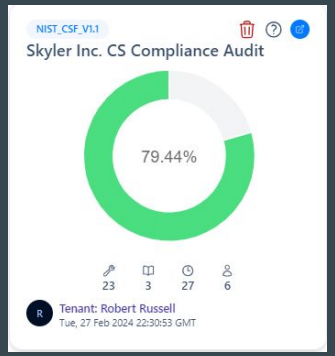
"Risk of doing this is high, but move forward as is. Leadership says they're willing to accept the risk."

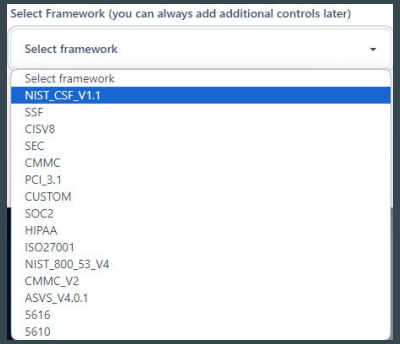
Gapps

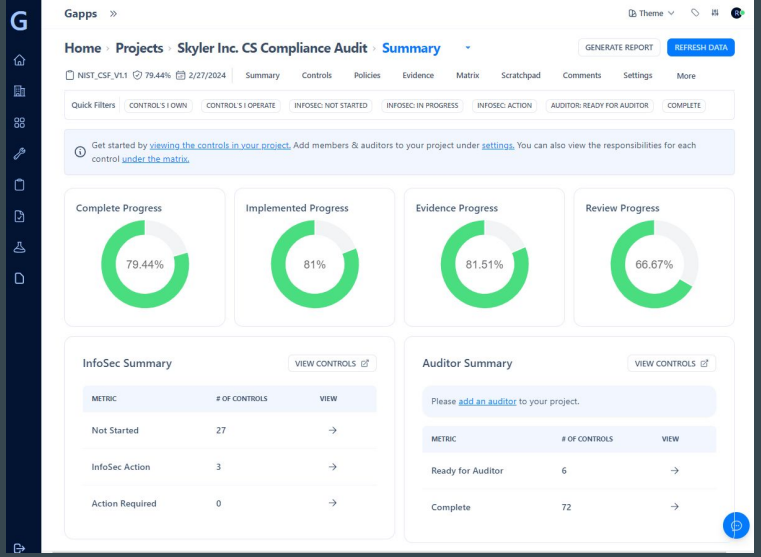
Tool

Free open-source GRC compliance web application



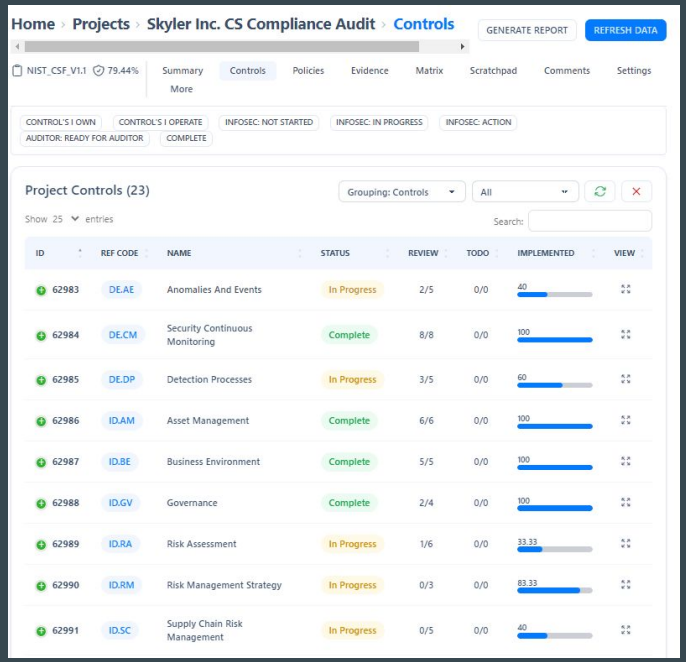


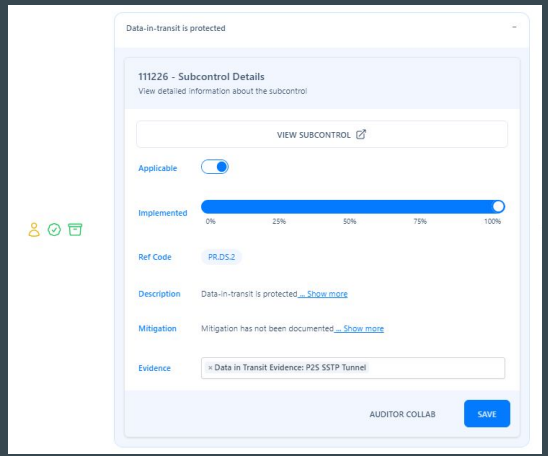




Dashboard

Controls complete and in progress





PR.DS.2 implemented and approved

Demonstration

Summary

GRC Frameworks
- ➢ The Cover to the Book

NIST CSF
- ➢ An Industry-leading framework

Policies
- ➢ High-level statements to direct subsidiary decisions

Controls
- ➢ A Measure that modifies risk

Risk Appetite
- ➢ The Level of risk a companies willing to accept to reach their goals

Gapps
- ➢ Free open-source GRC compliance platform

THANK YOU!

Sources

Gapps: https://gapps.darkbanner.com/

Gapps Repository: https://github.com/bmarsh9/gapps

NIST CSF V2.0: https://doi.org/10.6028/NIST.CSWP.29

Azure NIST CSF CRM: https://servicetrust.microsoft.com/ViewPage/BlueprintLegacy?command=Download&downloadType=Document&downloadId=89ec5635-be07-4a5d-87d3-51783e4d3002

Azure and NIST CSF: https://learn.microsoft.com/en-us/azure/compliance/offerings/offering-nist-csf

CS Compliance: https://www.upguard.com/blog/difference-between-compliance-and-auditing-in-information-security

Framework in GRC: https://aws.amazon.com/what-is/grc/#:~:text=A%20GRC%20framework%20is%20a,the%20company%20toward%20its%20goals

Policy vs Control: https://complianceforge.com/grc/policy-vs-standard-vs-control-vs-procedure

Guide to Getting Starting with a CS Risk Assessment: https://www.cisa.gov/sites/default/files/video/22_1201_safecom_guide_to_cybersecurity_risk_assessment_508-r1.pdf