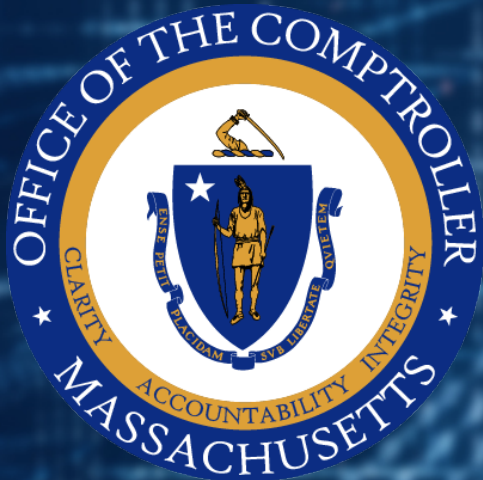


CTR CYBER

Executive Office of Technology Services and Security (EOTSS)
Enterprise Information Security Standards Self Assessment Questionnaire
Walkthrough



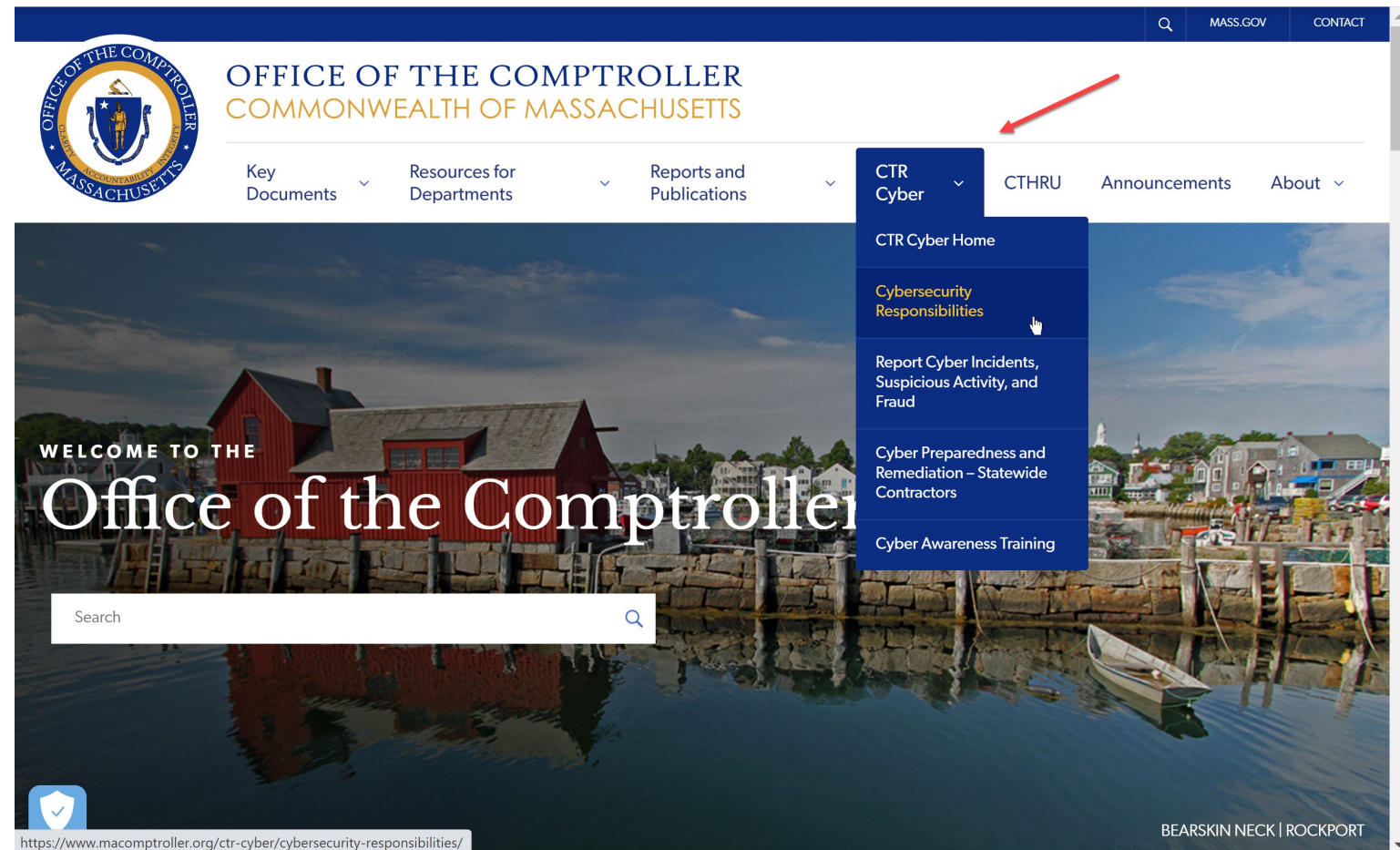
Jenny Hedderman

Risk Counsel

Office of the Comptroller

EOTSS Enterprise Information Security Standards Self Assessment Questionnaire Walkthrough

- Go to <https://www.macomptroller.org/>
- In the Navigation Bar, select “[CTR Cyber](#)”



EOTSS Enterprise Information Security Standards Self Assessment Questionnaire Walkthrough

- On the CTR Cyber page, select “[Visit page](#)” under [Cybersecurity Responsibilities for Leadership and Managers](#)



The screenshot shows the official website of the Office of the Comptroller, Commonwealth of Massachusetts. The header includes the state seal and navigation links for Key Documents, Resources for Departments, Reports and Publications, CTR Cyber, CTHRU, Announcements, and About. The main content area is titled "CTR Cyber" and describes the purpose of the CTR Cyber initiative. Below this, there are three featured sections: "Cybersecurity Tips and Alerts", "CTR Cyber 5", and "Cybersecurity Responsibilities for Leadership and Managers". The third section, "Cybersecurity Responsibilities for Leadership and Managers", is highlighted with a red arrow pointing to the "VISIT PAGE" button.

CTR Cyber

The Office of the Comptroller has developed CTR Cyber to identify key cybersecurity internal controls for Commonwealth of Massachusetts departments, and to promote cybersecurity awareness and cyber vigilance for everyone in these organizations. With increasingly sophisticated cyber attacks, everyone has a role and responsibility to help prevent disruptions and theft of Commonwealth data and resources through cyber fraud, phishing, malware, and social engineering attacks.

CYBERSECURITY TIP OF THE WEEK

Cybersecurity Tips and Alerts

CTR posts weekly Cybersecurity Tips and Alerts. Please share these updates with co-workers, especially those who continue to work remotely.

[VIEW ALERTS](#)

CTR CYBER 5

CTR Cyber 5

We are pleased to launch The Cyber 5, a series of short videos featuring cybersecurity experts from the public and private sectors.

[WATCH THE CYBER 5](#)

CYBERSECURITY RESPONSIBILITIES FOR LEADERSHIP AND MANAGERS


Cybersecurity Responsibilities for Leadership and Managers

Management is responsible for ensuring that cybersecurity internal controls are in place and tested to prevent losses and disruption from cyber incidents.

[VISIT PAGE](#)

EOTSS Enterprise Information Security Standards Self Assessment Questionnaire Walkthrough

- On this page you will find the link to the EOTSS Enterprise Security Standards by selecting “[Visit on Mass.gov](#)”. Visit this page to download the official versions of the Enterprise Security PDF versions “IS.000-IS.016”.
- On this page you can also download the “[Enterprise Information Security Standards Self Assessment Questionnaire](#)” (Excel) to help you evaluate your level of compliance.



OFFICE OF THE COMPTROLLER
COMMONWEALTH OF MASSACHUSETTS

[Key Documents](#) - [Resources for Departments](#) - [Reports and Publications](#) - [CTB Cyber](#) - [CTHRU](#) - [Announcements](#) - [About](#)

Cybersecurity Responsibilities

Key compliance information for the most common cybersecurity and data security internal control standards that leadership of Commonwealth departments is responsible for managing as part of their normal operations.

About

Department leadership and managers are responsible for establishing a “tone from the top” and assigning appropriate staff to ensure that cybersecurity internal controls are developed, tested, updated and that all staff are routinely trained to prevent operational disruption and data or financial losses due to a cyber incident.

Government financial and operational audits now evaluate data reliability and cybersecurity internal controls as a standard part of normal government operations.

Enterprise Security Standards are now included as part of a department’s Internal Controls and have compliance responsibilities at all levels of the organization.

Assign Key Staff to Ensure Cybersecurity Compliance

As part of cybersecurity preparedness, leadership and managers must assign appropriate staff at all levels of the organization to ensure compliance with required cybersecurity and data protection internal controls.

Cybersecurity internal controls require collaboration across the organization including IT, HR, Legal, Policy, Fiscal, Budget, Payroll, Program and Operations staff and extend to any contractor or 3rd party supporting operations.

INTERNAL CONTROLS SHOULD INCLUDE:

- Enterprise information security policies and standards
- Telework guidance and advisories
- Ransomware preparedness and mitigation
- Compliance obligations for business and other entities handling personally identifiable information
- Other unique data privacy standards
 - Credit card payment standards (if accepting credit cards)
 - Health care privacy (HIPAA) health and medical records
 - Protecting student privacy (FERPA)

Enterprise Information Security Policies and Standards

The Commonwealth’s default data and security standards and internal controls must be included in a Department’s Internal Control Plan, implemented, tested, and included in staff training. These standards apply to all Executive Department offices and agencies and are the default standard for non-Executive Departments who have not adopted comparable cyber and data security standards as part of their Internal Control Plan.

[VIEW ON MASS.GOV](#)

See Enterprise Information Security Policies and Standards Self Assessment Questionnaire tool below to assist in assessing your compliance with these standards.

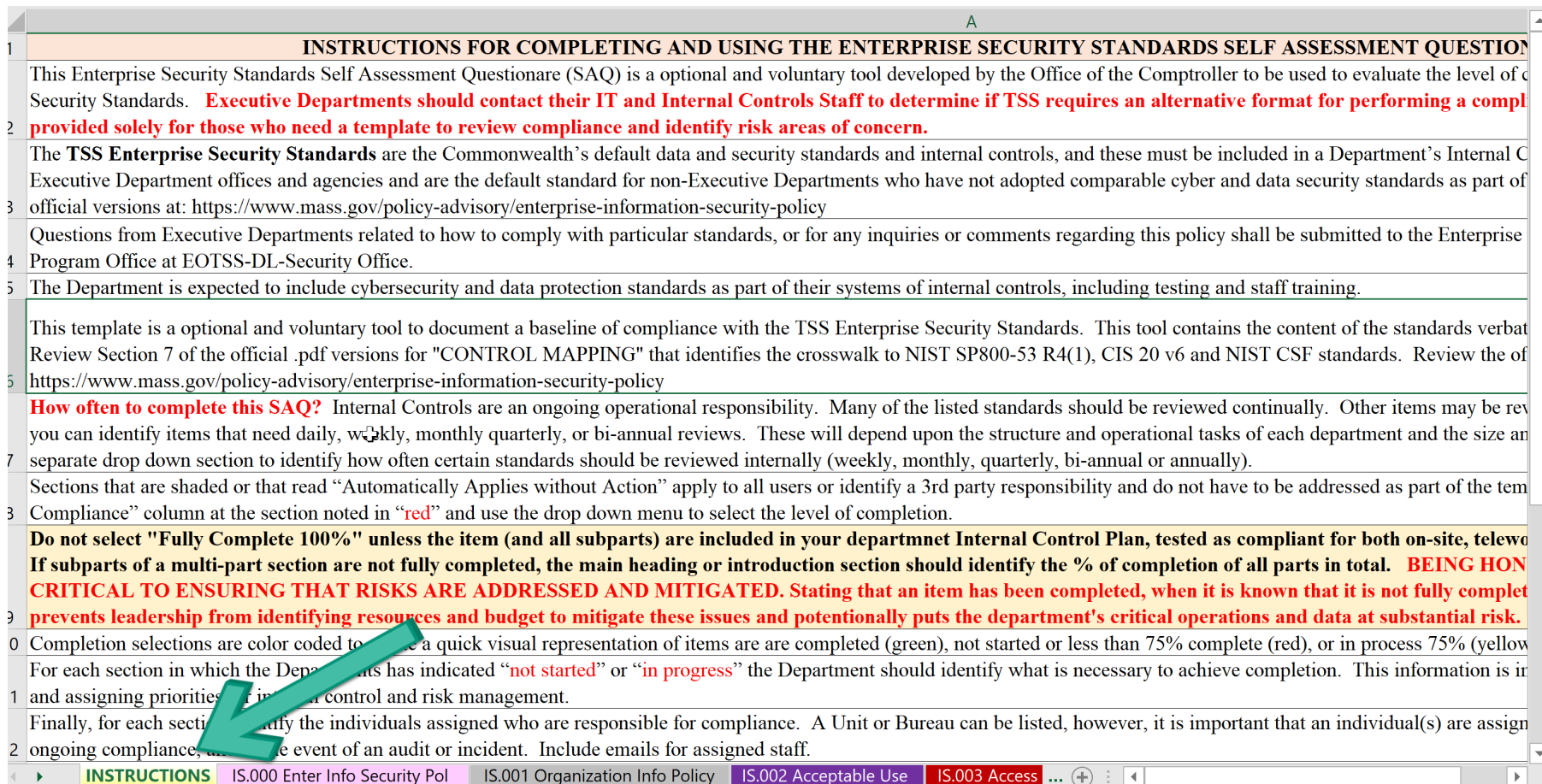
Primary Cyber and Data Security Internal Controls

The following are several tools to assist with compliance with implementation of the Enterprise Security Policies and Standards. These should be part of Commonwealth departments’ systems of internal controls.

Enterprise Information Security Standards Self Assessment Questionnaire	CTB has developed this voluntary tool to be used to evaluate the level of compliance with EOTSS Enterprise Security Standards.	VIEW EXCEL
Enterprise Information Security Standards Self Assessment Questionnaire Walkthrough	Instructions for completing the Self Assessment Questionnaire for the Enterprise Information Security Standards Self Assessment Questionnaire	VIEW PDF
Lessons Learned from Cyber Incidents	CTB has compiled lessons learned from prior cyber incidents to assist with targeting areas of weakness, and recommendations to prevent and immediate cyber events.	VIEW PDF
Template: Four Steps to Prepare for a Cybersecurity Risk Assessment	CTB has created an informational document with four steps to prepare an entity to perform a cybersecurity risk assessment that identifies and mitigates security risks.	VIEW PDF

EOTSS Enterprise Information Security Standards Self Assessment Questionnaire Walkthrough

- See the first tab for instructions for using the template



INSTRUCTIONS FOR COMPLETING AND USING THE ENTERPRISE SECURITY STANDARDS SELF ASSESSMENT QUESTIONNAIRE

This Enterprise Security Standards Self Assessment Questionnaire (SAQ) is a optional and voluntary tool developed by the Office of the Comptroller to be used to evaluate the level of compliance with the Enterprise Security Standards. **Executive Departments should contact their IT and Internal Controls Staff to determine if TSS requires an alternative format for performing a compliance assessment provided solely for those who need a template to review compliance and identify risk areas of concern.**

The **TSS Enterprise Security Standards** are the Commonwealth's default data and security standards and internal controls, and these must be included in a Department's Internal Control Plan. Executive Department offices and agencies and are the default standard for non-Executive Departments who have not adopted comparable cyber and data security standards as part of their systems of internal controls. Official versions at: <https://www.mass.gov/policy-advisory/enterprise-information-security-policy>

Questions from Executive Departments related to how to comply with particular standards, or for any inquiries or comments regarding this policy shall be submitted to the Enterprise Security Standards Program Office at EOTSS-DL-Security Office.

The Department is expected to include cybersecurity and data protection standards as part of their systems of internal controls, including testing and staff training.

This template is a optional and voluntary tool to document a baseline of compliance with the TSS Enterprise Security Standards. This tool contains the content of the standards verbatim from Review Section 7 of the official .pdf versions for "CONTROL MAPPING" that identifies the crosswalk to NIST SP800-53 R4(1), CIS 20 v6 and NIST CSF standards. Review the official versions at: <https://www.mass.gov/policy-advisory/enterprise-information-security-policy>

How often to complete this SAQ? Internal Controls are an ongoing operational responsibility. Many of the listed standards should be reviewed continually. Other items may be reviewed on a periodic basis. You can identify items that need daily, weekly, monthly quarterly, or bi-annual reviews. These will depend upon the structure and operational tasks of each department and the size and complexity of the organization. A separate drop down section to identify how often certain standards should be reviewed internally (weekly, monthly, quarterly, bi-annual or annually).

Sections that are shaded or that read "Automatically Applies without Action" apply to all users or identify a 3rd party responsibility and do not have to be addressed as part of the template. The "Compliance" column at the section noted in "red" and use the drop down menu to select the level of completion.

Do not select "Fully Complete 100%" unless the item (and all subparts) are included in your department's Internal Control Plan, tested as compliant for both on-site, telework and off-site. If subparts of a multi-part section are not fully completed, the main heading or introduction section should identify the % of completion of all parts in total. BEING HONEST IS CRITICAL TO ENSURING THAT RISKS ARE ADDRESSED AND MITIGATED. Stating that an item has been completed, when it is known that it is not fully completed prevents leadership from identifying resources and budget to mitigate these issues and potentially puts the department's critical operations and data at substantial risk.

Completion selections are color coded to provide a quick visual representation of items are completed (green), not started or less than 75% complete (red), or in process 75% (yellow).

For each section in which the Department has indicated "not started" or "in progress" the Department should identify what is necessary to achieve completion. This information is used for assigning priorities for internal control and risk management.

Finally, for each section identify the individuals assigned who are responsible for compliance. A Unit or Bureau can be listed, however, it is important that an individual(s) are assigned to ensure ongoing compliance, and in the event of an audit or incident. Include emails for assigned staff.

INSTRUCTIONS IS.000 Enter Info Security Pol IS.001 Organization Info Policy IS.002 Acceptable Use IS.003 Access ...

EOTSS Enterprise Information Security Standards Self Assessment Questionnaire Walkthrough

- This Enterprise Security Standards Self Assessment Questionnaire is an optional and voluntary tool developed by the Office of the Comptroller to be used to evaluate the level of compliance with the EOTSS Enterprise Security Standards.
- **Executive Departments should contact their IT and Internal Controls Staff to determine if EOTSS requires an alternative format for performing a compliance review.** This tool is optional and provided solely for those who need a template to review compliance and identify risk areas of concern.
- The EOTSS Enterprise Security Standards are the Commonwealth's default data and security standards and internal controls, and these must be included in a Department's Internal Control Plan.
- These standards apply to all Executive Department offices and agencies and are the default standard for non-Executive Departments who have not adopted comparable cyber and data security standards as part of their Internal Control Plan.
- Review the official versions at: <https://www.mass.gov/policy-advisory/enterprise-information-security-policy>

EOTSS Enterprise Information Security Standards Self Assessment Questionnaire Walkthrough

- Questions from Executive Departments related to how to comply with particular standards, or for any inquiries or comments regarding this policy should be submitted to the Enterprise Security Office by contacting the Security Program Office at EOTSS-DL-Security Office@mass.gov.
- The Department is expected to include cybersecurity and data protection standards as part of their systems of internal controls, including testing and staff training.
- This template is an optional and voluntary tool to document a baseline of compliance with the TSS Enterprise Security Standards. This tool contains the content of the standards verbatim as these appear in the PDF versions.
- Review Section 7 of the official PDF versions for "CONTROL MAPPING" that identifies the crosswalk to NIST SP800-53 R4(1), CIS 20 v6 and NIST CSF standards. Review the official versions at: <https://www.mass.gov/policy-advisory/enterprise-information-security-policy>

EOTSS Enterprise Information Security Standards Self Assessment Questionnaire Walkthrough

- Do not select "Fully Complete 100%" unless the item (and all subparts) are included in your department Internal Control Plan, tested as compliant for both on-site, teleworking and 3rd parties and staff are trained.
- If subparts of a multi-part section are not fully completed, the main heading or introduction section should identify the % of completion of all parts in total.
- **BEING HONEST IN THE SELECTIONS IS CRITICAL TO ENSURING THAT RISKS ARE ADDRESSED AND MITIGATED.**
- Stating that an item has been fully 100% completed, when it is known that it is not fully completed, misrepresents the state of security and prevents leadership from identifying resources and budget to mitigate these issues and potentially puts the department's critical operations and data at substantial risk.

EOTSS Enterprise Information Security Standards Self Assessment Questionnaire Walkthrough

Sections that are shaded or that read “Automatically Applies without action” apply to all users or identifies a 3rd party responsibility and do not have to be addressed as part of the template. Users will start under “Select Level of Completion” column at the section noted in “red” and use the drop-down menu to select the level of completion.

	A	B	C	
1		ENTERPRISE SECURITY STANDARDS SELF ASSESSMENT QUESTIONNAIRE. FOR EACH LIS		
2	Section #	ENTERPRISE SECURITY STANDARDS IS.002 Acceptable Use of Information Technology Policy https://www.mass.gov/policy-advisory/acceptable-use-of-information-technology-policy	Select Level of Completion from the drop down menu that appears in *unshaded cells Under " Policy Statements "	Description of achieved or what
20	IS.002.6.1.3.	Job-specific: Commonwealth agencies may have some job functions that require additional information security training. The agency will provide the additional training requirements as needed. Examples may include personnel who have access to systems that store confidential information or job responsibilities such as Developers and database Administrators. The Commonwealth CISO determines the job functions that require additional training.		
21	IS.002.6.1.4.	A quarterly training report will be sent to the Enterprise Security Office to track overall completion rates.	Fully Completed 100% Standard Not Applicable Not Started In Process - 25% In Process - 50% In Process - 75%	
22	IS.002.6.2	Acceptable Use of Information Assets: The Commonwealth's information assets further organizational goals and priorities. In using the Commonwealth's information assets, Commonwealth Executive Offices and Agencies should encourage their personnel to act in a professional and ethical manner and comply with their applicable Code of Conduct, relevant enterprise, and agency-level policies and/or applicable contractual obligations.		

EOTSS Enterprise Information Security Standards Self Assessment Questionnaire Walkthrough

Do not select “Fully Complete 100%” unless the item (and all subparts) are included in Internal Control Plan, tested as compliant for both on-site, teleworking and 3rd parties and staff are trained. If subparts of a multi-part section are not fully completed, the main heading or introduction section should identify the % of completion of all parts in total.

1	ENTERPRISE SECURITY STANDARDS SELF ASSESSMENT QUESTIONNAIRE. FOR EACH LISTED STANDARD			
2	Section #	ENTERPRISE SECURITY STANDARDS IS.016 Vulnerability Management Standard (https://www.mass.gov/advisory/vulnerability-management-standard)	Select Level of Completion from the drop down menu that appears in *unshaded cells Under STANDARD STATEMENTS.	Description of How this requirement is achieved or what has been completed process
17	IS.016.6.1	Vulnerability Management. Processes to identify, classify and remediate vulnerabilities across all technology environments and platforms to reduce the Commonwealth's exposure to cyber threats must be documented.		
18	IS.016.6.1.1	Establish a vulnerability and patch management process to:		Level of Completion Do Not select "Fully Complete 100%" unless the item (and all subparts) are included in your Internal Control Plan, tested as compliant for both on-site, teleworking and 3rd parties, and staff are trained.
19	IS.016.6.1.1.1	Ensure information systems are patched in a timely manner.		
20	IS.016.6.1.1.2	Ensure that the patch management process and cadence is consistent with the recommendation of patch providers.		
21	IS.016.6.1.1.3	Reduce the number of service disruptions, incidents and problems caused by vulnerabilities.		
22	IS.016.6.1.1.4	Provide a defined, repeatable method for ensuring consistent execution of associated patch management activities and tasks.		
23	IS.016.6.1.1.5	Provide clarity around stakeholder/participant roles and responsibilities.		
		Enable key performance metrics to be captured for performance		

EOTSS Enterprise Information Security Standards Self Assessment Questionnaire Walkthrough

Completion selections are color coded to create a quick visual representation of items are completed (green), not started or less than 75% complete (red), or in process 75% (yellow).

	A	B	C	D	
1	ENTERPRISE SECURITY STANDARDS SELF ASSESSMENT QUESTIONNAIRE. FOR EACH LISTED STANDARD COMPLETE INFORMATION				
2	Section #	ENTERPRISE SECURITY STANDARDS	Select Level of Completion from the drop down menu that appears in *unshaded cells Under "Policy Statements"	Description of How this requirement is being achieved or what has been completed if in process	Location : that outlines document
81	IS.002.6.4.1.1.	Authorization: Users must have an active user ID to access information assets on the Commonwealth family of networks.	Fully Completed 100%		
82	IS.002.6.4.1.2.	Authentication: Information assets that access or store confidential information must authenticate a user's identity (e.g., password) prior to granting access.	Standard Not Applicable		
83	IS.002.6.4.1.3.	Access requests: Users must request access to technology infrastructure and/or applications required for job responsibilities using the Commonwealth-approved access request tools.	In Process - 25%		
84	IS.002.6.4.1.4.	Least privilege: Users must not be granted access to technology infrastructure and/or applications that are not required to perform his/her job responsibilities. Managers are responsible for ensuring their direct reports have the appropriate access to systems.	In Process - 50%		
85	IS.002.6.4.1.5.	Reviews of user's access to applications and/or technology infrastructure will be performed by Managers at least annually to ensure access is appropriate to perform his/her job responsibilities.	In Process - 75%		
86	IS.002.6.4.1.6.	Segregation of duties: Users must not be granted access to information assets that would allow entitlements to perform job responsibilities that are not compatible with each other (e.g., having the ability to both request and approve a change).	In Process - 50%		

EOTSS Enterprise Information Security Standards Self Assessment Questionnaire Walkthrough

For each section, departments should describe briefly how this requirement is being achieved or what has been completed if in process and document the location and title of internal control documents that outline in detail all supporting information documenting completion or progress to completion. This information is helpful for audit and risk assessment purposes.

	D	E	
	ASSESSMENT FOR EACH LISTED STANDARD COMPLETE INFORMATION (IN THE UNSHADED CELLS) TO		
	Description of How this requirement is being achieved or what has been completed if in process	Location and title of internal control documents that outline in detail all supporting information documenting completion or progress to completion	If necessary
RDS			
o access of networks.			
ore identity			
nology			
l access			
o technology red to			
available			

For each section in which the department has indicated “not started” or “in progress” the department should identify what is necessary to achieve completion. This information is important for budgeting, resource management and assigning priorities for internal control and risk management.

[illegible]

A Unit or Bureau can be listed. However, it is important that an individual(s) are assigned to manage and monitor completion and ongoing compliance. Include emails for assigned staff.

[illegible]



What does a department do with a completed Self Assessment Questionnaire for EOTSS Enterprise Information Security Standards?

How often should this Self Assessment Questionnaire be completed?

- Internal Controls are an ongoing operational responsibility. Many of the listed standards should be reviewed continually.
- Other items may be reviewed annually. As you complete the Self Assessment Questionnaire you can identify items that need daily, weekly, monthly quarterly, or bi-annual reviews.
- These will depend upon the structure and operational tasks of each department and the size and complexity of your department.
- There is a separate drop-down section to identify how often certain standards should be reviewed internally (weekly, monthly, quarterly, bi-annual or annually).

EOTSS Enterprise Information Security Standards Self Assessment Questionnaire Walkthrough

For each section identify how often the standard needs to be reviewed by staff for compliance. High Risk items may warrant more regular review. Other items may only require annual review. Items are color coded to create a quick visual representation of high risk items in red and yellow.

H	I	J	K
	How Often should compliance of this section be reviewed by Department staff? High Risk items may warrant more regular review. Other items may only require annual review (Select Drop Down Menu)	NOTES AND COMMENTS	
Contact mail of responsible individual(s)			
	Highest Risk - Weekly Review		
	High Risk - Monthly Review		
	Medium-High Risk - Quarterly Review		
	Moderate Risk - bi-annual Review		
	Annual Internal Controls - Annual Review		

EOTSS Enterprise Information Security Standards Self Assessment Questionnaire Walkthrough

- The Self Assessment Questionnaire is not an assignment to be turned in to an authority like homework. Instead, the Self Assessment Questionnaire is a useful tool to be used by a Department internally (and assigned contractors) to provide:
 - **Compliance Level.** Assists departments gauge the level of compliance with required Enterprise Security Standards and to identify for leadership the items that need attention, resources and budgeting
 - **Risk Assessment Baseline.** Provides a baseline structure to perform a Cybersecurity Risk Assessment to evaluate the risks, likelihood, potential impact and mitigating controls that are in place, or that need to be in place to mitigate these risks. Note that risk assessments are required under Internal Controls requirements and under the EOTSS Enterprise Security Standard IS.010.
 - **Incident Response Baseline.** Provides a baseline structure to investigate an incident in the event a cyber or other security incident has happened. 3rd parties often request compliance questionnaires when investigating an incident.
 - **Audit Review Baseline.** Provides documentation for an audit, either operational or information technology, to identify the level of internal control compliance.



What does a department do with a completed Self Assessment Questionnaire for EOTSS Enterprise Information Security Standards?

When the Self Assessment Questionnaire is completed, it should be reviewed by:

- Leadership
- Management
- Fiscal staff
- Internal control staff
- Legal staff
- Operational staff

to discuss the key risk areas, remediation strategies and required updates to internal controls, and operations to achieve or sustain compliance.

Thank you!

For more information on Cybersecurity Internal Controls check out macomptroller.org/ctr-cyber