CySAFE℠

Cyber Security Assessment for Everyone

Overview

In the world of cyber security, local governments 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 government agencies 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 379 controls from all three frameworks into one condensed list, removing any redundant controls and assess the controls against the government agency's current IT security capabilities. Next, the master list of 36 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. The evaluation was completed in a collaborative effort by the IT specialists from the six participating Michigan government agencies (See Appendix).

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 36 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 worksheet.

Step 2: Become Familiar With the Tool

CySAFE was built in a Microsoft Excel workbook with eight 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 36 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 the government agency'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 19 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 6 selected controls including: control descriptions, examples of controls in place and the basic security level recommended

- **Appendix:** 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 adapted 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 government agency'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 36 controls with the rating and CySAFE Score sorted from highest to lowest priority and will be also be color coded to depict your government agency'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

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 government agency 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: CySAFE is a suggested tool for evaluating security measures for local government entities. It is not intended to be relied upon or used as a comprehensive means to protect against all potential security risks. A review of additional security standards such as NIST Cyber Security Framework, ISO 27001 and 20 Critical Controls is recommended, as well as a thorough review of each government's unique security requirements. Although CySAFE was drafted by individuals from several governments, it is not an official publication or policy of any of those governments. No governmental entity with a participant in the drafting of CySAFE, may be held liable for any errors or omissions in CySAFE, or held liable for damages resulting from reliance upon the information contained in the CySAFE.

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		No Score Yet
20 CC	Critical Control 2: Inventory of Authorized and Unauthorized Software	3	2	3	8		No Score Yet
20 CC	Critical Control 3: Secure Configurations for Hardware and Software on Mobile Devices, Laptops, Workstations, and Servers	3	2	3	8		No Score Yet
20 CC	Critical Control 4: Continuous Vulnerability Assessment and Remediation	3	1	3	7		No Score Yet
20 CC	Critical Control 5: Malware Defenses	3	3	3	9		No Score Yet
20 CC	Critical Control 6: Application Software Security	1	2	2	5		No Score Yet
20 CC	Critical Control 7: Wireless Device Control	3	3	2	8		No Score Yet
20 CC	Critical Control 8: Data Recovery Capability	2	2	3	7		No Score Yet
20 CC	Critical Control 9: Security Skills Assessment and Appropriate Training to Fill Gaps	3	2	3	8		No Score Yet
20 CC	Critical Control 10: Secure Configurations for Network Devices such as Firewalls, Routers, and Switches	3	2	3	8		No Score Yet
20 CC	Critical Control 11: Limitation and Control of Network Ports, Protocols, and Services	3	1	2	6		No Score Yet
20 CC	Critical Control 12: Controlled Use of Administrative Privileges	3	3	3	9		No Score Yet
20 CC	Critical Control 13: Boundary Defense	3	2	3	8		No Score Yet
20 CC	Critical Control 14: Maintenance, Monitoring, and Analysis of Audit Logs	3	3	1	7		No Score Yet
20 CC	Critical Control 15: Controlled Access Based on the Need to Know	3	1	3	7		No Score Yet
20 CC	Critical Control 16: Account Monitoring and Control	3	2	2	7		No Score Yet
20 CC	Critical Control 17: Data Loss Prevention	2	2	2	6		No Score Yet
20 CC	Critical Control 18: Incident Response and Management	3	2	3	8		No Score Yet
20 CC	Critical Control 19: Secure Network Engineering	1	1	2	4		No Score Yet

Framework	Control Name	Cost	Time	Risk	Total	Rating	CySAFE Score
ISO	Define Scope	3	3	3	9		No Score Yet
ISO	Setup the Information Security Team and Approach	3	2	3	8		No Score Yet
ISO	Communicate Information Security Policy	3	1	2	6		No Score Yet
ISO	Identify Resources, Ownership and Standard Operating Procedures for IT Processes	3	1	2	6		No Score Yet
ISO	Complete Summary of Controls	3	3	3	9		No Score Yet
ISO	Define and Generate Records (evidence)	3	1	1	5		No Score Yet
ISO	Perform Business Management Review (if applicable)	3	1	1	5		No Score Yet
ISO	Conduct Internal ISMS Audits	3	1	3	7		No Score Yet
ISO	Measure Effectiveness of Controls	3	1	2	6		No Score Yet
ISO	Update Annual Planning	3	2	3	8		No Score Yet
ISO	Data Classification (not in the ISMS but valuable)	3	2	3	8		No Score Yet

Framework	Control Name	Cost	Time	Risk	Total	Rating	CySAFE Score
NIST	Business Environment	3	2	3	8		No Score Yet
NIST	Governance	3	1	2	6		No Score Yet
NIST	Risk Management Strategy	3	1	2	6		No Score Yet
NIST	Maintenance	2	2	3	7		No Score Yet
NIST	Anomalies and Events	3	1	2	6		No Score Yet
NIST	Detection Processes	3	3	3	9		No Score Yet

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)

<u>**Example: Critical Control 1 with a Rating of 2**</u>
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	

Assessment Results

Framework	Control Name	Rating	CySAFE Score
20 CC	Critical Control 1: Inventory of Authorized and Unauthorized Devices		**No Score Yet**
20 CC	Critical Control 2: Inventory of Authorized and Unauthorized Software		**No Score Yet**
20 CC	Critical Control 3: Secure Configurations for Hardware and Software on Mobile Devices, Laptops, Workstations, and Servers		**No Score Yet**
20 CC	Critical Control 4: Continuous Vulnerability Assessment and Remediation		**No Score Yet**
20 CC	Critical Control 5: Malware Defenses		**No Score Yet**
20 CC	Critical Control 6: Application Software Security		**No Score Yet**
20 CC	Critical Control 7: Wireless Device Control		**No Score Yet**
20 CC	Critical Control 8: Data Recovery Capability		**No Score Yet**
20 CC	Critical Control 9: Security Skills Assessment and Appropriate Training to Fill Gaps		**No Score Yet**
20 CC	Critical Control 10: Secure Configurations for Network Devices such as Firewalls, Routers, and Switches		**No Score Yet**
20 CC	Critical Control 11: Limitation and Control of Network Ports, Protocols, and Services		**No Score Yet**
20 CC	Critical Control 12: Controlled Use of Administrative Privileges		**No Score Yet**
20 CC	Critical Control 13: Boundary Defense		**No Score Yet**
20 CC	Critical Control 14: Maintenance, Monitoring, and Analysis of Audit Logs		**No Score Yet**
20 CC	Critical Control 15: Controlled Access Based on the Need to Know		**No Score Yet**
20 CC	Critical Control 16: Account Monitoring and Control		**No Score Yet**
20 CC	Critical Control 17: Data Loss Prevention		**No Score Yet**
20 CC	Critical Control 18: Incident Response and Management		**No Score Yet**
20 CC	Critical Control 19: Secure Network Engineering		**No Score Yet**
ISO	Define Scope		**No Score Yet**
ISO	Setup the Information Security Team and Approach		**No Score Yet**
ISO	Communicate Information Security Policy		**No Score Yet**
ISO	Identify Resources, Ownership and Standard Operating Procedures for IT Processes		**No Score Yet**
ISO	Complete Summary of Controls		**No Score Yet**
ISO	Define and Generate Records (evidence)		**No Score Yet**
ISO	Perform Business Management Review (if applicable)		**No Score Yet**
ISO	Conduct Internal ISMS Audits		**No Score Yet**
ISO	Measure Effectiveness of Controls		**No Score Yet**
ISO	Update Annual Planning		**No Score Yet**
ISO	Data Classification (not in the ISMS but valuable)		**No Score Yet**
NIST	Business Environment		**No Score Yet**
NIST	Governance		**No Score Yet**
NIST	Risk Management Strategy		**No Score Yet**
NIST	Maintenance		**No Score Yet**
NIST	Anomalies and Events		**No Score Yet**
NIST	Detection Processes		**No Score Yet**

Control Category and Summary

Category Summary

Framework	Control Category: Strategy/Scope	Rating	CySAFE Score
NIST	Business Environment	0	No Score Yet
NIST	Governance	0	No Score Yet
NIST	Risk Management Strategy	0	No Score Yet
ISO	Update Annual Planning	0	No Score Yet
ISO	Define Scope	0	No Score Yet
ISO	Setup the Information Security Team and Approach	0	No Score Yet
ISO	Communicate Information Security Policy	0	No Score Yet
ISO	Perform Business Management Review (if applicable)	0	No Score Yet
ISO	Complete Summary of Controls	0	No Score Yet
	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)

Framework	Control Category: Planning/Design/Configuration	Rating	CySAFE Score
ISO	Data Classification (not in the ISMS but valuable)	0	No Score Yet
ISO	Identify Resources, Ownership and Standard Operating Procedures for IT Processes	0	No Score Yet
20 CC	Critical Control 10: Secure Configurations for Network Devices such as Firewalls, Routers, and Switches	0	No Score Yet
20 CC	Critical Control 9: Security Skills Assessment and Appropriate Training to Fill Gaps	0	No Score Yet
20 CC	Critical Control 2: Inventory of Authorized and Unauthorized Software	0	No Score Yet
20 CC	Critical Control 1: Inventory of Authorized and Unauthorized Devices	0	No Score Yet
20 CC	Critical Control 19: Secure Network Engineering	0	No Score Yet
20 CC	Critical Control 3: Secure Configurations for Hardware and Software on Mobile Devices, Laptops, Workstations, and	0	No Score Yet
20 CC	Critical Control 6: Application Software Security	0	No Score Yet
	Average Rating	0.00	

Framework	Control Category: Operations	Rating	CySAFE Score
NIST	Detection Processes	0	No Score Yet
NIST	Maintenance	0	No Score Yet
20 CC	Critical Control 12: Controlled Use of Administrative Privileges	0	No Score Yet
20 CC	Critical Control 13: Boundary Defense	0	No Score Yet
20 CC	Critical Control 16: Account Monitoring and Control	0	No Score Yet
20 CC	Critical Control 15: Controlled Access Based on the Need to Know	0	No Score Yet
20 CC	Critical Control 17: Data Loss Prevention	0	No Score Yet
20 CC	Critical Control 11: Limitation and Control of Network Ports, Protocols, and Services	0	No Score Yet
20 CC	Critical Control 5: Malware Defenses	0	No Score Yet
20 CC	Critical Control 7: Wireless Device Control	0	No Score Yet
20 CC	Critical Control 4: Continuous Vulnerability Assessment and Remediation	0	No Score Yet
	Average Rating	0.00	

Framework	Control Category: Monitoring/Metrics	Rating	CySAFE Score
ISO	Measure Effectiveness of Controls	0	No Score Yet
ISO	Conduct Internal ISMS Audits	0	No Score Yet
ISO	Define and Generate Records (evidence)	0	No Score Yet

20 CC	Critical Control 14: Maintenance, Monitoring, and Analysis of Audit Logs	0	No Score Yet
	Average Rating	**0.00**	

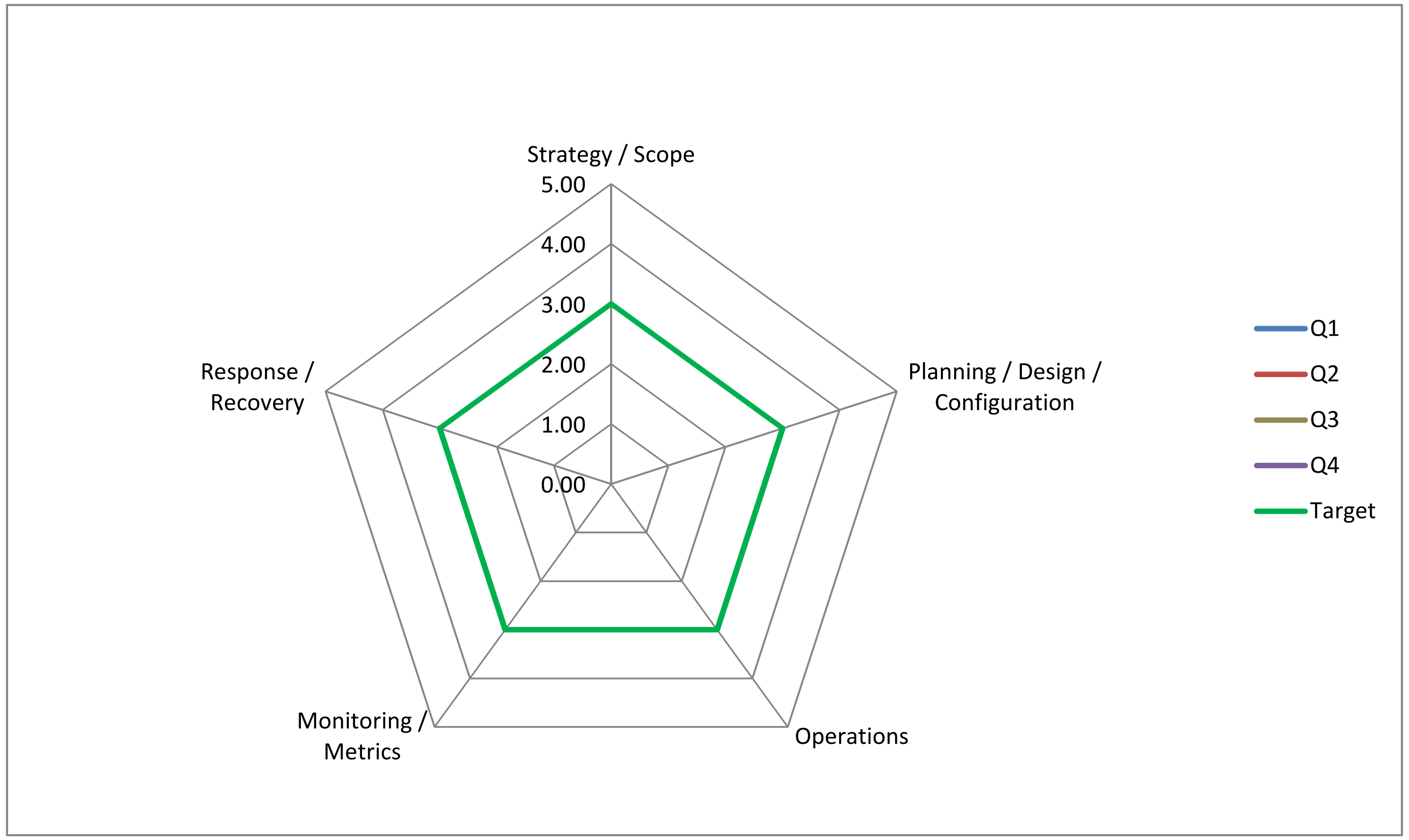
Framework	Control Category: Response/Recovery	Rating	CySAFE Score
NIST	Anomalies and Events	0	No Score Yet
20 CC	Critical Control 18: Incident Response and Management	0	No Score Yet
20 CC	Critical Control 8: Data Recovery Capability	0	No Score Yet
	Average Rating	**0.00**	

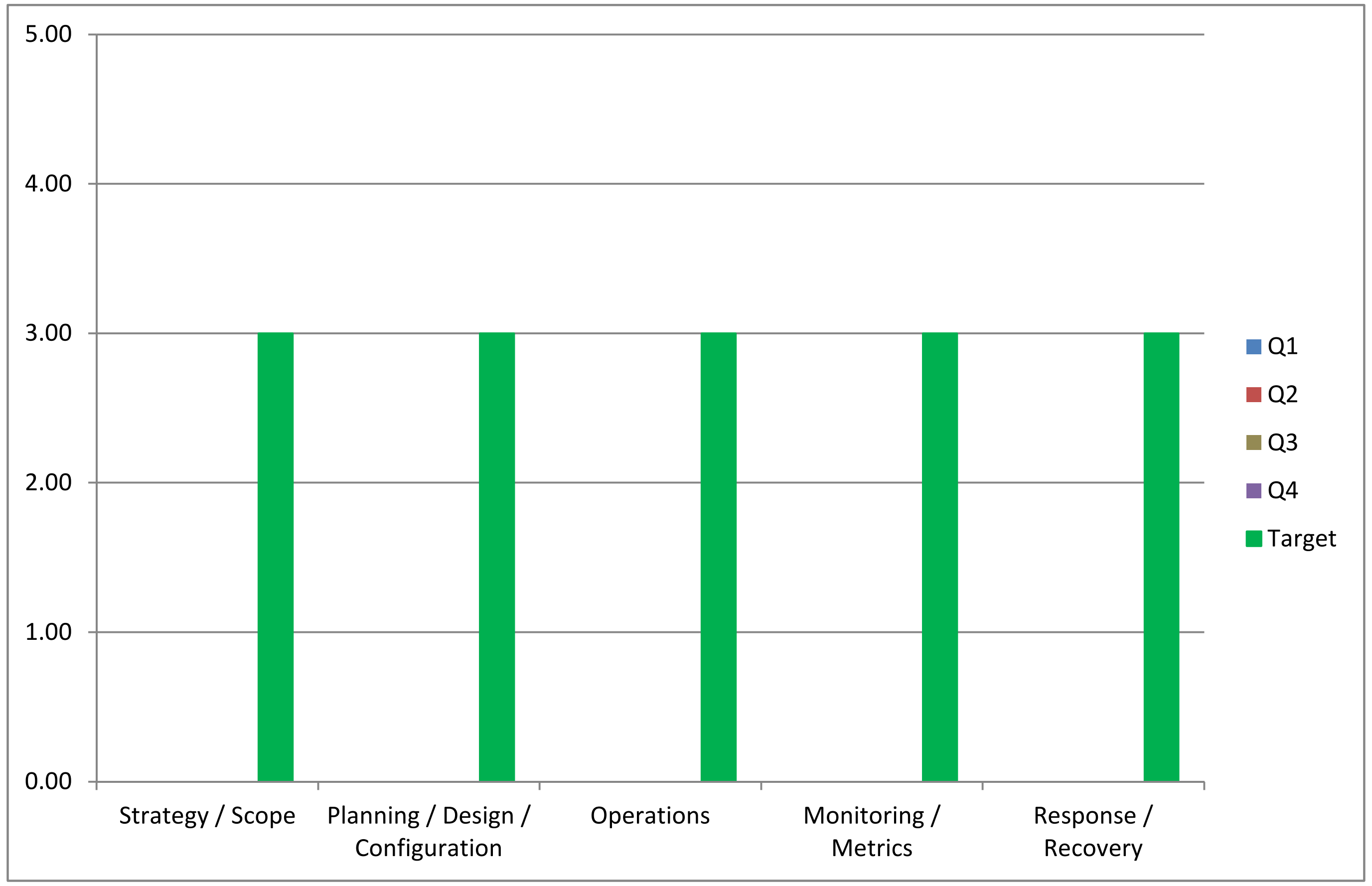
Progress Chart and Graphs

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.

Q1 ▼

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





20 Critical Controls

Control Name	Control Description	Example of Controls in Place	Basic	Cost	Time	Risk	Total
Critical Control 1: Inventory of Authorized and Unauthorized Devices	The processes and tools used to track/control/prevent/correct network access by devices (computers, network components, printers, anything with IP addresses) based on an asset inventory of which devices are allowed to connect to the network.	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	The processes and tools organizations use to track/control/prevent/correct installation and execution of software on computers based on an asset inventory of approved software.	Software inventory for servers, applications, PCs; No 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	The processes and tools organizations use to track/control/prevent/correct security weaknesses in the configurations of the hardware and software of mobile devices, laptops, workstations, and servers based on a formal configuration management and change control process.	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	The processes and tools used to detect/prevent/correct security vulnerabilities in the configurations of devices that are listed and approved in the asset inventory database.	Penetration Test Vulnerability Test Proxy Patching	Monthly Patching (OS/Browser) Vulnerability Scan (Yearly)	3	1	3	7
Critical Control 5: Malware Defenses	The processes and tools used to detect/prevent/correct installation and execution of malicious software on all devices.	PC Antivirus Anti-Matlare IPS IDS	Antivirus Malware protection	3	3	3	9
Critical Control 6: Application Software Security	The processes and tools organizations use to detect/prevent/correct security weaknesses in the development and acquisition of software applications.	SDLC QA tools / process 3rd party reviews	Many small governments do not develop applications	1	2	2	5
Critical Control 7: Wireless Device 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	Password protect Access Points Awareness of Access Don't Broadcast SSID Use more complex encryption (WPA2)	3	3	2	8
Critical Control 8: 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
Critical Control 9: Security Skills Assessment and Appropriate Training to Fill Gaps	The process and tools to make sure an organization understands the technical skill gaps within its workforce, including an integrated plan to fill the gaps through policy, training, and awareness.	User IT Security Awareness Training IT team security training (SANS or MERIT)	Organization wide awareness training	3	2	3	8

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

20 Critical Controls

Control Name	Control Description	Example of Controls in Place	Basic	Cost	Time	Risk	Total
Critical Control 10: Secure Configurations for Network Devices such as Firewalls, Routers, and Switches	The processes and tools used to track/control/prevent/correct security weaknesses in the configurations in network devices such as firewalls, routers, and switches based on formal configuration management and change control processes.	Secure Configurations for Network equipment	Secure configuration	3	2	3	8

Critical Control 11: Limitation and Control of Network Ports, Protocols, and Services	The processes and tools used to track/control/prevent/correct use of ports, protocols, and services on networked devices.	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 12: 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 13: Boundary Defense	The processes and tools used to 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 14: Maintenance, Monitoring, and Analysis of Audit Logs	The processes and tools used to detect/prevent/correct the use of systems and information based on audit logs of events that are considered significant or could impact the security of an organization.	Event Logging	Enable logging; Monitor monthly	3	3	1	7
Critical Control 15: Controlled Access Based on the Need to Know	The processes and tools used to track/control/prevent/correct secure access to information according to the formal determination of which persons, computers, and applications have a need and right to access information 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 16: Account Monitoring and Control	The processes and tools used to rack/control/prevent/correct the use of system and application accounts.	Review User Lifecycle Management System	Disable terminated accounts;
			On-board/Exit procedures;
			Process in place to periodically review of access to systems
				3	2	2	7

Critical Control 17: Data Loss Prevention	The processes and tools used to track/control/prevent/correct data transmission and storage, based on the data’s content and associated classification.	Bitlocker Disk Encryption	Bitlocker	2	2	2	6
Critical Control 18: Incident Response and Management	The process and tools to make sure an organization has a properly tested plan with appropriate trained resources for dealing with any adverse events or threats of adverse events. Note: This control has one or more sub-controls that must be validated manually.	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

ISO 27001

Control Name	Control Description	Example of Controls in Place	Basic	Cost	Time	Risk	Total
Define Scope	Has the scope of the Information Security Management System (ISMS) been defined, 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
Setup the Information Security Team and Approach	Overall Information Security responsibility; Team roles and responsibilities; Has the Information Security Management Team (ISMT) been defined and set up, including the meeting structure (ISMT agenda, ISMT minutes)?	Periodic meetings	Meetings dedicated to discussing current SECURITY threats, issues and projects	3	2	3	8
Communicate Information Security Policy	Is the Information Security Policy documented, approved and communicated 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
Identify Resources, Ownership and Standard Operating Procedures for IT Processes	Have the relevant resource owners been identified and approved 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
Complete Summary of Controls	Does the "Summary of Controls" document: (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
Define and Generate Records (evidence)	Has a list of records to provide evidence of conformity to requirements and the effective operation of the ISMS and controls including the protection requirements been 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
Perform Business Management Review (if applicable)	Has a Business Management review been conducted in the IT Service Center (ITSC) at a regular base to support ITSCs activities?	Senior Management review of Information Security Managagment System (ISMS); Do the levels of controls match the business risk?	Yearly review of control status with senior business management team.	3	1	1	5
Conduct Internal ISMS Audits	Has a procedure for internal audits been established and are internal ISMS audits conducted at planned intervals?	Audit controls to ensure control objectives are implemented	Audit controls after implementation to assess if requirements have been satisfied	3	1	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

ISO 27001

Control Name	Control Description	Example of Controls in Place	Basic	Cost	Time	Risk	Total
Measure Effectiveness of Controls	Has a procedure to measure the effectiveness of controls been implemented?	Establish control objective and measurement along with targets	Measure controls periodically to gauge effectiveness of program	3	1	2	6
Update Annual Planning	Has IT Security been considered in the 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
Data Classification (not in the ISMS but valuable)	Have you classified what type of data? Where it resides?	Create Data Classification Inventory	Classify data and where is resides and is accessed from.	3	2	3	8

NIST

Control Name	Control Description	Example of Controls in Place	Basic	Cost	Time	Risk	Total
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
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
Risk Management Strategy	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
Maintenance	Maintenance (PR.MA): Maintenance and repairs of industrial control and information system components is performed consistent with policies and procedures.	Includes the management of industrial control systems such as SCADA.	Maintenance and repairs of industrial control and information system components is performed consistent with policies and procedures.	2	2	3	7
Anomalies and Events	DE.AE-1: A baseline of network operations and expected data flows for users and systems is established and managed.	Basic network diagrams are required to ensure proper data flow. Baseline network connections and usage;	Basic network diagrams are required to ensure proper data flow.	3	1	2	6

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

Detection Processes	DE.DP-1: Roles and responsibilities for detection are well defined to ensure accountability.	Basic understanding of RACI (Responsible, Accountable, Consult, Inform) for detecting security events. There must be a clear understand of who is responsible for detect security events;	Basic understanding of RACI (Responsible, Accountable, Consult, Inform) for detecting security events.	3	3	3	9

Appendix

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 C^3 Voluntary Program	http://www.dhs.gov/about-critical-infrastructure-cyber-community-c^3-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