Discovering the TAC 202 Information Security Standard

This PathMaker Group white paper describes the subject matter within the standard and purpose of each area of measurement.

Ryker Exum

PATHMAKER GROUP

Introduction

The TAC 202 is a freely available security standards framework that can be adapted and applied in many different types of organizations looking for guidance for securing their environment. There are essentially two different variants of the standard. The first is focused on Texas state agencies while the second covers guidance for Texas State Universities. For these two targets, the standard is a requirement. However, it can be applied to a diverse set of environment with a little adaptation. While the TAC 202 would not be considered the definitive security standard for securing your environment unless required, it can represent a great foundation toward building or enhancing your security program.

The Texas Administrative Code Title 1, Part 10, Chapter 202 (TAC 202 for short) is administered by the Texas Department of Information Resources and can be found free of charge through the Texas Secretary of State's website. As you look through the link standard, you will find the TAC 202 covers the basic terms, definitions, and two groups of subsections focused on either a Texas state agency or a Texas Institution of Higher Education. The definitions for the standard can be found in §202.1-3. The coverage for Texas state agencies will be outlined in §202.20-28. The code for higher education will be outlined in §202.70-78. If you review the two sections you will find that they are very similar. You will find minor changes in wording throughout the document to adapt for the two different target audiences. (State agency vs. institution of higher education) If you are using this standard outside of these two targets, you can quickly adapt the standard to your environment using a simple find and replace and disregarding a few of the line items within.

Application

One of the key advantages of the TAC 202 is this body of guidance is freely open in its entirety. Many of the enterprise security standards like the ISO27002 or COBIT are behind a paywall which prevents ease of access. If you have spent some time working with the major frameworks, you will notice some similarities in coverage without the cost. This makes the TAC202 a great guidance option for developing an information security program in community colleges and K-12 environments for example. This can also easily work for school systems and government agencies outside of Texas which may not have well developed guidance to work from yet. This standard also prevents the need for sifting through the very extensive NIST 800 series documentation to find areas to apply in your specific environment. The TAC 202 has been specifically targeted for the needs of a government body or education system.

Content

Only a limited amount of information on this standard can be found from third party sources other than the actual standard itself. The following content will work through the different areas of the standard to enhance the common knowledge around this standard. The Texas Administrative Code chapter 202 is comprised of nine sections, listed as follows:

1. Security Standards Policy
2. Management and Staff Responsibilities
3. Managing Security Risks
4. Managing Physical Security
5. Business Continuity Planning
6. Information Resources Security Safeguards
7. Security Incidents
8. User Security Practices
9. Removal of Data from Data Processing Equipment

Copyright © 2013 PathMaker Group

SECTION ONE (Security Standards Policy) is very straightforward. It is a high-level policy that should be implemented in your environment to provide some high level guidance regarding information security concerns. There are eight line items in this section and together create a core policy which address different forms confidentiality, integrity, availability, authorization, and accountability. In the information security world these policies address components of the CIA triad and AAA.

SECTION TWO (Management and Staff Responsibilities) begins the process of defining roles and responsibilities within the information security program. This area will help you understand how you should be breaking down approval processes, assigning roles and responsibilities, establish a review schedule, and understand the related terms which are commonly found in this area. You will get an understanding between the different roles such as an information owner or custodian and what their areas of responsibility will be in your environment. "One of the most important reasons to document role and responsibility assignments is to demonstrate top management support."[1] Assignment of roles and responsibilities will be critical to your security programs success!

SECTION THREE (Managing Security Risks) helps to outline the process for performing a risk assessment within your environment and how to rank the findings. It should be noted that a risk assessment can be a time-consuming process but it is an essential step to identifying where risks exist in your environment that should be addressed. A risk assessment is a standard component in any business continuity plan (BCP). The process of identifying risks may be more easily completed when preceded by a business impact analysis (BIA).

"A BIA predicts the consequences of disruption of a business function and process and gathers information needed to develop recovery strategies."[2] A business impact analysis will be used to prioritize the criticality of the different areas of your business, school, or government agency. This criticality evaluation will absolutely assist in assigning risk levels and move through the process more effectively.

In SECTION FOUR (Managing Physical Security) details the development of a proper physical security program. Protecting your critical assets is of obvious importance and security measures should be properly planned and reviewed. If your perimeter security can be defeated by walking through a propped open door to the server room, your security has failed and your systems could be compromised. Other key areas as environmental risks, development of emergency procedures, and building in a review process should all be addressed as you work through section 4.

SECTION FIVE walks through the subject of Business Continuity Planning. In this section you are just filling in the gaps not previously addressed in section three by adding the third main component of a BCP, a disaster recovery plan. (DRP) This section will outline how you plan to handle a severe outage that lasts more than just a few hours or day. These commonly are useful during hurricanes, floods, earthquakes, etc. Development of a DRP is dependent on your already identified asset criticality and associated risks. These details will help create a step-by-step plan for ensuring critical systems can be restored in order of importance. Throughout DRP process you should be conducting tabletop exercises as you develop content to ensure they are effective and cover the necessary information. Will the process you have on paper work in a perfect

[1] Wood, C. (2013, 05). *The Importance of Defining and Documenting Information Security Roles and Responsibilities.* Retrieved from http://www.informationshield.com/: http://www.informationshield.com/papers/SecurityRolesAndResponsibilities.pdf

[2] FEMA. (2013, 05). BUSINESS IMPACT ANALYSIS. Retrieved from Ready.Gov: http://www.ready.gov/business-impact-analysis

Copyright © 2013 PathMaker Group

world only? What if the disaster causes you to lose access to major utilities for an extended period of time? What if your most experienced staff member cannot be reached due to widespread communication outage? Will your plan succeed?

If you are a medium-size community college, consider this scenario. The community college is staffed by 20 IT personnel plus a department manager. The college has two single-building campuses and a datacenter located in the primary facility. The sites are connected via a single P2P connection. The datacenter is powered via UPS systems housed in the basement of the building. The school is in a hurricane prone zone. All telecommunications run through the same room as the UPS systems, including the schools EAS system. Wireless is provided to staff and students and is on the same local LAN as the workstations and printers in the school. Servers are administered by IT staff via RDP. Desktops have a quarterly patch cycle.

Using this quick scenario, you should be able to start picking out areas with a higher criticality than others. You will begin to think, what is more critical to business operations and must be more heavily protected or corrected before an incident to reduce the potential impact? This is the basic thought process for a BIA. Also, as you begin to rank these different items by priority, consider incorporating recovery point and time objectives (RPO & RTO) into each line item. Essentially these measures detail acceptable downtime and the maximum allowed time to restore functionality.

With this information in hand, will it be easier to perform an annual risk assessment in your environment? Absolutely. It will become quickly apparent that the legwork that has been performed in the BIA process has just saved time and potential confusion during the risk assessment process. Once you have identified areas in which your business can be impacted as well as their associated risks, you can then strategize the disaster recovery process. It is recommended to work through the BCP in order as outlined in the TAC 202. As you develop your BCP you will gain an understanding of:

- What components of your business are the most essential to survival
- How long you think the business could survive an outage
- How long can critical systems be down before a serious business impact occurs and causes a serious financial impact

Information Resources Security Safeguards are covered in SECTION SIX of the TAC202. Sections 5 and 6 will more than likely be the two sections that consume most of your TAC 202 adoption time. This section is about protecting data from unauthorized persons. This includes data protection mechanisms like AAA, encryption, storage, network design, security integration with the SDLC, and proper set of security policies. You will notice that this section is mostly comprised of policy development requirements. This area assists users in identifying the necessary foundation to develop the security documentation within their environment. The policies, once approved by senior management, will give you the support necessary to fund the development of your security program. Depending on the way the policies are worded, they may also have some “teeth” for enforcement. What normally makes section six so time-consuming is the time spent writing the necessary policies and going through the approval process. If you have never written a security policy or lack the resources to perform this internally, please get in touch as our experienced consultants can assist in the development and ensuring proper coverage. Reviews can also be performed to ensure existing policies contain the proper content.

Requirements around security incidents makes up SECTION SEVEN. This section is mostly comprised of subjects which fall into digital forensics and incident response or DIFR in short. Section 7 will help you define how you plan to handle the unexpected. Will you report criminal offenses to local law enforcement? Who in the

Copyright © 2013 PathMaker Group

chain of command should an incident be reported to? An incident can be something as small as a damaged set of backup tapes or as large as a 0-day exploit against the primary domain controller. Guidance should be developed to help administrators know the proper actions to take and whom to inform.

User security practices are outlined in SECTION EIGHT. This section should be fairly easy to work through with the right knowledge and resources. Users will be required to acknowledge they will abide by your policies via a method of your choosing. Any publically available kiosks should be heavily restricted from unauthorized access. NDAs should be developed and used where appropriate in your environment. Also, one of the most consistently missed areas of information security, user awareness training should be developed. Many of the recently successful attacks PathMaker Group consultants have seen against companies with reasonable levels of security have been through user phishing attacks. Do your users know if the email receipt that just came in from FedEx with an EXE extension is really a receipt? If you have a well-developed and deployed user awareness training program they should know something is wrong in a heartbeat. PathMaker Group has successfully worked with our clients to develop customized training materials for their staff. We can also recommend additional resources you can leverage for long term success.

The final section, Removal of Data from Data Processing Equipment, makes up SECTION NINE. This section should be the easiest to address as it deals with the destruction and disposal of data. Are you properly wiping you data from disk? Are your system administrators supposed to be running all drives through a degaussing machine before final destruction? You will also find guidance on what type of documentation should be created during the destruction of records and storage media.

End Notes

We hope that you have found some useful insight into what makes up the Texas Administrative Code Chapter 202 and how it can benefit your organization. It is obviously targeted in its original form, but it can be adapted to fit your needs in the process of building a robust information security program. We recommend that all sections be appropriately covered even though you may not be actually required to implement the TAC 202.

It is important to mention that our team at PathMaker Group is here to assist you in the development of your information security program from end-to-end. From simple policy and procedure development to a full assessment and/or remediation of discovered issues, our team of certified industry experts will help you succeed. If you would like to schedule a call to discuss how the TAC 202 or other information security standard can have a positive impact on your environment, simply submit the form on our contact us page or give us a call!

About PathMaker Group

PathMaker Group is a specialized Identity and Security Management consultancy, blending core technical and product expertise, consultative know-how and extensive implementation experience. Driven by your unique business, compliance requirements and specific environment, we help you assess, plan, select, and integrate the right mix of products and solutions to optimize and secure your business IT, reduce your project risk, and maximize performance. We provide complete solutions by blending software, hardware, managed service solutions, professional services, and customized training. We work to leverage your investments by integrating new solutions with your current products. PathMaker Group is headquartered near Fort Worth, Texas and can be reached at (817) 704-3644 or online at www.pathmaker-group.com.

Copyright © 2013 PathMaker Group