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?

The Regulators

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

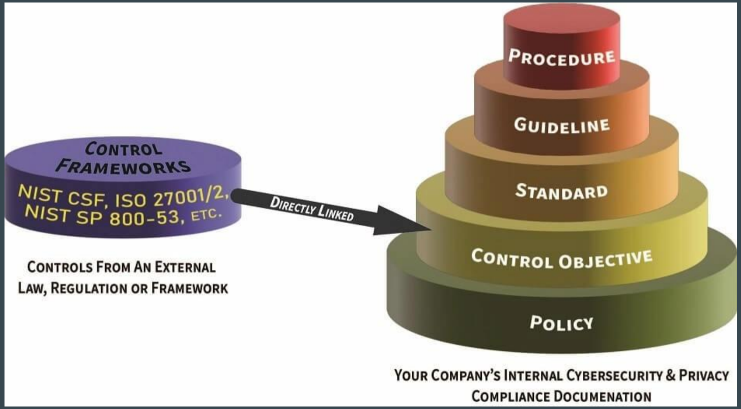
pwc

Deloitte.

EY

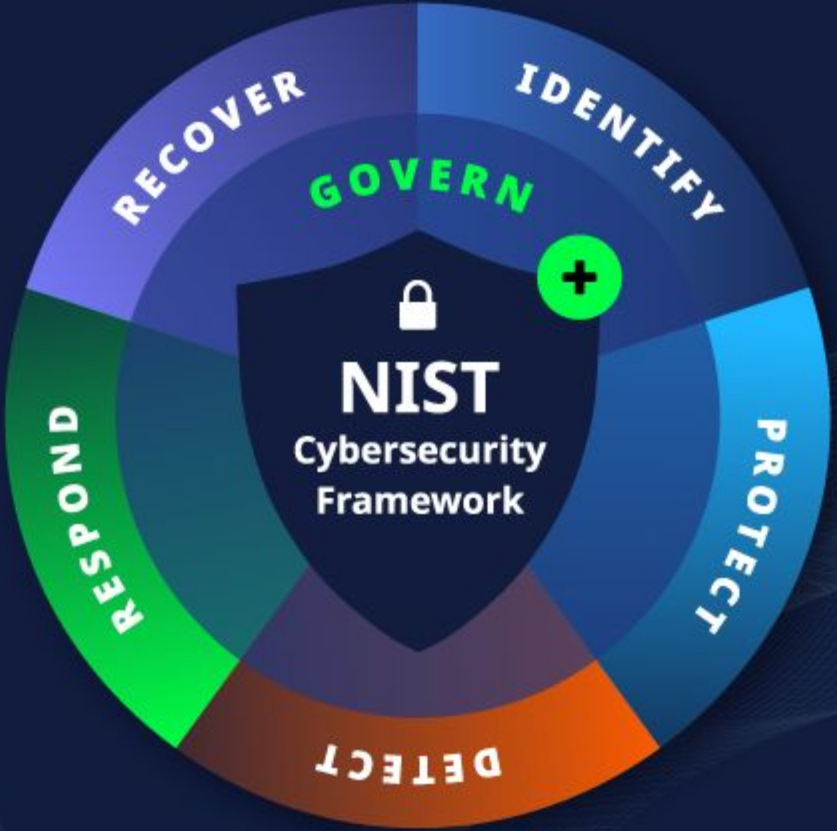
Governance, Risk, and Compliance Frameworks

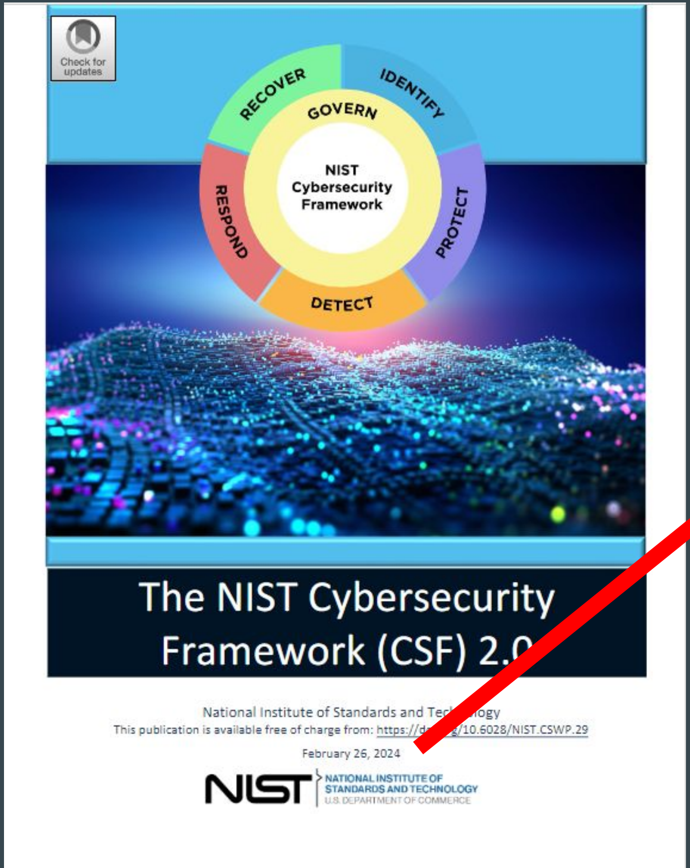
Governance, Risk, and Compliance Frameworks


Control Frameworks
NIST CSF, ISO 27001/2, NIST SP 800-53, etc.
Directly Linked
Controls From An External Law, Regulation or Framework
Procedure
Guideline
Standard
Control Objective
Policy
Your Company's Internal Cybersecurity & Privacy Compliance Documenation

The Cover

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


NIST
Cybersecurity
Framework
GOVERN
IDENTIFY
PROTECT
DETECT
RESPOND
RECOVER
+

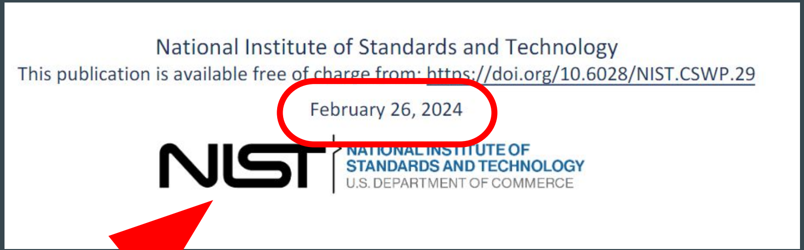


The NIST Cybersecurity Framework (CSF) 2.0

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



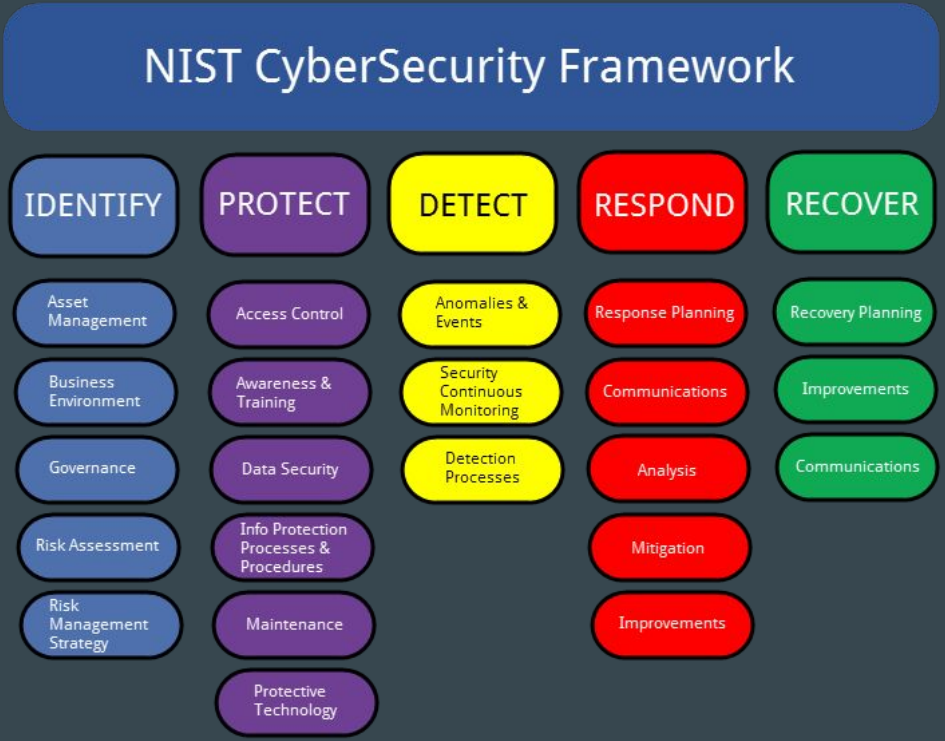
National Institute of Standards and Technology
This publication is available free of charge from: https://doi.org/10.6028/NIST.CSWP.29

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



NIST CyberSecurity Framework

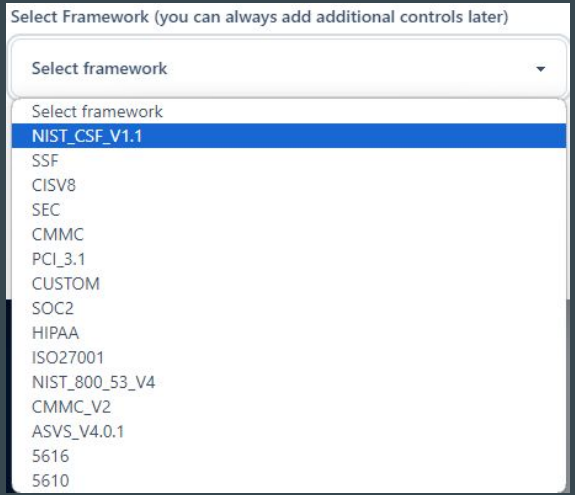
IDENTIFY
Asset Management
Business Environment
Governance
Risk Assessment
Risk Management Strategy

PROTECT
Access Control
Awareness & Training
Data Security
Info Protection Processes & Procedures
Maintenance
Protective Technology

DETECT
Anomalies & Events
Security Continuous Monitoring
Detection Processes

RESPOND
Response Planning
Communications
Analysis
Mitigation
Improvements

RECOVER
Recovery Planning
Improvements
Communications



Select Framework (you can always add additional controls later)

Select framework

Select framework
NIST_CSF_V1.1
SSF
CISV8
SEC
CMMC
PCI_3.1
CUSTOM
SOC2
HIPAA
ISO27001
NIST_800_53_V4
CMMC_V2
ASVS_V4.0.1
5616
5610

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

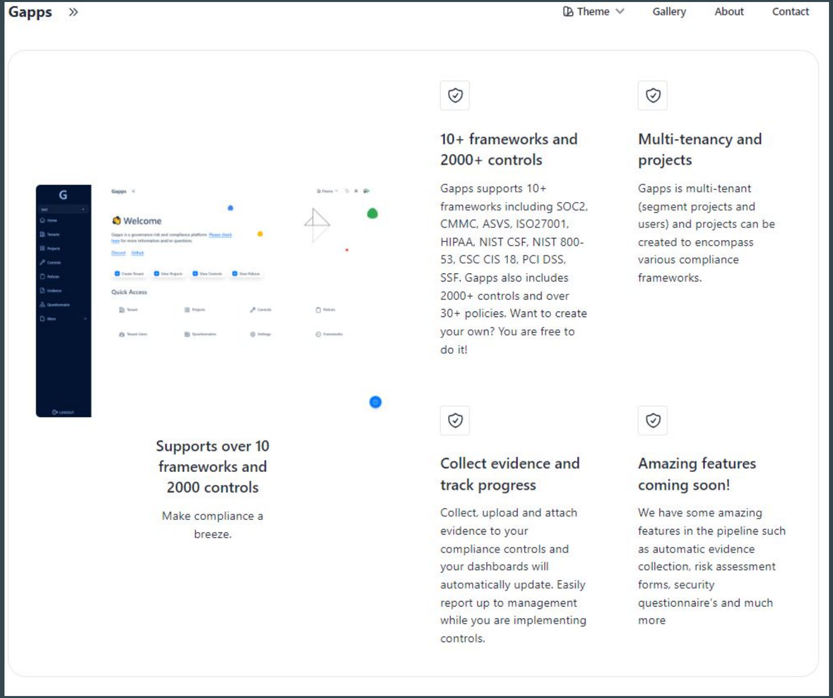
Technical/administrative/physical safeguards to mitigate the exploitation of a vulnerability.

“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



Supports over 10 frameworks and 2000 controls

Make compliance a breeze.

10+ frameworks and 2000+ controls

Gapps supports 10+ frameworks including SOC2, CMMC, ASVS, ISO27001, HIPAA, NIST CSF, NIST 800-53, CSC CIS 18, PCI DSS, SSF. Gapps also includes 2000+ controls and over 30+ policies. Want to create your own? You are free to do it!

Multi-tenancy and projects

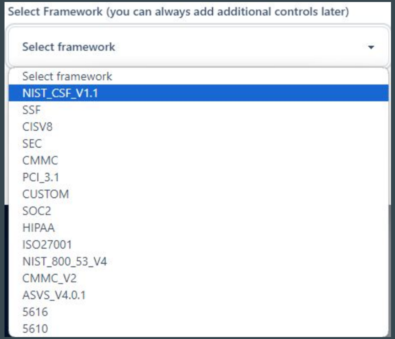
Gapps is multi-tenant (segment projects and users) and projects can be created to encompass various compliance frameworks.

Collect evidence and track progress

Collect, upload and attach evidence to your compliance controls and your dashboards will automatically update. Easily report up to management while you are implementing controls.

Amazing features coming soon!

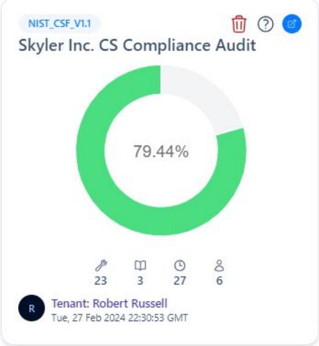
We have some amazing features in the pipeline such as automatic evidence collection, risk assessment forms, security questionnaire's and much more



Select Framework (you can always add additional controls later)

Select framework

- Select framework
- NIST_CSF_V1.1
- SSF
- CISV8
- SEC
- CMMC
- PCI_3.1
- CUSTOM
- SOC2
- HIPAA
- ISO27001
- NIST_800_53_V4
- CMMC_V2
- ASVS_V4.0.1
- 5616
- 5610



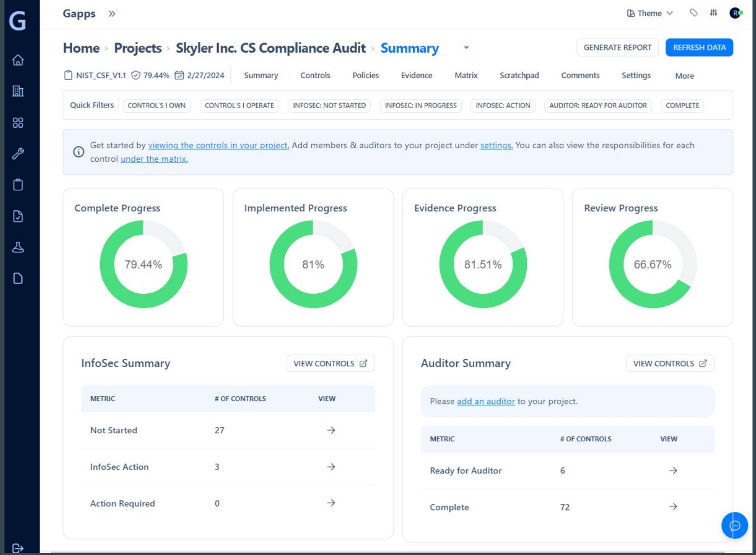
NIST_CSF_V1.1

Skyler Inc. CS Compliance Audit

79.44%

23 3 27 6

Tenant: Robert Russell
Tue, 27 Feb 2024 22:30:53 GMT



Gapps

Home › Projects › Skyler Inc. CS Compliance Audit › Summary

GENERATE REPORT | REFRESH DATA

NIST_CSF_V1.1 79.44% 2/27/2024 | Summary | Controls | Policies | Evidence | Matrix | Scratchpad | Comments | Settings | More

Quick Filters: CONTROL'S I OWN | CONTROL'S I OPERATE | INFOSEC: NOT STARTED | INFOSEC: IN PROGRESS | INFOSEC: ACTION | AUDITOR: READY FOR AUDITOR | COMPLETE

Get started by viewing the controls in your project. Add members & auditors to your project under settings. You can also view the responsibilities for each control under the matrix.

Complete Progress	Implemented Progress	Evidence Progress	Review Progress
79.44%	81%	81.51%	66.67%

InfoSec Summary — VIEW CONTROLS

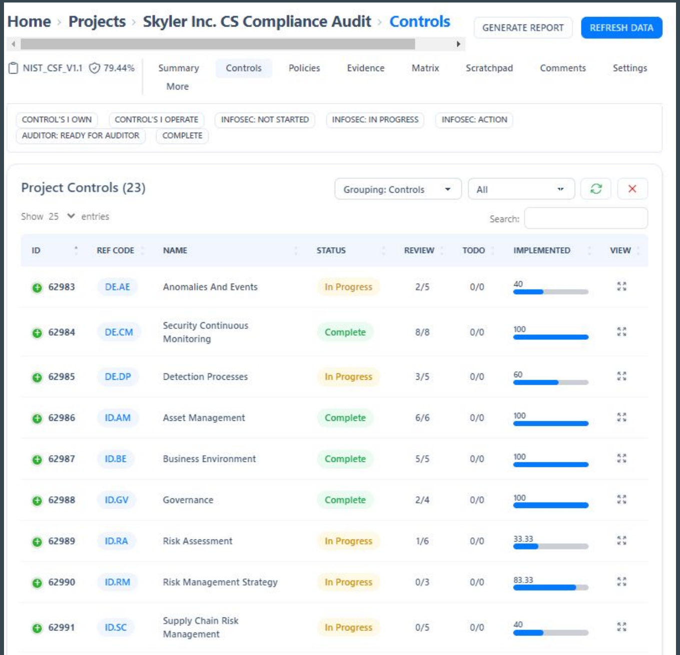
METRIC	# OF CONTROLS	VIEW
Not Started	27	→
InfoSec Action	3	→
Action Required	0	→

Auditor Summary — VIEW CONTROLS

Please add an auditor to your project.

METRIC	# OF CONTROLS	VIEW
Ready for Auditor	6	→
Complete	72	→

Dashboard



Home › Projects › Skyler Inc. CS Compliance Audit › Controls

GENERATE REPORT | REFRESH DATA

NIST_CSF_V1.1 79.44% | Summary | Controls | Policies | Evidence | Matrix | Scratchpad | Comments | Settings | More

CONTROL'S I OWN | CONTROL'S I OPERATE | INFOSEC: NOT STARTED | INFOSEC: IN PROGRESS | INFOSEC: ACTION | AUDITOR: READY FOR AUDITOR | COMPLETE

Project Controls (23)

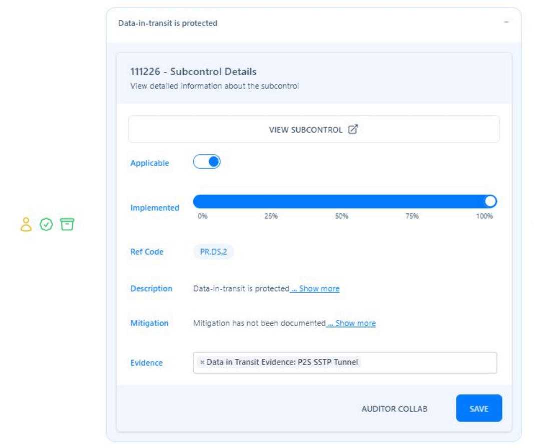
Grouping: Controls | All

Show 25 entries

Search:

ID	REF CODE	NAME	STATUS	REVIEW	TODO	IMPLEMENTED	VIEW
62983	DE.AE	Anomalies And Events	In Progress	2/5	0/0	40	
62984	DE.CM	Security Continuous Monitoring	Complete	8/8	0/0	100	
62985	DE.DP	Detection Processes	In Progress	3/5	0/0	60	
62986	ID.AM	Asset Management	Complete	6/6	0/0	100	
62987	ID.BE	Business Environment	Complete	5/5	0/0	100	
62988	ID.GV	Governance	Complete	2/4	0/0	100	
62989	ID.RA	Risk Assessment	In Progress	1/6	0/0	33.33	
62990	ID.RM	Risk Management Strategy	In Progress	0/3	0/0	83.33	
62991	ID.SC	Supply Chain Risk Management	In Progress	0/5	0/0	40	

Controls complete and in progress



Data-in-transit is protected

111226 - Subcontrol Details

View detailed information about the subcontrol

VIEW SUBCONTROL

Applicable: on

Implemented: 0% 25% 50% 75% 100%

Ref Code: PR.DS.2

Description: Data-in-transit is protected ... Show more

Mitigation: Mitigation has not been documented ... Show more

Evidence: × Data in Transit Evidence: P2S SSTP Tunnel

AUDITOR COLLAB | SAVE

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