Overview

In the world of cyber security, organizations often struggle to keep pace with an ever-changing threat environment. CySAFE was created through a collaborative effort, driven by five Michigan counties and the State of Michigan to develop a free IT security assessment tool to help small and mid-sized organizations assess, understand and prioritize their **basic** IT security needs.

CySAFE was created from three well-known IT security frameworks: 20 Critical Controls, ISO 27001 and NIST. The goal was to combine the **400+** controls from all three frameworks into one condensed list, removing any redundant controls and assess the controls against the organization's current IT security capabilities. Next, the master list of 35 controls were evaluated over three key factors – cost to implement, time to implement and risk – and were assigned a number based on each key factor.

Changes in CySAFE 2.0

There were three major changes to CySAFE 2.0: 1) Creation of CySAFE Handbook 2) Addition of "Summary of Controls" 3) CySAFE was updated to reflect the changes made to the three frameworks (20 Critical Controls, ISO 27001 and NIST) along with feedback received by the organizations using the CySAFE framework for the past three years. Six controls were deleted and five controls were added. The five new controls are

- *Email and Web Browser Protections*
- *Penetration Tests and Red Team Exercises*
- *Physical And Environmental Security*
- *Monitoring and Review of Third Party Services*
- *Compliance*

For more information on the changes, see Appendix A.

How to Use CySAFE

Step 1: Understand the Source Frameworks

CySAFE was built upon current industry IT security standards: 20 Critical Controls, ISO 27001 and NIST. For a description of the 35 controls from each framework used with CySAFE, review the worksheets labelled 20 CC, ISO and NIST. This will provide you with an understanding of the recommended IT security controls, descriptions and approaches. For more detailed background information on the security standards documents, refer to the links found in the Appendix B worksheet.

Step 2: Become Familiar With the Tool

CySAFE was built in a Microsoft Excel workbook with nine worksheets. Each worksheet plays a different role in evaluating and understanding IT security readiness.

The following worksheets are included:

Instructions: Provides a general overview on how to use CySAFE

- Assessment: The assessment consists of a master list of 35 controls, across three key factors (cost, time and risk) and a rating scale of 0-5

- Assessment Results: Provides a color-coded list of each security control ordered by highest to lowest priority with the rating and CySAFE score, indicating organization's most important IT security initiatives

- Control Category & Summary: Controls are grouped into five categories and summarized in a chart and graphs to help improve IT security posture and track progress over time

- 20 CC: Provides a list of 20 selected controls including: control descriptions, examples of controls in place and the basic security level recommended

- ISO: Provides a list of 11 selected controls including: control descriptions, examples of controls in place and the basic security level recommended

- NIST: Provides a list of 4 selected controls including: control descriptions, examples of controls in place and the basic security level recommended

- **Appendix A:** Provides details regarding the differences between CySAFE Version 1 and 2

- Appendix B: Provides links to the standards documents, reference documents and CySAFE contributors

Step 3: Conduct an Assessment

To begin the assessment, review the rating scale below and become familiar with the description for each number. The Assessment Rating Scale is adapt ed from the Carnegie Mellon University's Capability Maturity Model Integration (CMMI), a process improvement training and appraisal program.

Next, select the **Assessment** worksheet and enter a rating from 0-5 in **Column I** for each security control. To further understand each control, click or hover over the Control Name to see more detailed information. Lastly, it is important to conduct an accurate assessment of your organization's IT security controls to produce the most meaningful benefits from this tool.

You will need to Enable Macros before you enter your rating or the assessment will not work properly. Depending on which version of Excel is installed, the steps to do so may vary. In most cases, there will be a yellow bar appearing below the Ribbon interface with an option to "Enable Content". This must be clicked for the CySAFE assessment to function properly.

Assessment Rating Scale:

0 - Non-Existent Management Processes are not in place

Complete lack of any recognizable processes. The organization has not recognized that there is an issue to be addressed.

1 - Initial Processes are ad hoc and disorganized

There is evidence that the organization has recognized that the issues exist and need to be addressed. However, there are no standardized processes. There are ad hoc approaches that tend to be applied on an individual or case-by-case basis. The overall approach to management is disorganized.

2 - Repeatable Processes follow a regular pattern

Processes have developed to a stage where different people undertaking the same task follow similar procedures. There is no formal training or communication of standard procedures and responsibility is left to the individual. There is a high degree of reliance on the knowledge of individuals

and errors are likely as a result.

3 - Defined Processes are documented and communicated

Procedures have been standardized and documented and communicated through formal training. However, compliance with the procedures is left to each individual and it is unlikely that deviations will be detected. The procedures themselves are not sophisticated, but are the formalization of existing practices.

4 - Managed Processes are monitored and measured

It is possible to monitor and measure compliance with procedures and to take action where processes appear not to be working effectively. Processes are under constant improvement and provide good practice. Automation and tools are used in a limited or fragmented way.

5 - Optimized Best Practices are followed and automated

Processes have been refined to a level of best practice, based on the results of continuous improvement and benchmarking with other organizations and industry best practices. It is used in an integrated way to automate the workflow, providing tools to improve quality and effectiveness, making the enterprise quick to adapt.

Step 4: Review Your Assessment Results

Once the assessment is completed, select the **Assessment Results** worksheet and review the results. The worksheet will list 35 controls with the rating and CySAFE Score sorted from highest to lowest priority and will be also be color coded to depict your organizations's most important IT security initiatives. Controls highlighted in red indicate the highest priority for IT security initiatives. Controls highlighted in orange indicate the next highest priority for IT security initiative, with those highlighted in yellow being the next highest priority.

Step 5: Implement New Controls/Enhance Security Capability

The NEW CySAFE Handbook can be used as a reference to improve each of the 35 controls. Refer to the 20 Critical Controls, ISO 27001 and NIST documentation for information on how to mitigate the risks, enhance or implement the security controls. These documents will provide the much needed detail and foundational information for you to move your security program forward. CySAFE is only a guide that helps you assess your IT security needs, determine your organization's priorities and provide you additional information.

Step 6: Reevaluate on a Periodic Basis

A reassessment with CySAFE should be done quarterly or at the very least, annually or when your organization implements any new IT products or processes. We have added quarterly graphing capabilities in the **Control Category and Summary** worksheet to help you track your progress.

Disclaimer: Cyber Security Assessment for Everyone (CySAFE) is a tool for evaluating security measures. It was developed by and for local government entities and is intended to provide guidance on cybersecurity. It is a public document and may be used for guidance by the general public. However, it is not intended to be relied upon or used as a comprehensive means to protect against potential security risks or threats. A review of additional security standards such as NIST Cyber Security Framework, ISO 27001 and CIS 20 Critical Controls is strongly recommended as well as a thorough review of a government's , company's or individual's unique security requirements.

CySAFE was drafted by individuals from several governmental entities in Michigan. It is not an official government standard or regulation. No governmental entity that participated in drafting CySAFE may be held liable for any errors or omissions in CySAFE or held liable for any damages that may result from relying on the information it contains. CySAFE is offered AS IS without warranties of any type.

Assessment

Framework	Control Name	Cost	Time	Risk	Total	Rating	CySAFE Score
20 CC	Critical Control 1: Inventory of Authorized and Unauthorized Devices	3	3	2	8	0	89
20 CC	Critical Control 2: Inventory of Authorized and Unauthorized Software	3	2	3	8	0	89
20 CC	Critical Control 3: Secure Configurations for Hardware and Software on Mobile Devices, Laptops, Workstations, and Servers	3	2	3	8	0	89
20 CC	Critical Control 4: Continuous Vulnerability Assessment and Remediation	3	1	3	7	0	78
20 CC	Critical Control 5: Controlled Use of Administrative Privileges	3	3	3	9	0	100
20 CC	Critical Control 6: Maintenance, Monitoring, and Analysis of Audit Logs	3	3	1	7	0	78
20 CC	Critical Control 7: Email and Web Browser Protections	3	3	2	8	0	89
20 CC	Critical Control 8: Malware Defenses	3	3	3	9	0	100
20 CC	Critical Control 9: Limitation and Control of Network Ports, Protocols, and Services	3	1	2	6	0	67
20 CC	Critical Control 10: Data Recovery Capability	2	2	3	7	0	78
20 CC	Critical Control 11: Secure Configurations for Network Devices such as Firewalls, Routers, and Switches	3	2	3	8	0	89
20 CC	Critical Control 12: Boundary Defense	3	2	3	8	0	89
20 CC	Critical Control 13: Data Protection	2	2	2	6	0	67
20 CC	Critical Control 14: Controlled Access Based on the Need to Know	3	1	3	7	0	78
20 CC	Critical Control 15: Wireless Access Control	3	3	2	8	0	89
20 CC	Critical Control 16: Account Monitoring and Control	3	2	2	7	0	78
20 CC	Critical Control 17: Security Skills Assessment and Appropriate Training to Fill Gaps	3	2	3	8	0	89
20 CC	Critical Control 18: Application Software Security	1	2	2	5	0	56
20 CC	Critical Control 19: Incident Response and Management	3	2	3	8	0	89
20 CC	Critical Control 20: Penetration Tests and Red Team Exercises	2	1	2	5	0	56

Framework	Control Name	Cost	Time	Risk	Total	Rating	CySAFE Score
ISO	ISO - Define Scope	3	3	3	9	0	100
ISO	ISO - Setup the Information Security Team and Approach	3	2	3	8	0	89
ISO	ISO - Communicate Information Security Policy	3	1	2	6	0	67
ISO	ISO - Identify Resources, Ownership and Standard Operating Procedures for IT Processes	3	1	2	6	0	67
ISO	ISO - Monitoring and Review of Third Party Services	3	3	3	9	0	100
ISO	ISO - Complete Summary of Controls	3	3	3	9	0	100
ISO	ISO - Define and Generate Records (evidence)	3	1	1	5	0	56
ISO	ISO - Physical And Environmental Security	2	2	3	7	0	78
ISO	ISO - Measure Effectiveness of Controls	3	1	3	7	0	78
ISO	ISO - Update Annual Planning	3	2	3	8	0	89
ISO	ISO - Compliance	2	2	3	7	0	78

Framework	Control Name	Cost	Time	Risk	Total	Rating	CySAFE Score
NIST	NIST - Business Environment	3	2	3	8	0	89
NIST	NIST - Governance	3	1	2	6	0	67
NIST	NIST - Risk Management Strategy	3	1	2	6	0	67
NIST	NIST - Maintenance	2	2	3	7	0	78

Assessment Rating Scale Legend

0 - Non-Existent Management processes are not in place (Complete lack of any recognizable processes. The organization has not recognized that there is an issue to be addressed).

1 - Initial Processes are ad hoc and disorganized (There is evidence that the organization has recognized that the issues exist and need to be addressed. However, there are no standardized processes; there are ad hoc approaches that tend to be applied on an individual or case-by-case basis. The overall approach to management is disorganized).

2 - Repeatable Processes follow a regular pattern (Processes have developed to a stage where different people undertaking the same task follow similar procedures. There is no formal training or communication of standard procedures and responsibility is left to the individual. There is a high degree of reliance on the knowledge of individuals and errors are likely as a result).

3 - Defined Processes are documented and communicated (Procedures have been standardized and documented and communicated through formal training. However, compliance with the procedures is left to each individual and it is unlikely that deviations will be detected. The procedures themselves are not sophisticated, but are the formalization of existing practices).

4 - Managed Processes are monitored and measured (It is possible to monitor and measure compliance with procedures and to take action where processes appear not to be working effectively. Processes are under constant improvement and provide good practice. Automation and tools are used in a limited or fragmented way).

5 - Optimized Best practices are followed and automated (Processes have been refined to a level of best practice, based on the results of continuous improvement and benchmarking with other organizations and industry best practices. IT is used in an integrated way to automate the workflow, providing tools to improve quality and effectiveness, making the enterprise quick to adapt).

CySAFE Score Calculation

CySAFE takes a weighted approach for the purposes of scoring each control. When a Control is assessed at a lower Rating, it is treated with a higher weight. For example, a Rating of 0 (Non-Existent) is considered a higher priority than a Rating of 5 (Optimized) according to the Capability Maturity Model Integration (CMMI) model. The conversions are listed below:

Weighted Rating Conversion
Rating 0 = 100
Rating 1 = 85
Rating 2 = 70
Rating 3 = 50
Rating 4 = 25
Rating 5 = 10

CySAFE Score Calculation
CySAFE Score = ((Weighted Rating * Total)/10)*(10/9)
(Possible score out of 100)

Example: Critical Control 1 with a Rating of 2
Step 1: A Rating of 2 is weighted to 70; CC1 has a Total of 8
Step 2: Plug numbers into formula and solve

CySAFE Score = ((70 * 8)/10) * (10/9)
CySAFE Score = (560/10) * (10/9)
CySAFE Score = (56) * (10/9)
CySAFE Score = 62.222...

Step 3: Round the score to the nearest whole number
CySAFE Score = 62.222... ≈ 62
CySAFE Score = 62

Legend

The values assigned to **Cost (Column E)**, **Time (Column F)** and **Risk (Column G)** for all controls were determined through a collaborative effort between five Michigan Counties and the State of Michigan based on 2014 implementation trends.

Cost (Column E)	Time (Column F)	Risk (Column G)	Total (Column H)
3 0 < $25K	3 < 60 days	3 High	Cost + Time + Risk
2 $25K - $75K	2 61-120 days	2 Med	
1 > $75K	1 > 121 days	1 Low	

CySAFE
CYBER SECURITY ASSESSMENT FOR EVERYONE
VERSION 2.0

Assessment Results

Framework	Control Name	Rating	CySAFE Score	Control Description	Current Controls in Place	Exceptions	Planned Work
20 CC	Critical Control 5: Controlled Use of Administrative Privileges	0	**100**	The processes and tools used to track/control/prevent/correct the use, assignment, and configuration of administrative privileges on computers, networks, and applications.			
20 CC	Critical Control 8: Malware Defenses	0	**100**	Control the installation, spread, and execution of malicious code at multiple points in the enterprise, while optimizing the use of automation to enable rapid updating of defense, data gathering, and corrective action.			
ISO	ISO - Define Scope	0	**100**	The organization has defined the scope of the Information Security Management System (ISMS), taking into account the characteristics of the business, its location and technology.			
ISO	ISO - Monitoring and Review of Third Party Services	0	**100**	The services, reports and records provided by the third party are monitored, reviewed, and audits carried out regularly.			
ISO	ISO - Complete Summary of Controls	0	**100**	The Organization has a "Summary of Controls" document that includes: a) the control(s) selected and reasons for their selection (control objectives); b) the reason for the exclusion of controls; c) the controls currently implemented; d the status and due date for the controls that still need to be implemented; and e) reference to the Information Security Risk Analysis, directives and procedures.			
20 CC	Critical Control 1: Inventory of Authorized and Unauthorized Devices	0	**89**	Actively manage (inventory, track, and correct) all hardware devices on the network so that only authorized devices are given access, and unauthorized and unmanaged devices are found and prevented from gaining access.			
20 CC	Critical Control 2: Inventory of Authorized and Unauthorized Software	0	**89**	Actively manage (inventory, track, and correct) all software on the network so that only authorized software is installed and can execute, and that unauthorized and unmanaged software is found and prevented from installation or execution.			
20 CC	Critical Control 3: Secure Configurations for Hardware and Software on Mobile Devices, Laptops, Workstations, and Servers	0	**89**	Establish, implement, and actively manage (track, report on, correct) the security configuration of laptops, servers, and workstations using a rigorous configuration management and change control process in order to prevent attackers from exploiting vulnerable services and settings.			
20 CC	Critical Control 7: Email and Web Browser Protections	0	**89**	Minimize the attack surface and the opportunities for attackers to manipulate human behavior though their interaction with web browsers and email systems.			
20 CC	Critical Control 11: Secure Configurations for Network Devices such as Firewalls, Routers, and Switches	0	**89**	Establish, implement, and actively manage (track, report on, correct) the security configuration of network infrastructure devices using a rigorous configuration management and change control process in order to prevent attackers from exploiting vulnerable services and settings.			
20 CC	Critical Control 12: Boundary Defense	0	**89**	Detect/prevent/correct the flow of information transferring networks of different trust levels with a focus on security-damaging data.			
20 CC	Critical Control 15: Wireless Access Control	0	**89**	The processes and tools used to track/control/prevent/correct the security use of wireless local area networks (LANS), access points, and wireless client systems.			
20 CC	Critical Control 17: Security Skills Assessment and Appropriate Training to Fill Gaps	0	**89**	For all functional roles in the organization (prioritizing those mission-critical to the business and its security), identify the specific knowledge, skills, and abilities needed to support defense of the enterprise; develop and execute an integrated plan to assess, identify gaps, and remediate through policy, organizational planning, training, and awareness programs.			
20 CC	Critical Control 19: Incident Response and Management	0	**89**	Protect the organization's information, as well as its reputation, by developing and implementing an incident response infrastructure (e.g., plans, defined roles, training, communications, management oversight) for quickly discovering an attack and then effectively containing the damage, eradicating the attacker's presence, and restoring the integrity of the network and systems.			
ISO	ISO - Setup the Information Security Team and Approach	0	**89**	Organization has defined and set up the overall Information Security responsibility; Team roles and responsibilities; including the meeting structure (ISMT agenda, ISMT minutes).			
ISO	ISO - Update Annual Planning	0	**89**	IT Security is considered in the Organization's Annual planning.			
NIST	NIST - Business Environment	0	**89**	Business Environment (ID.BE): The organization's mission, objectives, stakeholders, and activities are understood and prioritized; this information is used to inform cybersecurity roles, responsibilities, and risk management decisions.			
20 CC	Critical Control 4: Continuous Vulnerability Assessment and Remediation	0	**78**	Continuously acquire, assess, and take action on new information in order to identify vulnerabilities, remediate, and minimize the window of opportunity for attackers.			
20 CC	Critical Control 6: Maintenance, Monitoring, and Analysis of Audit Logs	0	**78**	Collect, manage, and analyze audit logs of events that could help detect, understand, or recover from an attack.			
20 CC	Critical Control 10: Data Recovery Capability	0	**78**	The processes and tools used to properly back up critical information with a proven methodology for timely recovery of it.			
20 CC	Critical Control 14: Controlled Access Based on the Need to Know	0	**78**	The processes and tools used to track/control/prevent/correct secure access to critical assets (e.g., information, resources, systems) according to the formal determination of which persons, computers, and applications have a need and right to access these critical assets based on an approved classification.			
20 CC	Critical Control 16: Account Monitoring and Control	0	**78**	Actively manage the life cycle of system and application accounts – their creation, use, dormancy, deletion – in order to minimize opportunities for attackers to leverage them.			
ISO	ISO - Physical And Environmental Security	0	**78**	Critical or sensitive information-processing facilities are physically protected from unauthorized access, damage, interference, and environmental threats.			

Framework	Control Name	Rating	CySAFE Score	Control Description	Current Controls in Place	Exceptions	Planned Work
ISO	ISO - Measure Effectiveness of Controls	0	**78**	Organization has implemented procedures to measure the effectiveness of controls.			
ISO	ISO - Compliance	0	**78**	Organization has explicitly defined, documented, and kept up to date all relevant statutory, regulatory, and contractual requirements and the organization's approach to meet these requirements should be for each information system. There is an organizational focus on compliance with security policies and standards, and technical compliance.			
NIST	NIST - Maintenance	0	**78**	Maintenance (PR.MA): Maintenance and repair of Information systems is performed consistent with organizational policies and procedures.			
20 CC	Critical Control 9: Limitation and Control of Network Ports, Protocols, and Services	0	**67**	Manage (track/control/correct) the ongoing operational use of ports, protocols, and services on networked devices in order to minimize windows of vulnerability available to attackers.			
20 CC	Critical Control 13: Data Protection	0	**67**	The processes and tools used to prevent data exfiltration, mitigate the effects of exfiltrated data, and ensure the privacy and integrity of sensitive information.			
ISO	ISO - Communicate Information Security Policy	0	**67**	Organization has documented, approved, and communicated, the Information Security Policy to the employees of the Information Security Management System (ISMS) scope.			
ISO	ISO - Identify Resources, Ownership and Standard Operating Procedures for IT Processes	0	**67**	Organization has identified and approved the relevant resource owners within the Information Security Management System (ISMS) scope.			
NIST	NIST - Governance	0	**67**	Governance (ID.GV): The policies, procedures, and processes to manage and monitor the organization's regulatory, legal, risk, environmental, and operational requirements are understood and inform the management of cybersecurity risk.			
NIST	NIST - Risk Management Strategy	0	**67**	Risk Management Strategy (ID.RM): The organization's priorities, constraints, risk tolerances, and assumptions are established and used to support operational risk decisions.			
20 CC	Critical Control 18: Application Software Security	0	**56**	Manage the security life cycle of all in-house developed and acquired software in order to prevent, detect, and correct security weaknesses.			
20 CC	Critical Control 20: Penetration Tests and Red Team Exercises	0	**56**	Test the overall strength of an organization's defenses (the technology, the processes, and the people) by simulating the objectives and actions of an attacker.			
ISO	ISO - Define and Generate Records (evidence)	0	**56**	A list of records to provide evidence of conformity to requirements and the effective operation of the ISMS and controls, including the protection requirements is defined and maintained.			

Control Category and Summary

Category Summary

Framework	Control Category: Strategy/Scope	Rating	CySAFE Score
ISO	ISO - Define Scope	0	100
ISO	ISO - Complete Summary of Controls	0	100
ISO	ISO - Setup the Information Security Team and Approach	0	89
ISO	ISO - Update Annual Planning	0	89
NIST	NIST - Business Environment	0	89
ISO	ISO - Compliance	0	78
ISO	ISO - Communicate Information Security Policy	0	67
NIST	NIST - Governance	0	67
NIST	NIST - Risk Management Strategy	0	67
	Average Rating	**0.00**	

Framework	Control Category: Planning/Design/Configuration	Rating	CySAFE Score
20 CC	Critical Control 8: Malware Defenses	0	100
20 CC	Critical Control 1: Inventory of Authorized and Unauthorized Devices	0	89
20 CC	Critical Control 2: Inventory of Authorized and Unauthorized Software	0	89
20 CC	Critical Control 3: Secure Configurations for Hardware and Software on Mobile Devices, Laptops, Workstations, and Servers	0	89
20 CC	Critical Control 11: Secure Configurations for Network Devices such as Firewalls, Routers, and Switches	0	89
20 CC	Critical Control 12: Boundary Defense	0	89
20 CC	Critical Control 15: Wireless Access Control	0	89
20 CC	Critical Control 17: Security Skills Assessment and Appropriate Training to Fill Gaps	0	89
20 CC	Critical Control 9: Limitation and Control of Network Ports, Protocols, and Services	0	67
20 CC	Critical Control 13: Data Protection	0	67
ISO	ISO - Identify Resources, Ownership and Standard Operating Procedures for IT Processes	0	67
	Average Rating	**0.00**	

Framework	Control Category: Operations	Rating	CySAFE Score
20 CC	Critical Control 5: Controlled Use of Administrative Privileges	0	100
ISO	ISO - Monitoring and Review of Third Party Services	0	100
20 CC	Critical Control 7: Email and Web Browser Protections	0	89
20 CC	Critical Control 4: Continuous Vulnerability Assessment and Remediation	0	78
20 CC	Critical Control 14: Controlled Access Based on the Need to Know	0	78
20 CC	Critical Control 16: Account Monitoring and Control	0	78
ISO	ISO - Physical And Environmental Security	0	78
NIST	NIST - Maintenance	0	78
20 CC	Critical Control 18: Application Software Security	0	56
	Average Rating	**0.00**	

Framework	Control Category: Monitoring/Metrics	Rating	CySAFE Score
20 CC	Critical Control 6: Maintenance, Monitoring, and Analysis of Audit Logs	0	78
ISO	ISO - Measure Effectiveness of Controls	0	78
ISO	ISO - Define and Generate Records (evidence)	0	56
	Average Rating	**0.00**	

Framework	Control Category: Response/Recovery	Rating	CySAFE Score
20 CC	Critical Control 19: Incident Response and Management	0	89
20 CC	Critical Control 10: Data Recovery Capability	0	78
20 CC	Critical Control 20: Penetration Tests and Red Team Exercises	0	56
	Average Rating	**0.00**	

Controls are grouped into five different categories:
1. Strategy/Score
2. Planning/Design/Configuration
3. Operations
4. Monitoring/Metrics
5. Response/Recovery

Each category will show each control's Rating and CySAFE Score. The Ratings are averaged per category and summarized in the chart and graphs below.

The Rating averages will help track progress over time in the Capability Maturity Model Integration (CMMI)

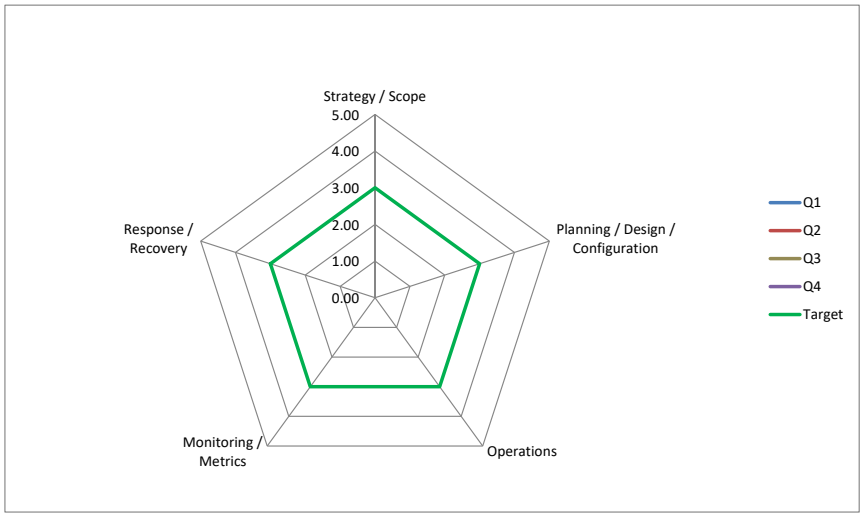
CySAFE℠
CYBER SECURITY ASSESSMENT FOR EVERYONE
VERSION 2.0

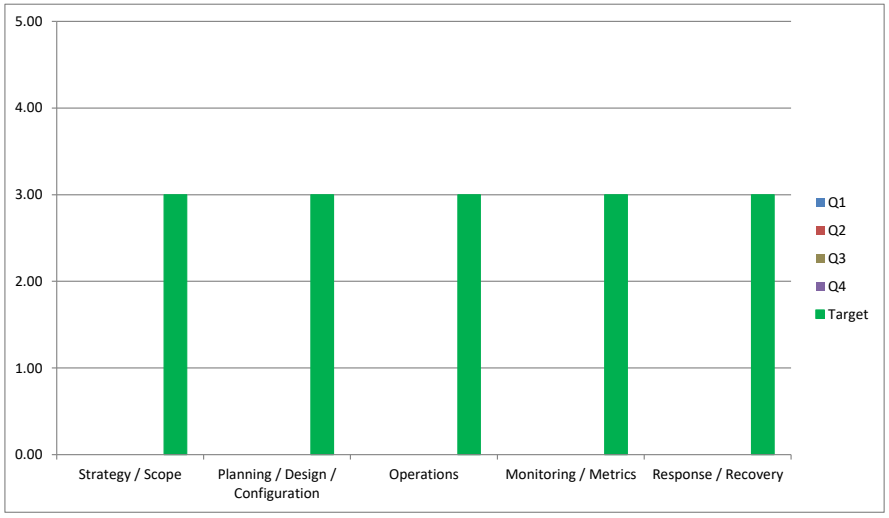
Progress Chart and Graphs

Q1

The graphs below will be generated using the average of the Ratings provided on the Assessment sheet. To save the averages, select which quarter they should be saved into and click "Save Quarter". The Average Ratings will automatically be filled in and the graphs will be generated. Target can be filled based on the business risk level. A Target of 3.0 is the basic recommendation.

Control Category	Q1	Q2	Q3	Q4	Target
Strategy / Scope	0.00	0.00	0.00	0.00	3.0
Planning / Design / Configuration	0.00	0.00	0.00	0.00	3.0
Operations	0.00	0.00	0.00	0.00	3.0
Monitoring / Metrics	0.00	0.00	0.00	0.00	3.0
Response / Recovery	0.00	0.00	0.00	0.00	3.0





Control Name	Control Description	Example of Controls in Place	Basic	Cost	Time	Risk	Total
Critical Control 1: Inventory of Authorized and Unauthorized Devices	Actively manage (inventory, track, and correct) all hardware devices on the network so that only authorized devices are given access, and unauthorized and unmanaged devices are found and prevented from gaining access.	Inventories for PCs, Servers, Network, Mobile devices	Have device inventory management process implemented for PCs, Servers, Network and Mobile devices (Excel Spreadsheet)	3	3	2	8
Critical Control 2: Inventory of Authorized and Unauthorized Software	Actively manage (inventory, track, and correct) all software on the network so that only authorized software is installed and can execute, and that unauthorized and unmanaged software is found and prevented from installation or execution.	Software inventory for servers, applications, PCs Mobile software inventory	Have software inventory management process implemented for PCs, Servers, Network and Mobile devices (Excel Spreasheet)	3	2	3	8
Critical Control 3: Secure Configurations for Hardware and Software on Mobile Devices, Laptops, Workstations, and Servers	Establish, implement, and actively manage (track, report on, correct) the security configuration of laptops, servers, and workstations using a rigorous configuration management and change control process in order to prevent attackers from exploiting vulnerable services and settings.	Change default passwords Limit services and ports Implement Firewall Rules	Secure configuration Change default passwords Limit ports/services to only those needed Firewall rules	3	2	3	8
Critical Control 4: Continuous Vulnerability Assessment and Remediation	Continuously acquire, assess, and take action on new information in order to identify vulnerabilities, remediate, and minimize the window of opportunity for attackers.	Penetration Test Vulnerability Test Proxy Patching	Monthly Patching (OS/Browser) Vulnerability Scan (Yearly)	3	1	3	7
Critical Control 5: Controlled Use of Administrative Privileges	The processes and tools used to track/control/prevent/correct the use, assignment, and configuration of administrative privileges on computers, networks, and applications.	Limit admin access Dual factor Remove access rights	Control/remove admin access	3	3	3	9
Critical Control 6: Maintenance, Monitoring, and Analysis of Audit Logs	Collect, manage, and analyze audit logs of events that could help detect, understand, or recover from an attack.	Event Logging	Enable logging monthly monitor of logs	3	3	1	7
Critical Control 7: Email and Web Browser Protections	Minimize the attack surface and the opportunities for attackers to manipulate human behavior though their interaction with web browsers and email systems.	Policy regarding supported web browsers and email clients. Process to scan and block all e-mail attachments entering the organization's e-mail gateway. Sender Policy Framework (SPF) To lower the chance of spoofed e-mail messages.	Browser Restrictions Scanning emails	3	3	2	8
Critical Control 8: Malware Defenses	Control the installation, spread, and execution of malicious code at multiple points in the enterprise, while optimizing the use of automation to enable rapid updating of defense, data gathering, and corrective action.	PC Antivirus Anti-Malware IPS IDS	Antivirus Malware protection	3	3	3	9
Critical Control 9: Limitation and Control of Network Ports, Protocols, and Services	Manage (track/control/correct) the ongoing operational use of ports, protocols, and services on networked devices in order to minimize windows of vulnerability available to attackers.	FW Access Control Lists Change default passwords Limit services and ports Implement Firewall Rules	Change default pwd Limit ports/services FW rules	3	1	2	6
Critical Control 10: Data Recovery Capability	The processes and tools used to properly back up critical information with a proven methodology for timely recovery of it.	Nightly backups Key management DR tests	Periodic Backup/Recovery Processes	2	2	3	7

Legend

Cost
3 0 < $25K
2 $25K - $75K
1 > $75K

Time
3 < 60 days
2 61-120 days
1 > 121 days

Risk
3 High
2 Med
1 Low

Total
Cost + Time + Risk

Control Name	Control Description	Example of Controls in Place	Basic	Cost	Time	Risk	Total
Critical Control 11: Secure Configurations for Network Devices such as Firewalls, Routers, and Switches	Establish, implement, and actively manage (track, report on, correct) the security configuration of network infrastructure devices using a rigorous configuration management and change control process in order to prevent attackers from exploiting vulnerable services and settings.	Standard hardened Configurations for Network Equipment. Separate VLANs or, preferably, on entirely different physical connectivity for management sessions for network devices.	Secure configuration	3	2	3	8
Critical Control 12: Boundary Defense	Detect/prevent/correct the flow of information transferring networks of different trust levels with a focus on security-damaging data.	Firewall IPS Proxy DMZ FTP/SSH (File Transfer) Tool/Management	Firewall	3	2	3	8
Critical Control 13: Data Protection	The processes and tools used to prevent data exfiltration, mitigate the effects of exfiltrated data, and ensure the privacy and integrity of sensitive information.	Data Classification to identify sensitive data Bitlocker Disk Encryption Network-based DLP solutions	Bitlocker Network-based DLP solutions	2	2	2	6
Critical Control 14: Controlled Access Based on the Need to Know	The processes and tools used to track/control/prevent/correct secure access to critical assets (e.g., information, resources, systems) according to the formal determination of which persons, computers, and applications have a need and right to access these critical assets based on an approved classification.	Classification of systems and data Architecture strategy Required controls based on data type	Classify Systems by Confidential/Internal Use/Public based on department and applications access	3	1	3	7
Critical Control 15: Wireless Access Control	The processes and tools used to track/control/prevent/correct the security use of wireless local area networks (LANS), access points, and wireless client systems.	Segement network Create Guest network Create User Agreements Network vulnerability scanning tools to detect rogue Wireless devices on the network Disable split tunneling.	Password protect Access Points Awareness of Access Don't Broadcast SSID Use more complex encryption (WPA2)	3	3	2	8
Critical Control 16: Account Monitoring and Control	Actively manage the life cycle of system and application accounts – their creation, use, dormancy, deletion – in order to minimize opportunities for attackers to leverage them.	Periodic Account Review Review User Lifecycle Management System Configure account lockouts after failed login attempts. Dual-Factor accounts for high privilege accounts.	Disable terminated accounts On-board/Exit procedures Process in place to periodically review of access to systems	3	2	2	7
Critical Control 17: Security Skills Assessment and Appropriate Training to Fill Gaps	For all functional roles in the organization (prioritizing those mission-critical to the business and its security), identify the specific knowledge, skills, and abilities needed to support defense of the enterprise; develop and execute an integrated plan to assess, identify gaps, and remediate through policy, organizational planning, training, and awareness programs.	User IT Security Awareness Training Specialized IT Security training for the IT Staff (SANS)	Organization wide awareness training	3	2	3	8
Critical Control 18: Application Software Security	Manage the security life cycle of all in-house developed and acquired software in order to prevent, detect, and correct security weaknesses.	SDLC QA tools / process 3rd party reviews Protect web applications by deploying web application firewalls (WAFs)	Many small governments do not develop applications	1	2	2	5

Control Name	Control Description	Example of Controls in Place	Basic	Cost	Time	Risk	Total
Critical Control 19: Incident Response and Management	Protect the organization's information, as well as its reputation, by developing and implementing an incident response infrastructure (e.g., plans, defined roles, training, communications, management oversight) for quickly discovering an attack and then effectively containing the damage, eradicating the attacker's presence, and restoring the integrity of the network and systems.	Cyber Incident Response Plan (CISP)- practice refine, review incident metric, and adjust operation processes	Have Cyber Incident Response Plan. Communicate plan to staff. Execute as needed.	3	2	3	8
Critical Control 20: Penetration Tests and Red Team Exercises	Test the overall strength of an organization's defenses (the technology, the processes, and the people) by simulating the objectives and actions of an attacker.	Penetration Tests and Red Team Exercises	Penetration Tests and Red Team Exercises	2	1	2	5

Control Name	Control Description	Example of Controls in Place	Basic	Cost	Time	Risk	Total
ISO - Define Scope	The organization has defined the scope of the Information Security Management System (ISMS), taking into account the characteristics of the business, its location and technology.	Scope limited to Critical systems, Primary ERP system or ALL systems supported by IT	Documented control scope and clear exclusions	3	3	3	9
ISO - Setup the Information Security Team and Approach	Organization has defined and set up the overall Information Security responsibility; Team roles and responsibilities; including the meeting structure (ISMT agenda, ISMT minutes).	Periodic meetings	Meetings dedicated to discussing current SECURITY threats, issues and projects	3	2	3	8
ISO - Communicate Information Security Policy	Organization has documented, approved, and communicated, the Information Security Policy to the employees of the Information Security Management System (ISMS) scope.	Written, approved and communicated policy	Written, approved and communicated policy	3	1	2	6
ISO - Identify Resources, Ownership and Standard Operating Procedures for IT Processes	Organization has identified and approved the relevant resource owners within the Information Security Management System (ISMS) scope.	Resource/Asset owner list	List(s) of current assets such as People, Documents, Location, Servers, Network gear, PCs, Applications, Middleware and mobile devices	3	1	2	6
ISO - Monitoring and Review of Third Party Services	The services, reports and records provided by the third party are monitored, reviewed, and audits carried out regularly.	Information security terms and conditions are included in the agreements (Contracts, SOW) with the third party service providers. Information security terms and conditions in the agreements are being adhered to by the service providers. The organization maintains sufficient overall control and visibility into all security aspects for sensitive or critical information or information processing facilities accessed, processed or managed by the third party service providers.	Information security terms and conditions included in the vendor agreements (Contracts, SOW). The responsibility for managing the relationship with the third party should be assigned to a designated individual/team. Records of security events, operational problems, failures, tracings of faults and disruptions related to the service delivered are maintained and reviewed by the responsible individual/team.	3	3	3	9
ISO - Complete Summary of Controls	The Organization has a "Summary of Controls" document that includes: a) the control(s) selected and reasons for their selection (control objectives); b) the reason for the exclusion of controls; c) the controls currently implemented; d the status and due date for the controls that still need to be implemented; and e) reference to the Information Security Risk Analysis, directives and procedures.	Output from Risk analysis, risk treatment plans and managed risk processes.	Summary of risks, plans and decisions	3	3	3	9
ISO - Define and Generate Records (evidence)	A list of records to provide evidence of conformity to requirements and the effective operation of the ISMS and controls, including the protection requirements is defined and maintained.	Define what output proves the controls are established so the output can be included in the control requirement; This helps when an audit is performed.	Defined list of records for the controls	3	1	1	5

Legend

Cost
3 0 < $25K
2 $25K - $75K
1 > $75K

Time
3 < 60 days
2 61-120 days
1 > 121 days

Risk
3 High
2 Med
1 Low

Total

Control Name	Control Description	Example of Controls in Place	Basic	Cost	Time	Risk	Total
ISO - Physical And Environmental Security	Critical or sensitive information-processing facilities are physically protected from unauthorized access, damage, interference, and environmental threats.	Physical entry controls, securing offices, rooms, and facilities. Physical protection and guidelines for working in secure areas. Public access, delivery, and loading areas are controlled. Physical protection against damage from fire, flood, earthquake, explosion, civil unrest, and other forms of natural or man-made disaster should be designed and applied.	Well defined Security Perimeters, Site Permiters are physically sound, Manned reception area,Intruder detection systems. Only Authorized personnel are allowed to access the facilities.	2	2	3	7
ISO - Measure Effectiveness of Controls	Organization has implemented procedures to measure the effectiveness of controls.	Establish control objective and measurement along with targets	Measure controls periodically to gauge effectiveness of program	3	1	3	7

Control Name	Control Description	Example of Controls in Place	Basic	Cost	Time	Risk	Total
ISO - Update Annual Planning	IT Security is considered in the Organization's Annual planning.	Build security into project reqquirements; Budget and plan for security improvements projects	Plan for security improvements and new projects	3	2	3	8
ISO - Compliance	Organization has explicitly defined, documented, and kept up to date all relevant statutory, regulatory, and contractual requirements and the organization's approach to meet these requirements should be for each information system. There is an organizational focus on compliance with security policies and standards, and technical compliance.	Applicable legislations and compliance requirements are identified. The specific controls and individual responsibilities to meet these requirements should be similarly defined and documented. Intellectual property rights (IPR), appropriate procedures are implemented to ensure compliance with legislative, regulatory, and contractual requirements on the use of material in respect of which there may be intellectual property rights and on the use of proprietary software products. Compliance with organization's security policies and standards - security procedures are identified. Responsibilities are defined and documented. Technical compliance checking - Information systems are regularly checked for compliance with security implementation standards.	Identify Compliance requirements (HIPAA, PCI, CJIS) Management prioritizes compliance requirement RACI for compliance programs Annual review of internal and external compliance requirements.	2	2	3	7

Control Name	Control Description	Example of Controls in Place	Basic	Cost	Time	Risk	Total
NIST - Business Environment	Business Environment (ID.BE): The organization's mission, objectives, stakeholders, and activities are understood and prioritized; this information is used to inform cybersecurity roles, responsibilities, and risk management decisions.	This information should be known by the IT Director in order to effectly perform the IT leadership role.	Scope of understanding of the organizations security risk posture, protocols and structure.	3	2	3	8
NIST - Governance	Governance (ID.GV): The policies, procedures, and processes to manage and monitor the organization's regulatory, legal, risk, environmental, and operational requirements are understood and inform the management of cybersecurity risk.	Basic understanding of RACI (Responsible, Accountable, Consult, Inform) for all cyber security topics; Example: IT acts as the data steward for the business units; Legal is responsible for informing IT of regulatory changes; Business management is responsible for managing and adhering to operational security procedures;	Basic understanding of RACI (Responsible, Accountable, Consult, Inform) for policies, procedures, and processes to manage and monitor the organization's regulatory, legal, risk, environmental, and operational requirements are understood and inform the management of cybersecurity risk.	3	1	2	6
NIST - Risk Management Strate	Risk Management Strategy (ID.RM): The organization's priorities, constraints, risk tolerances, and assumptions are established and used to support operational risk decisions.	Ongoing communications to the organization about cybersecurity risks and rationale for investment in cybersecurity tools.	Ongoing communications to the organization about cybersecurity risks and rationale for investment in cybersecurity tools.	3	1	2	6
NIST - Maintenance	Maintenance (PR.MA): Maintenance and repair of Information systems is performed consistent with organizational policies and procedures.	Operating procedures are documented, maintained for the Information System Admins. Responsibilities the management and operation of all information processing facilities are established. Changes to information processing facilities and systems are controlled. Development, test, and operational facilities are separated to reduce the risks of unauthorised access or changes to the operational system. Hardware/Software upgrades/patches are applied to remove or reduce security weaknesses as needed.	Periodic Patching, System Upgrades	2	2	3	7

Post Rating (0-5)

Legend

Cost
3 0 < $25K
2 $25K - $75K
1 > $75K

Time
3 < 60 days
2 61-120 days
1 > 121 days

Risk
3 High
2 Med
1 Low

Total
Cost + Time + Risk

Appendix - A

Instructions for the Existing CySAFE 1.0 migrating Assessment Results to CySAFE 2.0			
Framework	**CySAFE 2.0**	**CySAFE 1.0**	**Action**
20 CC	Critical Control 1: Inventory of Authorized and Unauthorized Devices	Critical Control 1: Inventory of Authorized and Unauthorized Devices	No Change Needed - Use the Assessment Results from CySAFE 1.0 as the baseline.
20 CC	Critical Control 2: Inventory of Authorized and Unauthorized Software	Critical Control 2: Inventory of Authorized and Unauthorized Software	No Change Needed - Use the Assessment Results from CySAFE 1.0 as the baseline.
20 CC	Critical Control 3: Secure Configurations for Hardware and Software on Mobile Devices, Laptops, Workstations, and Servers	Critical Control 3: Secure Configurations for Hardware and Software on Mobile Devices, Laptops, Workstations, and Servers	No Change Needed - Use the Assessment Results from CySAFE 1.0 as the baseline.
20 CC	Critical Control 4: Continuous Vulnerability Assessment and Remediation	Critical Control 4: Continuous Vulnerability Assessment and Remediation	No Change Needed - Use the Assessment Results from CySAFE 1.0 as the baseline.
20 CC	Critical Control 5: Controlled Use of Administrative Privileges	Critical Control 12: Controlled Use of Administrative Privileges	Refer to Critical Control 12 Assessment Results in CySAFE 1.0
20 CC	Critical Control 6: Maintenance, Monitoring, and Analysis of Audit Logs	Critical Control 14: Maintenance, Monitoring, and Analysis of Audit Logs	Refer to Critical Control 14 Assessment Results in CySAFE 1.0
20 CC	Critical Control 7: Email and Web Browser Protections		New Control - Refer to Control details in the 20 CC worksheet.
20 CC	Critical Control 8: Malware Defenses	Critical Control 5: Malware Defenses	Refer to Critical Control 5 Assessment Results in CySAFE 1.0
20 CC	Critical Control 9: Limitation and Control of Network Ports, Protocols, and Services	Critical Control 11: Limitation and Control of Network Ports, Protocols, and Services	Refer to Critical Control 11 Assessment Results in CySAFE 1.0
20 CC	Critical Control 10: Data Recovery Capability	Critical Control 8: Data Recovery Capability	Refer to Critical Control 8 Assessment Results in CySAFE 1.0
20 CC	Critical Control 11: Secure Configurations for Network Devices such as Firewalls, Routers, and Switches	Critical Control 10: Secure Configurations for Network Devices such as Firewalls, Routers, and Switches	Refer to Critical Control 10 Assessment Results in CySAFE 1.0
20 CC	Critical Control 12: Boundary Defense	Critical Control 13: Boundary Defense	Refer to Critical Control 13 Assessment Results in CySAFE 1.0
20 CC	Critical Control 13: Data Protection	Critical Control 17: Data Loss Prevention	Refer to Critical Control 17 Assessment Results in CySAFE 1.0
20 CC	Critical Control 14: Controlled Access Based on the Need to Know	Critical Control 15: Controlled Access Based on the Need to Know	Refer to Critical Control 15 Assessment Results in CySAFE 1.0
20 CC	Critical Control 15: Wireless Access Control	Critical Control 7: Wireless Device Control	Refer to Critical Control 7 Assessment Results in CySAFE 1.0
20 CC	Critical Control 16: Account Monitoring and Control	Critical Control 16: Account Monitoring and Control	No Change Needed - Use the Assessment Results from CySAFE 1.0 as the baseline.
20 CC	Critical Control 17: Security Skills Assessment and Appropriate Training to Fill Gaps	Critical Control 9: Security Skills Assessment and Appropriate Training to Fill Gaps	Refer to Critical Control 9 Assessment Results in CySAFE 1.0
20 CC	Critical Control 18: Application Software Security	Critical Control 6: Application Software Security	Refer to Critical Control 6 Assessment Results in CySAFE 1.0
20 CC	Critical Control 19: Incident Response and Management	Critical Control 18: Incident Response and Management	Refer to Critical Control 18 Assessment Results in CySAFE 1.0
20 CC	Critical Control 20: Penetration Tests and Red Team Exercises		New Control - Refer to Control details in the 20 CC worksheet.
20 CC		Critical Control 19: Secure Network Engineering	Critical control deleted in CIS - Critical Control Ver 6.1

Instructions for the Existing CySAFE 1.0 migrating Assessment Results to CySAFE 2.0			
Framework	**CySAFE 2.0**	**CySAFE 1.0**	**Action**
ISO	Define Scope	Define Scope	No Change Needed - Use the Assessment Results from CySAFE 1.0 as the baseline.
ISO	Setup the Information Security Team and Approach	Setup the Information Security Team and Approach	No Change Needed - Use the Assessment Results from CySAFE 1.0 as the baseline.
ISO	Communicate Information Security Policy	Communicate Information Security Policy	No Change Needed - Use the Assessment Results from CySAFE 1.0 as the baseline.
ISO	Identify Resources, Ownership and Standard Operating Procedures for IT Processes	Identify Resources, Ownership and Standard Operating Procedures for IT Processes	No Change Needed - Use the Assessment Results from CySAFE 1.0 as the baseline.
ISO	Monitoring and review of third party services		New Control - Refer to Control details in the ISO worksheet.
ISO	Complete Summary of Controls	Complete Summary of Controls	No Change Needed - Use the Assessment Results from CySAFE 1.0 as the baseline.
ISO	Define and Generate Records (evidence)	Define and Generate Records (evidence)	No Change Needed - Use the Assessment Results from CySAFE 1.0 as the baseline.
ISO	Physical And Environmental Security		New Control - Refer to Control details in the ISO worksheet.
ISO	Measure Effectiveness of Controls	Measure Effectiveness of Controls	No Change Needed - Use the Assessment Results from CySAFE 1.0 as the baseline.
ISO	Update Annual Planning	Update Annual Planning	No Change Needed - Use the Assessment Results from CySAFE 1.0 as the baseline.
ISO	Compliance		New Control - Refer to Control details in the ISO worksheet.
ISO		Perform Business Management Review (if applicable)	ISO Control Deleted in CySAFE 2.0
ISO		Conduct Internal ISMS Audits	ISO Control Deleted in CySAFE 2.0
ISO		Data Classification (not in the ISMS but valuable)	ISO Control Deleted in CySAFE 2.0

Instructions for the Existing CySAFE 1.0 migrating Assessment Results to CySAFE 2.0			
Framework	**CySAFE 2.0**	**CySAFE 1.0**	**Action**
NIST	Business Environment	Business Environment	No Change Needed - Use the Assessment Results from CySAFE 1.0 as the baseline.
NIST	Governance	Governance	No Change Needed - Use the Assessment Results from CySAFE 1.0 as the baseline.
NIST	Risk Management Strategy	Risk Management Strategy	No Change Needed - Use the Assessment Results from CySAFE 1.0 as the baseline.
NIST	Maintenance	Maintenance	Expected ontrols aligned with Maintenance of IT Systems.
NIST		Anomalies and Events	NIST Control Deleted - CySAFE 1.0 Assessment can be migrated to Assessment of Critical Controls 6 in CySAFE 2.0.
NIST		Detection Processes	NIST Control Deleted - CySAFE 1.0 Assessment can be migrated to Assessment of Critical Controls 19 in CySAFE 2.0.

New Feature

Four columns were added to the ***Assessment Results*** tab to create a "SUMMARY of Controls" Worksheet which will help further clarify the sub controls are currently in place, list any exceptions and describe work is planned to improve that control.

Appendix - B

Standards Documents:

20 Critical Controls	http://www.sans.org/critical-security-controls
NIST	www.nist.gov/cyberframework/upload/cybersecurity-framework-021214.pdf
ISO 27001	www.iso.org/iso/home/standards/management-standards/iso27001.htm

Reference Documents:

NIST SP 800-53 Rev 4	http://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-53r4.pdf
Verizon Security Report	http://www.verizonenterprise.com/DBIR/
COIN	http://www.countyinnovation.us/
Capability Maturity Model Integration (CMMI)	http://en.wikipedia.org/wiki/Capability_Maturity_Model_Integration
DHS Cyber Security Homepage	http://www.dhs.gov/topic/cybersecurity
DHS Critical Infrastructure Cyber Community C³ Voluntary Program	http://www.dhs.gov/about-critical-infrastructure-cyber-community-c³-voluntary-program

CySAFE Contributors:

Phil Bertolini - Oakland County, MI - Deputy County Executive and CIO
Andrew Brush - Washtenaw County, MI - CIO
Chris Burrows - Oakland County, MI - CISO
Rodney Davenport - State of Michigan - CSO
Colleen Hinzmann - Monroe County, MI - IT Director
Rich Malewicz - Livingston County, MI - Deputy County Administrator/CIO
Jessica Moy - State of Michigan - DTMB Director, Technology Partnerships
Jeffrey Small - Wayne County. MI - Deputy CIO
Edward D. Winfield - Wayne County, MI - CIO