

Texas Administrative Code Ch. 202

WEDNESDAY, JULY 23, 2014 |

AUSTIN, TEXAS

TAC 202 Historical Perspective

- Previous to TAC 202, TAC 201.13 defined state security standards
- TAC 202 was originally proposed, drafted and published between 2002 and 2003
- Amended to include Higher Education Subchapter in November 2004
- Amended to address wireless technology in April 2006
- Amended to address firewalls, encryption and incident management in September 2009
- Amended to address encryption standards in June 2012

Subject to review every 4 years with no substantial changes since 2004

Technology in the New Millennium

- **2001 – Wikipedia and the iPod were launched**
- **2003 – Apple’s iTunes debut**
- **2003 – SQL Slammer Worm affected over 75K hosts within 10 min.**
- **2004 – Google IPO and the first 1 gigabyte SD Card was released**
- **2004 – T-Mobile had a Christmas launch of 3G mobile data service**
- **2004 – Broadband Internet access outpaced dial-up for the first time**
- **2004 – Facebook is launched**
- **2005 – USB flash drives replaced floppy disks**
- **2005 – YouTube is launched**
- **2006 – Twitter is launched**

Pros of current TAC 202

PROS

- **Sets a standard for the entire state**
- **Establishes a baseline of minimum security**
- **Organized to address differences between Higher Education and State Agencies**
- **As a rule, it is stronger than a policy**

Cons of current TAC 202

CONS

- **Easy to read structure makes defining technical requirements difficult**
- **As a rule as opposed to policy it is more cumbersome to modify**
- **Sections make consistency difficult when defining controls – creates interpretation gaps**
- **Structure blends people, process and technology roles that can create confusion and complexity**
- **Minimum security baseline has been eclipsed by increased risk and threats, as well as external requirements**

Drivers for Change

- **Doesn't address newer technologies**
- **Addresses some organizational controls,**
 - But places business functions within IT (Business Continuity Planning, Risk Acceptance)
- **Lacks many managerial controls (Process)**
- **Overly vague in many technical controls (Technology)**
- **Technical controls do not consider evolved technology**
 - Cloud, Mobile, Social Media



Information Security Program

TAC 202 Timeline



• Milestones

- July: Draft rule and Security Control Standards submitted to ITCHE for review and comment
- October: Draft rule and Security Control Standards submitted to the DIR board
- February 2015: Earliest possible adoption of new rule

SISAC Policy Sub-committee Membership

Member	Organization	Represents
Ken Palmquist	DIR	Article 1 (General Government)
Ed Tjarks	Texas Comptroller of Public Accounts	Article 1 (General Government)
Khatija Syeda	Health and Human	Article 2 (Health & Human Services)
Fred Lawson	Health and Human	Article 2 (Health & Human Services)
Darrell Bateman	Texas Tech University	Article 3 (Education)
Jeff McCabe	Texas A&M	Article 3 (Education)
Danny Miller	Texas A&M	Article 3 (Education)
John Skaarup	Texas Education Agency	Article 3 (Education)
Jana Chvatal	University of Houston	Article 3 (Education)
Miguel Soldi	University of Texas System	Article 3 (Education)
Richard Morse	Office of Court Administration	Article 4 (Judiciary)
Alan Ferretti	Texas Department of Public Safety	Article 5 (Public Safety & Criminal Justice)
Miguel Scott	Texas Department of Public Safety	Article 5 (Public Safety & Criminal Justice)
Angela Gower	Texas Department of Agriculture	Article 6 (Natural Resources)
Joshua Kuntz	Department of Motor Vehicles	Article 7 (Business and Economic Development)
Clarence Campbell	Texas Department of Licensing and Regulation	Article 8 (Regulatory)
Chad Lersch	DIR	General Counsel
Lon Bernquist	DIR	Policy
Christian Byrnes	Gartner	Private Sector
Mike Wyatt	Deloitte	Private Sector

SISAC Policy Subcommittee Process

- **Monthly meeting moved to bi-monthly**
- **Facilitated discussion, review and revision process**
- **Spirited debates with consensus results**
- **Broad representation provided critical insights**
- **Many thanks to the contributions and efforts of the group**
- **Provides a great forum for the ongoing review and revisions needed to continue to approach touch issues**

Legacy TAC

Legacy TAC 202
Applicable Terms and Technologies for Information Security
Institution of Higher Education
State Agency
Management and Staff Responsibilities
Security Incidents
Security Standards Policy
Managing Security Risks
Managing Physical Security
Business Continuity Planning
Information Resources Security Safeguards
User Security Practices
Removal of Data from Data Processing Equipment

- **Controls integrated into the rule itself**
- **Roles and responsibilities are intermingled with technical details**
- **Requirements are defined but not clearly specified**

FISMA

- **Focused on roles and responsibilities**
- **Controls are incorporated through NIST SP 800-53**
- **Enables controls to be more nimble**
- **Four updates since 2005**



Revisions to Federal rules

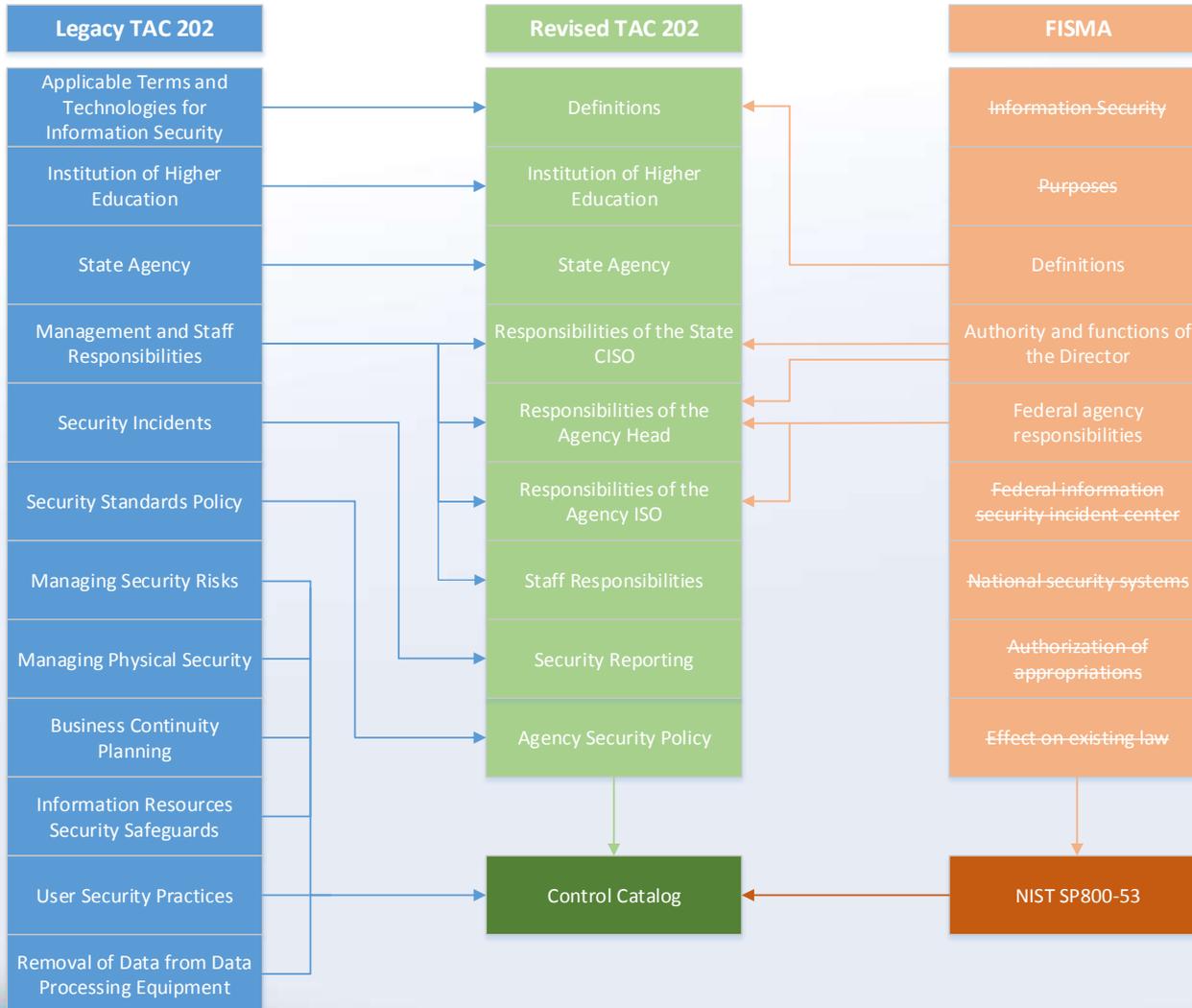
- **FISMA**

- Passed in 2002
- Amended in 2014

- **SP 800-53**

- Rev 1: Feb 2005
- Rev 2: Dec 2007
- Rev 3: Aug 2009
- Rev 4: Apr 2013

Moving TAC toward FISMA



Texas Administrative Code § 202

- **Definitions**
- **Institution of Higher Education**
- **State Agency**
- **Responsibilities of the State's Chief Information Security Officer**
- **Responsibilities of the Agency Head**
- **Responsibilities of the Information Security Officer**
- **Staff Responsibilities**
- **Security Reporting**
- **Agency Information Security Program**
- **Managing Security Risks**
- **Security Control Standards**

Security Control Standards

- Uses NIST SP800-53 nomenclature
- Provides control information
- Developed to provide for a state, agency, and departmental implementation

Group ID	[NIST Domain Name abbreviation, e.g. 'AC' for Access Control, 'AT' for Awareness and Training, etc...]			
Group Title	[Unabbreviated NIST control family description, e.g. 'Access Control']			
Control ID	[NIST 800-53 Rev. 4 Control (MOD) control number in sequence as applicable, e.g. 'AC-1']			
Control Title	[NIST 800-53 Rev. 4 Control (MOD) control name, e.g. 'Access Control Policy and Procedures']			
Risk Statement	[A high level statement of the potential risk present by not addressing the control activity]			
Priority / Baseline	P1	LOW – No	MOD – Yes	HIGH – Yes
Required Date	[Date which requirement will become effective. Note: Only "Low" baseline controls are mandatory for all systems. Other controls may be applicable based on the state organization risk assessment]			
Control Description	[Detailed NIST 800-53 Rev. 4 Control (MOD) control description]			
Implementation	State	[The State level requirements for the implementation of information security controls]		
	State organization	[To be determined for each state organization; To include organization specific components as applicable, e.g. if an organization has a specific mapping requirement under the Health Insurance Portability and Accountability Act (HIPAA); or other applicable regulatory driver) this relative control could be included here]		
	Compartment	[To be determined for each state organization; To include organization specific compartment or divisional level components as applicable, e.g. if an organization's department has a specific requirement under HIPAA, as an example, this relative control could be included here]		
Example	[This section includes example only considerations of how the control identified above may be applicable in a state organization security environment]			

Comprehensive Crosswalk

- Texas Cybersecurity Framework
- TAC202
- NIST 800-53 Rev. 4
- NIST Cybersecurity Framework (EO 13636)
- COBIT
- SANS 'Twenty Critical' Controls
- IRS Publication 1075
- CJIS Security Policy
- HIPAA Security
- FERPA
- Privacy Act of 1974
- Computer Fraud and Abuse Act of 1986
- Gramm-Leach-Bliley Act of 1999 (GLBA)
- Computer Security Act of 1987
- PCI DSS v2.0
- The Children's Internet Protection Act of 2000 (CIPA)
- The Children's Online Privacy Protection Rule of 2000 (COPPA)
- TX Business and Commerce Code, Ch. 503
- TX Business and Commerce Code, Ch. 521
- Texas Government Code, Chapter 2054 (Information Resources)
- Texas Health and Safety Code, Chapter 181 (Medical Records Privacy)
- Texas Health and Safety Code, Chapter 611 (Mental Health Records)
- Texas Government Code Chapter 552 (Public Information)
- Texas Occupations Code, Chapter 159 (Physician-Patient Communication)
- Texas Penal Code, Title 7, Chapter 33 (Computer Crimes)

Security Control Standards

- Uses NIST SP800-53 nomenclature
- Provides control information
- Developed to provide for a state, agency, and departmental implementation

Group ID	[NIST Domain Name abbreviation, e.g. 'AC' for Access Control, 'AT' for Awareness and Training, etc...]			
Group Title	[Unabbreviated NIST control family description, e.g. 'Access Control']			
Control ID	[NIST 800-53 Rev. 4 Control (MOD) control number in sequence as applicable, e.g. 'AC-1']			
Control Title	[NIST 800-53 Rev. 4 Control (MOD) control name, e.g. 'Access Control Policy and Procedures']			
Risk Statement	[A high level statement of the potential risk present by not addressing the control activity]			
Priority / Baseline	P1	LOW – No	MOD – Yes	HIGH – Yes
Required Date	[Date which requirement will become effective. Note: Only "Low" baseline controls are mandatory for all systems. Other controls may be applicable based on the state organization risk assessment]			
Control Description	[Detailed NIST 800-53 Rev. 4 Control (MOD) control description]			
Implementation	State	[The State level requirements for the implementation of information security controls]		
	State organization	[To be determined for each state organization; To include organization specific components as applicable, e.g. if an organization has a specific mapping requirement under the Health Insurance Portability and Accountability Act (HIPAA); or other applicable regulatory driver) this relative control could be included here]		
	Compartment	[To be determined for each state organization; To include organization specific compartment or divisional level components as applicable, e.g. if an organization's department has a specific requirement under HIPAA, as an example, this relative control could be included here]		
Example	[This section includes example only considerations of how the control identified above may be applicable in a state organization security environment]			

Baselines v. Priorities

- **Baselines are used to select which controls to implement**
 - Relate to the Impact of a system
 - Three Impact levels: Low, Moderate, High
- **Priorities are useful for sequencing control implementation**
 - Ensures that more fundamental controls are implemented first
 - Four Priorities: P1, P2, P3, P0

Security Control Standards Example

NIST SP800-53 control →

Current TAC 202 control →

Agency specific adjustment →

Group ID	AC			
Group Title	Access Control			
Control ID	AC-3			
Control Title	Access Enforcement			
Risk Statement	Misconfigured access controls provide unauthorized access to information held in application systems.			
Priority / Baseline	P1	LOW – Yes	MOD – Yes	HIGH – Yes
Required Date	February 2015			
Control Description	The organization enforces approved authorizations for logical access to the system in accordance with applicable policy.			
Implementation	State	<ol style="list-style-type: none"> 1. Access to state information resources shall be appropriately managed. 2. Each user of information resources shall be assigned a unique identifier except for situations where risk analysis demonstrates no need for individual accountability of users. User identification shall be authenticated before the information resources system may grant that user access. 		
	State Organization	[to be determined]		
	Compartment	[to be determined]		
Example(s)	- The organization has Implemented role-based access control to determine how users may have access strictly to those functions that are described in job responsibilities.			

Security Control Standards Example

- **Least Privilege is not required at “LOW”**
- **Many organizations will have requirements outside TAC 202**

Group ID	AC			
Group Title	Access Control			
Control ID	AC-6			
Control Title	Least Privilege			
Risk Statement	Information in applications is accessed by users and other personnel outside of defined business requirements.			
Priority / Baseline	P1	LOW – No	MOD – Yes	HIGH – Yes
Not Required				
Control Description	The organization employs the principle of least privilege, allowing only authorized accesses for users (or processes acting on behalf of users) which are necessary to accomplish assigned tasks in accordance with organizational missions and business functions.			
Implementation	State	No Statewide control		
	State organization	[to be determined]		
	Compartment	[to be determined]		
Example	- Only authorized users have authorized accounts to establish system accounts, configure access authorizations, filter firewall rules, manage cryptographic keys and access control lists.			

Phased approach

- Current TAC 202 controls move into the Security Control Standards as “Phase 1” controls
- Other NIST controls will be prioritized for implementation 1 year or 2 years out
 - Phase 2 = Low/P1 controls NOT in current TAC
 - Phase 3 = Low/P2&P3 controls NOT in current TAC

February 2015

Controls in
Legacy TAC

February 2016

Low / P1
Controls not in
Legacy TAC

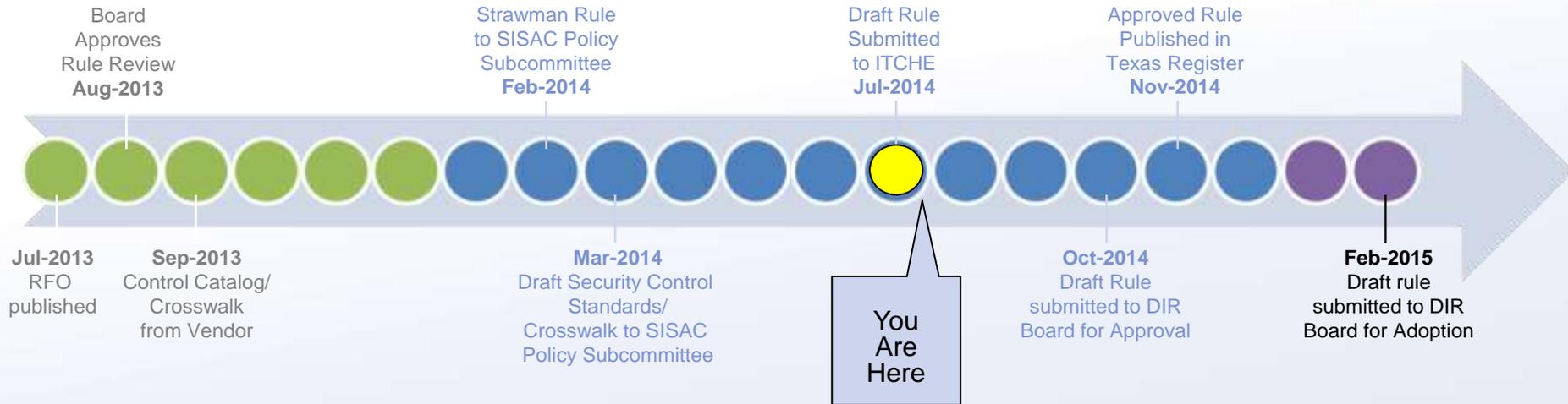
February 2017

Low / P2 & P3
Controls not in
Legacy TAC

Security Control Standards Updates

- **Governance for Security Control Standards proposed in the TAC 202 Rule**
 - Will be similar to rule review, but streamlined
 - Refer to 202.76 (d)
- **Anticipate updates as NIST 800-53 revisions occur**
 - But will include as part of the TAC 202 review cycle

What's Next?



- **We've reached a significant and critical milestone**
- **These TAC 202 changes are important to the state**
- **We thank you for the time today**

A large, faint watermark of the Texas state seal is visible in the background, centered behind the text. The seal depicts a five-pointed star surrounded by a wreath of olive and live oak branches, with the words "THE STATE OF TEXAS" and "1845" inscribed around the perimeter.

Questions?

dirsecurity@dir.texas.gov