

RSAC[®]Conference2015

San Francisco | April 20-24 | Moscone Center

SESSION ID: GRC-T08

Risk-Ops at Scale: Framework Operationalization to Address Business Risk

Eddie Block

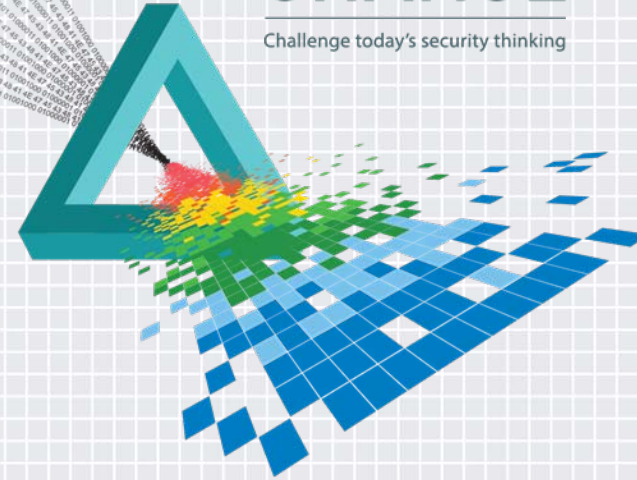
Chief Information Security Officer
State of Texas
@jurishacker

Nancy Rainosek

Statewide GRC Program Manager
State of Texas
@nsrainosek

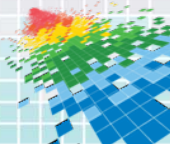
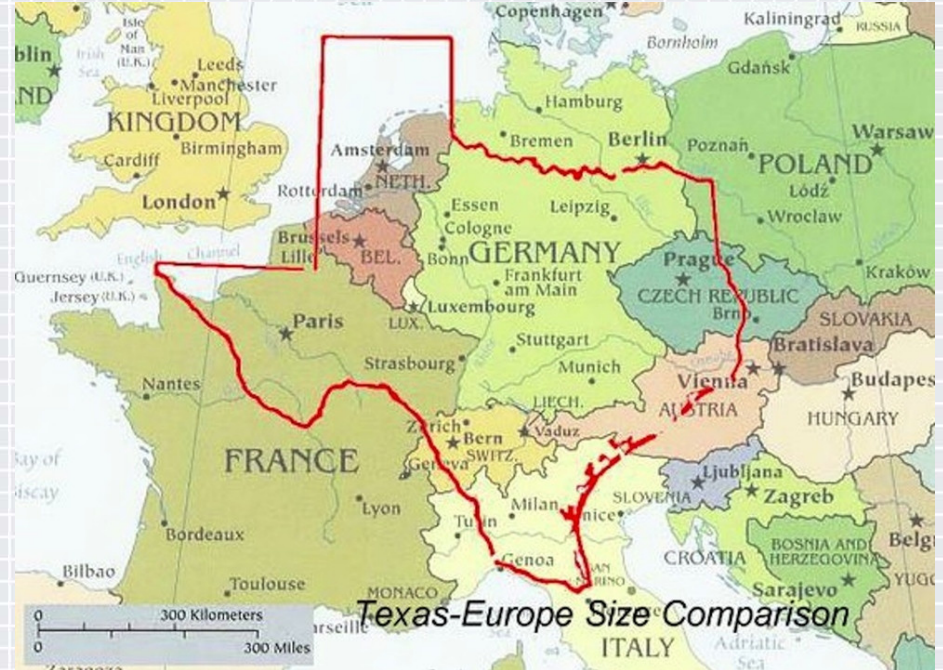
CHANGE

Challenge today's security thinking



Everything's Bigger in Texas

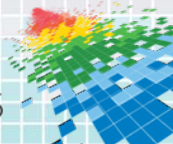
- ◆ 310,959+ state employees
- ◆ \$96.9 billion budget (25 on the Fortune 500)
- ◆ 3.5 million recipients of food assistance
- ◆ 4.1 million residents in the Medicaid program
- ◆ 5+ million students
- ◆ \$140 Billion in Texas retirement systems



The bad guys see us as **one**



but we fight with **200** separate armies



Today's Game Plan

RSA Conference 2015

San Francisco | April 20-24 | Moscone Center

- ◆ Challenges Facing the State of Texas
- ◆ Texas Cybersecurity Framework
- ◆ Instrumenting the Framework

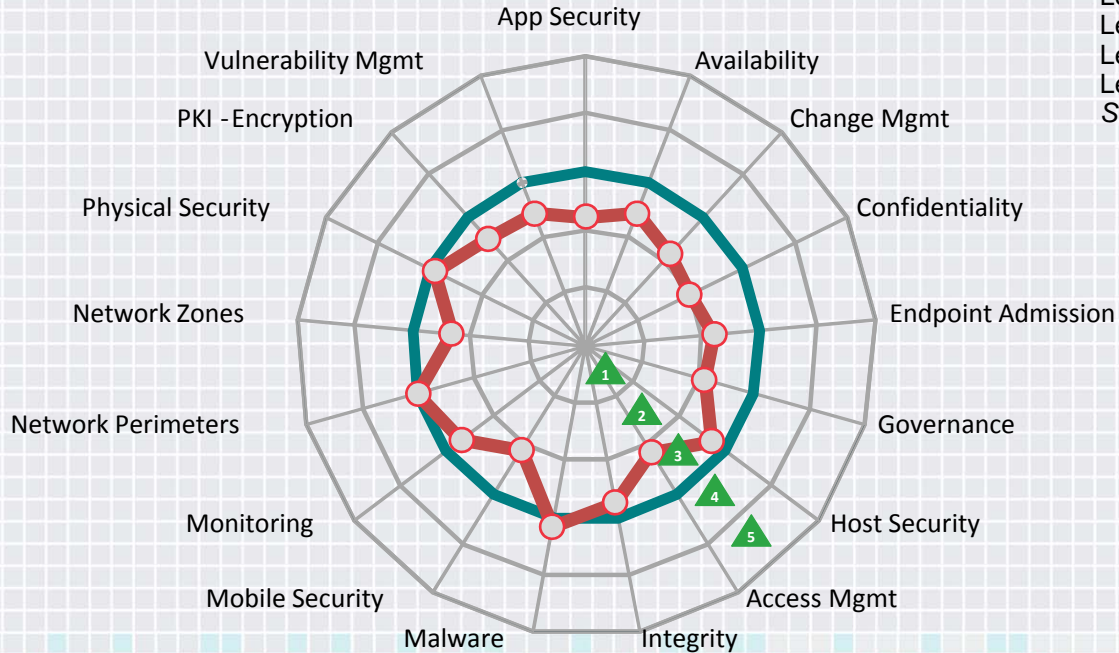


Security Assessment Benchmark

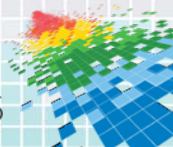
Security assessments Conducted 2011 through 2014

*Over 40 agencies comprising over 80% of State FTEs

Maturity Level Definitions
 Level 1: Initial/Ad Hoc
 Level 2: Developing/Reactive
 Level 3: Defined/Proactive
 Level 4: Managed
 Level 5: Optimized
 Source: Gartner

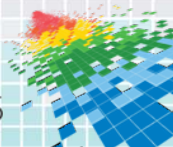


— Due Diligence Standard
 — State of the State



Trends

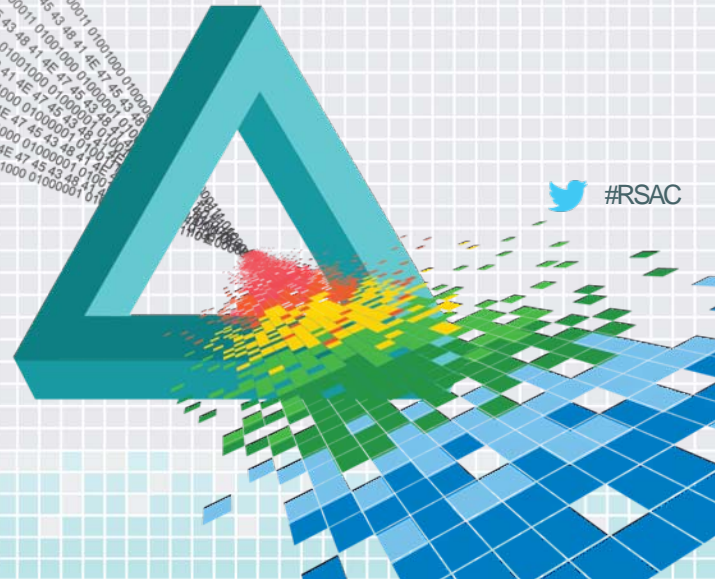
- IT staffing challenges
- Data classification
- Security governance / awareness
- Identity and access management standardization
- Security in software development
- Consistent event monitoring and analysis
- Internal network segmentation



RSA® Conference 2015

San Francisco | April 20-24 | Moscone Center

The Texas Cybersecurity Framework

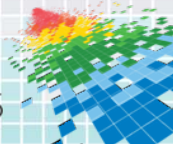


 #RSAC

The Texas Cybersecurity Framework

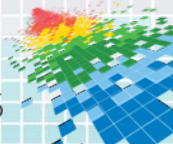
Objective 1:

Evolve the Texas Cybersecurity Framework to establish adaptable state policy, standards and guidelines that define appropriate levels of security and risk management for agencies and institutions of higher education.



The Texas Cybersecurity Framework

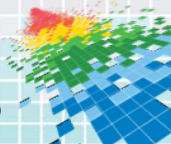
- ◆ **Agency security plan template** Implemented in January 2014
- ◆ **Vendor product / service template** Implemented in March 2014
- ◆ Updated information security rule Adopted February 2015
- ◆ Security control standards catalog Adopted February 2015
- ◆ Guidelines and whitepapers Ongoing effort
- ◆ Governance, risk and compliance solution In Progress



Agency Security Plans

FUNCTIONAL AREA	SECURITY OBJECTIVE
Identify	<ul style="list-style-type: none"> - Privacy and Confidentiality - Data Classification - Critical Information Asset Inventory - Enterprise Security Policy, Standards and Guidelines - Control Oversight and Safeguard Assurance - Information Security Risk Management - Security Oversight and Governance - Security Compliance and Regulatory Requirements Management - Cloud Usage and Security - Security Assessment and Authorization / Technology Risk Assessments - External Vendors and Third Party Providers
Protect	<ul style="list-style-type: none"> - Enterprise Architecture, Roadmap & Emerging Technology - Secure System Services, Acquisition and Development - Security Awareness and Training - Privacy Awareness and Training - Cryptography - Secure Configuration Management - Change Management - Contingency Planning - Media - Physical Environmental Protection - Personnel Security - Third-Party Personnel Security - System Configuration Hardening & Patch Management - Access Control - Account Management - Security Systems Management - Network Access and Perimeter Controls - Internet Content Filtering - Data Loss Prevention - Identification & Authentication - Spam Filtering - Portable & Remote Computing - System Communications Protection
Detect	<ul style="list-style-type: none"> - Malware Protection - Vulnerability Assessment - Security Monitoring and Event Analysis
Respond	<ul style="list-style-type: none"> - Cyber-Security Incident Response - Privacy Incident Response
Recover	<ul style="list-style-type: none"> - Disaster Recovery Procedures

- ◆ 40 Security objectives defined
- ◆ Aligned to “Framework for Improving Critical Infrastructure Cybersecurity” released by NIST in February 2014



Agency Security Maturity Levels

MATURITY LEVEL	DIR DESCRIPTION	KEYWORDS
0	There is no evidence of the organization meeting the objective.	None, Nonexistent
1	The organization has an ad hoc, inconsistent, or reactive approach to meeting the objective.	Ad-hoc, Initial
2	The organization has a consistent overall approach to meeting the objective, but it is still mostly reactive and undocumented. The organization does not routinely measure or enforce policy compliance.	Managed, Consistent, Repeatable
3	The organization has a documented, detailed approach to meeting the objective, and regularly measures its compliance.	Compliant, Defined
4	The organization uses an established risk management framework to measure and evaluate risk and integrate improvements beyond the requirements of applicable regulations.	Risk-Based, Managed
5	The organization has refined its standards and practices focusing on ways to improve its capabilities in the most efficient and cost-effective manner.	Efficient, Optimized, Economized

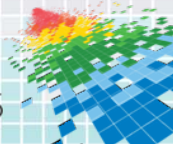
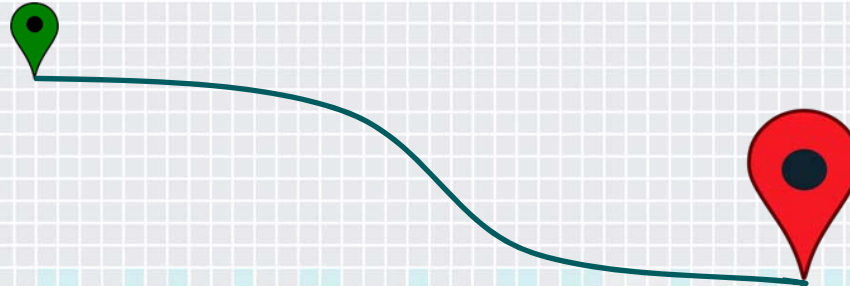
Highlights and Roadmap Improvements

Successes to build upon

- ◆ Spam filtering
- ◆ Account management
- ◆ Disaster recovery
- ◆ Security systems management

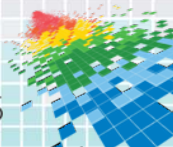
Areas for improvement

- ◆ Data loss prevention
- ◆ Secure systems services, development and acquisition
- ◆ Cloud usage and security



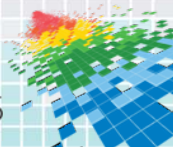
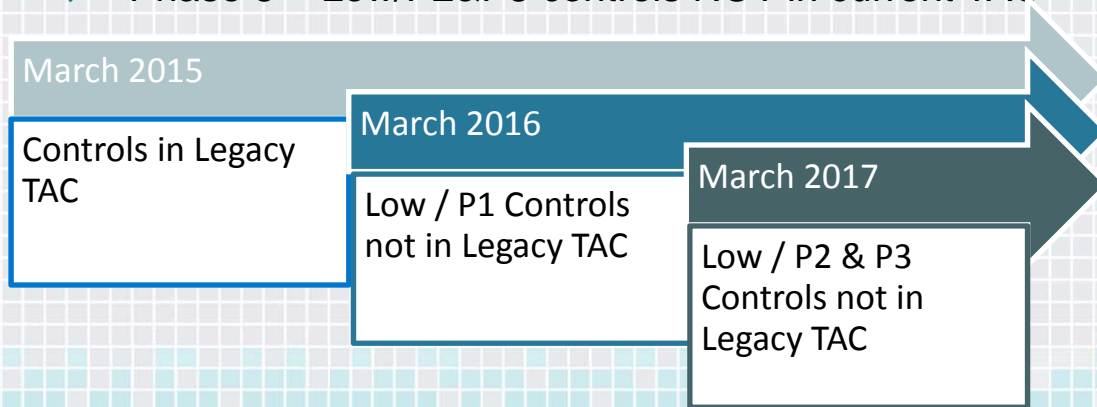
The Texas Cybersecurity Framework

- ◆ Agency security plan template Implemented in January 2014
- ◆ Vendor product / service template Implemented in March 2014
- ◆ **Updated information security rule** Adopted February 2015
- ◆ **Security control standards catalog** Adopted February 2015
- ◆ **Guidelines and whitepapers** Ongoing effort
- ◆ Governance, risk and compliance solution In Progress



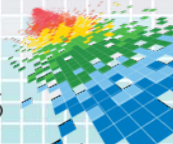
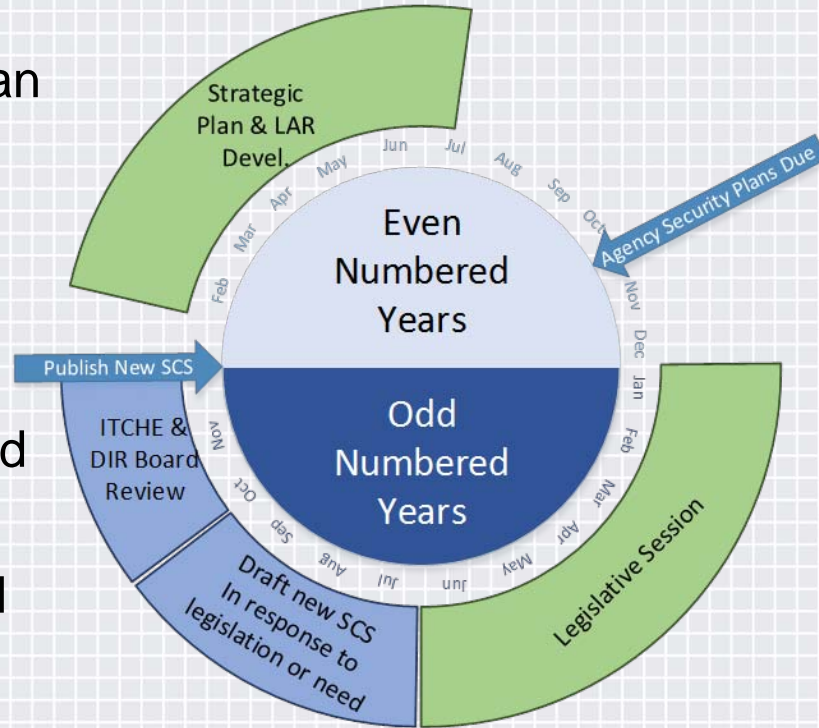
Phased approach

- ◆ Legacy 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



State of Texas Governance Timeline

- ◆ Updates to the Control Catalog can be based on
 - ◆ Legislation
 - ◆ Identified need
 - ◆ Changes in technology
- ◆ Changes published in time to be included in Strategic Plan and LAR decisions



RSA[®]Conference2015

San Francisco | April 20-24 | Moscone Center

Instrumenting the Framework.... Forming a Single Army



 #RSAC

Instrumenting the Framework

Objective 2 - Instrument the Texas Cybersecurity Framework within the GRC platform

- Enable the Agency Security Plan process
- Define Program Maturity Risk Assessment Methodology



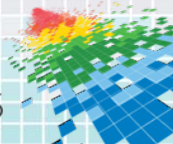
FUNCTIONAL AREA	SECURITY OBJECTIVE
Identify	<ul style="list-style-type: none"> • Identify and categorize risks • Risk identification • Critical information asset inventory • Enterprise security risks, threats and business • Control strength and safeguard assurance • Information security gap management • Security strategy and governance • Security operations and program requirements management • Trust usage and security • Security Assessment and Authorization / Technology Risk Assessment • External (supply and third party) threats
Protect	<ul style="list-style-type: none"> • Enterprise architecture, business & strategy mapping • Secure System Services, Acquisition and development • Security awareness and training • Privacy awareness and training • Configuration management • Change management • Configuration, Patching & Updates • Media • Physical Environmental Protection • Personnel Security • Privileged Account Security • System Configuration Monitoring & Patch Management • Access Control • Account Management • Security System Management • Network Access and Network Control • Network System Planning • Data Loss Prevention • Identification & Authentication • Data Privacy • Incident & Response Computing • System Communications, Protection
Monitor	<ul style="list-style-type: none"> • Malware Protection • Vulnerability Assessment • Security Monitoring and Event Analysis
Respond	<ul style="list-style-type: none"> • Cyber Security Incident Response • Privacy Incident Response
Recover	<ul style="list-style-type: none"> • Disaster Recovery Planning

Objective 3 - Support Agency Risk Management Processes

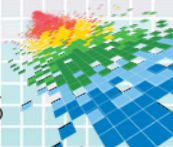
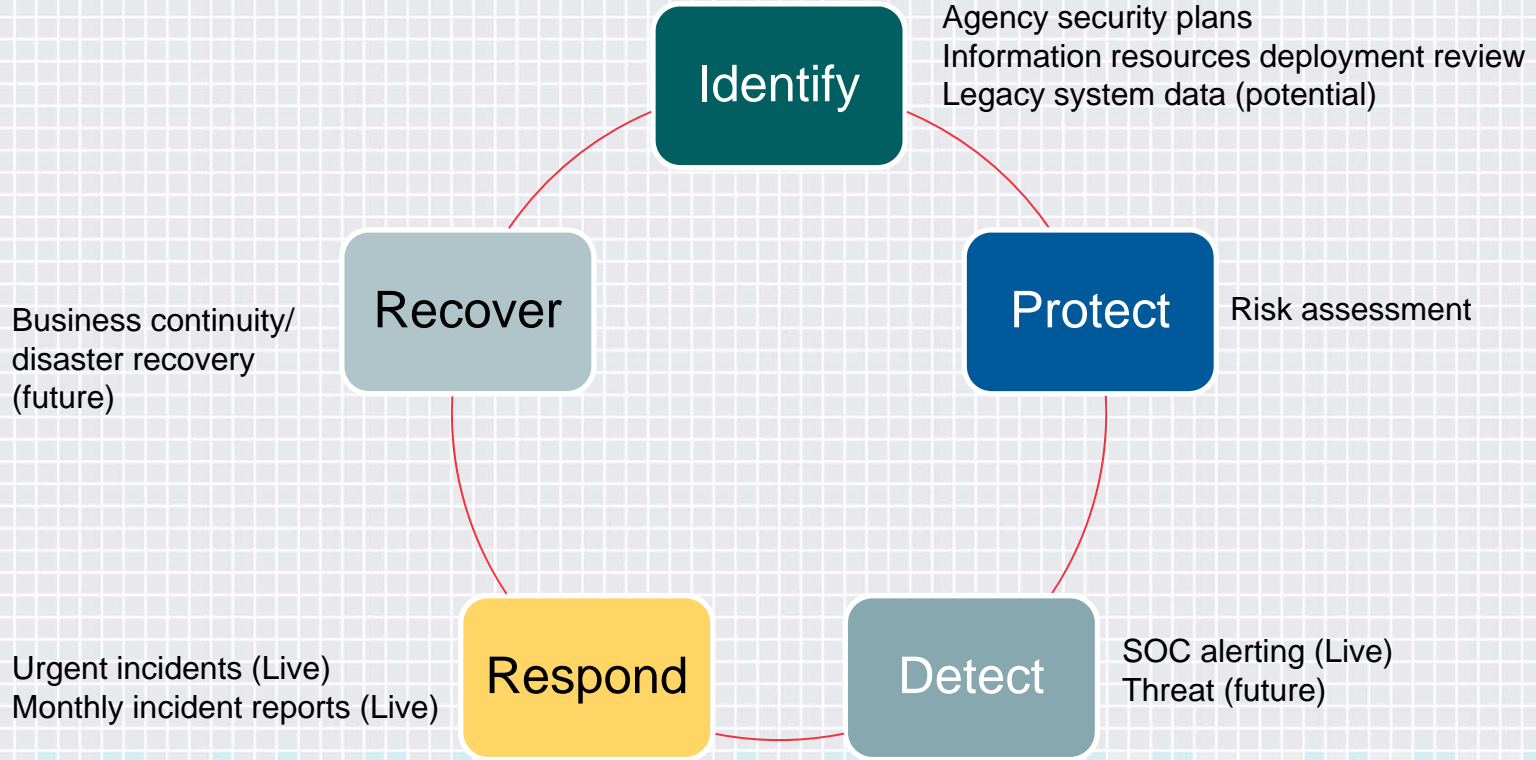
- Provide enterprise risk management capabilities within the GRC platform

The Texas Cybersecurity Framework

- ◆ Agency security plan template Implemented in January 2014
- ◆ Vendor product / service template Implemented in March 2014
- ◆ Updated information security rule Adopted February 2015
- ◆ Security control standards catalog Adopted February 2015
- ◆ Guidelines and whitepapers Ongoing effort
- ◆ **Governance, risk and compliance solution** In Progress



GRC Tool Implementation



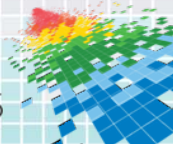
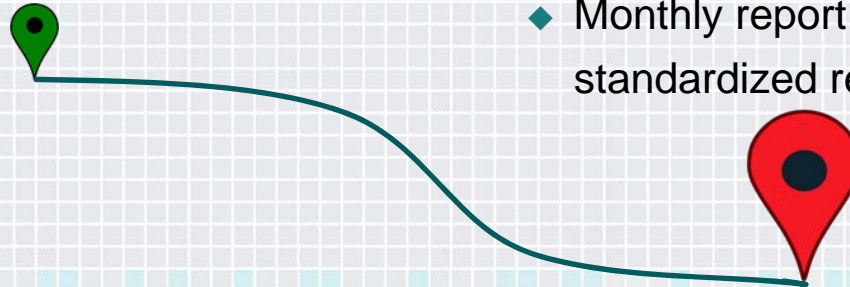
Incident Response

Issues

- ◆ No analytics capability for critical incidents
- ◆ Inconsistent reporting from agencies

Solution









- ◆ Urgent incidents must be reported through the GRC Incidents module
- ◆ Using the GRC platform as your incident response system will automatically generate your required monthly report
- ◆ Monthly report uses Veris framework for standardized reporting



Urgent Incident Reporting System

▼ Incident General Information

i This section captures general information about the incident. The main purpose is to allow organizations to identify, store, and retrieve incidents over time.

<p>Incident ID:</p> <p>Incident Name: <input type="text"/></p> <p>Source ID: <input type="text"/> Edit</p> <p>Affected Organization: <input type="text"/> Add</p> <p>Incident Date: <input type="text"/>  </p> <p>Discovery Date: <input type="text"/>  </p> <p>First Malicious Action Date: <input type="text"/>  </p> <p>Containment Date: <input type="text"/>  </p>	<p>Status: New</p> <p>Incident Confirmation: <input type="radio"/> Confirmed <input type="radio"/> Suspected <input type="radio"/> False Positive <input type="radio"/> Near Miss Edit</p> <p>Priority: <input type="radio"/> Low <input type="radio"/> Medium <input type="radio"/> High Edit</p> <p>Ticket Number: <input type="text"/></p> <p>Recorded By: Rainosek, Nancy</p> <p>Incident Owner: <input type="text"/></p> <p>Incident Reviewer: <input type="text"/></p> <p>Has Incident Been Associated to Monthly: No</p>
---	---

Incident General Information
Threat Actors/Actions
Indicators of Compromise
Security Attributes
Response
Impact Assessment

▼ Additional Information

Disclosure: Was non-public data disclosed? Yes (confirmed) Potentially (at risk) No Unknown [Edit](#)

Reported to Law Enforcement: Was this incident reported to law enforcement? (Police, etc.) Yes No Unknown [Edit](#)


Propagate to Others: Can this incident propagate to other state systems? Yes No Unknown [Edit](#)

Variety: What varieties of data were exposed or compromised? [Edit](#)

Number of Records: How many records were compromised?


Incident Tracking State: At the time of exposure or compromise, was the data being stored, transmitted, or processed? [Edit](#)

Incident Summary:



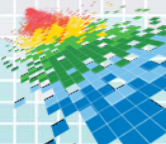
Office of the Chief Information Security Officer
— State of Texas —

21



Urgent Incident Reporting System









Incident General Information	Threat Actors/Actions	Indicators of Compromise	Security Attributes	Response
▼ Additional Information				
* Disclosure:	Was non-public data disclosed?			
* Reported to Law Enforcement:	Was this incident reported to law enforcement? (Police, etc.)			
* Propagate to Others:	Can this incident propagate to other state systems?			
Variety:	What varieties of data were exposed or compromised?			
Number of Records :	How many records were compromised?			
Incident Tracking State:	At the time of exposure or compromise, was the data being stored, transmitted, or processed?			
Incident Summary:	<input type="text"/>			
Alert DIR:	<input type="text"/>			<input type="button" value="Edit"/>



Urgent Incident Reporting System

Incident General Information

This section captures general information about the incident. The main purpose is to allow organizations to identify, store, and retrieve incidents over time.

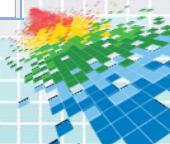
Incident ID:		Status:	
Incident Name:	<input type="text"/>	Incident Confirmed:	<input type="checkbox"/>
Source ID:	<input type="text"/> Edit	Priority:	
Affected Organization:	<input type="text"/> ... Add	Ticket Number:	
Incident Date:	<input type="text"/>  	Recorded By:	
Discovery Date:	<input type="text"/>  	Incident Owner:	
First Malicious Action Date:	<input type="text"/>  	Incident Review:	
Containment Date:	<input type="text"/>  	Has Incident Been Reviewed Monthly:	

Incident General Information | Threat Actors/Actions | Indicators of Compromise | Security Attributes | Response | Impact Assessment

Additional Information

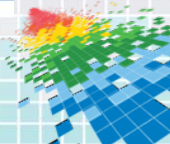
Disclosure:	Was non-public data disclosed?	<input type="radio"/> Yes (confirmed) <input type="radio"/> Potentially (at risk) <input type="radio"/> No <input type="radio"/> Unknown Edit
Reported to Law Enforcement:	Was this incident reported to law enforcement? (Police, etc.)	<input type="radio"/> Yes <input type="radio"/> No <input type="radio"/> Unknown Edit
Propagate to Others:	Can this incident propagate to other state systems?	<input type="radio"/> Yes <input type="radio"/> No <input type="radio"/> Unknown Edit
Variety:	What varieties of data were exposed or compromised?	<input type="text"/> ... Edit
Number of Records:	How many records were compromised?	<input type="text"/>
Incident Tracking State:	At the time of exposure or compromise, was the data being stored, transmitted, or processed?	<input type="text"/> ... Edit
Incident Summary:	<input type="text"/>	

- Incident General Information
- Threat Actors/Actions
- Indicators of Compromise
- Security Attributes
- Response
- Impact Assessment



Monthly Incident Reporting

Incidents	Impact	Totals																				
<p>▼ Previous Incident Threat Actions Logged During This Period</p> <p>i The numbers in this section will automatically populate from the Incident Application and the referenced incident records in the section below called "Incidents Logged During This Period"</p> <table border="1"> <tbody> <tr> <td>Malware Threats Logged During Reporting Period:</td> <td>13</td> <td>Physical Threats Logged During Reporting Period:</td> <td>0</td> </tr> <tr> <td>Hacking Threats Logged During Reporting Period:</td> <td>0</td> <td>Error Threats Logged During Reporting Period:</td> <td>1</td> </tr> <tr> <td>Misuse Threats Logged During Reporting Period:</td> <td>0</td> <td>Environmental Threats Logged During Reporting Period:</td> <td>0</td> </tr> <tr> <td>Social Engineering Threats Logged During Reporting Period:</td> <td>1</td> <td>Total Number of Incidents Logged :</td> <td>15</td> </tr> </tbody> </table>			Malware Threats Logged During Reporting Period:	13	Physical Threats Logged During Reporting Period:	0	Hacking Threats Logged During Reporting Period:	0	Error Threats Logged During Reporting Period:	1	Misuse Threats Logged During Reporting Period:	0	Environmental Threats Logged During Reporting Period:	0	Social Engineering Threats Logged During Reporting Period:	1	Total Number of Incidents Logged :	15				
Malware Threats Logged During Reporting Period:	13	Physical Threats Logged During Reporting Period:	0																			
Hacking Threats Logged During Reporting Period:	0	Error Threats Logged During Reporting Period:	1																			
Misuse Threats Logged During Reporting Period:	0	Environmental Threats Logged During Reporting Period:	0																			
Social Engineering Threats Logged During Reporting Period:	1	Total Number of Incidents Logged :	15																			
<p>▼ Additional Incidents Not Logged in Archer</p> <p>i Please enter the totals for each category below in the boxes. For more information on the category, please click the icon next to the text. Please enter "0" if not applicable. Also, note this is in addi</p> <table border="1"> <tbody> <tr> <td>Additional Malware Cleaned by People:</td> <td></td> <td>Additional Malware Cleaned by Automation:</td> <td></td> </tr> <tr> <td>Additional Hacking Incidents:</td> <td></td> <td>Additional Physical Incidents:</td> <td></td> </tr> <tr> <td>Additional Misuse Incidents:</td> <td></td> <td>Additional Error Incidents:</td> <td></td> </tr> <tr> <td>Additional Social Engineering Incidents:</td> <td></td> <td>Additional Environmental Incidents:</td> <td></td> </tr> <tr> <td>Additional Number of Incidents:</td> <td>0</td> <td></td> <td></td> </tr> </tbody> </table>			Additional Malware Cleaned by People:		Additional Malware Cleaned by Automation:		Additional Hacking Incidents:		Additional Physical Incidents:		Additional Misuse Incidents:		Additional Error Incidents:		Additional Social Engineering Incidents:		Additional Environmental Incidents:		Additional Number of Incidents:	0		
Additional Malware Cleaned by People:		Additional Malware Cleaned by Automation:																				
Additional Hacking Incidents:		Additional Physical Incidents:																				
Additional Misuse Incidents:		Additional Error Incidents:																				
Additional Social Engineering Incidents:		Additional Environmental Incidents:																				
Additional Number of Incidents:	0																					



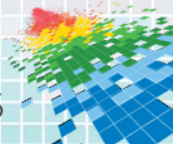
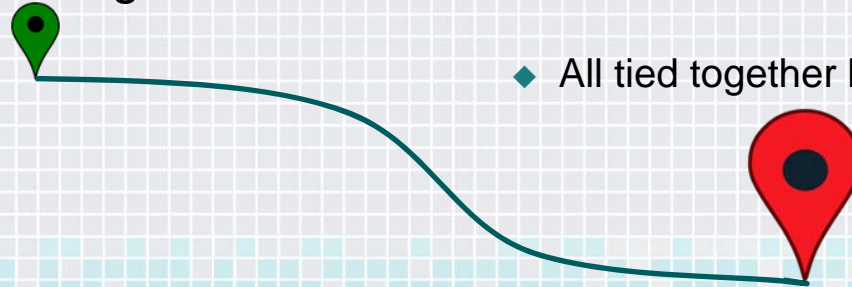
Security Plan Template

Issues

- ◆ Both plan formulation and analytics difficult using Excel spreadsheets
- ◆ Inaccurate responses received because of overriding Excel input
- ◆ Inconsistent reporting from agencies

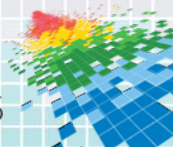
Solution

- ◆ Plan reporting must be done using GRC platform
- ◆ Analytics and charts are easily generated
- ◆ Future versions will include program maturity determination through risk assessment process
- ◆ All tied together by NIST 800-53



Security Plan Template: Exce Version


		MATURE LEVEL FOR THE IMPLEMENTED OBJECTIVE															
		LEVEL 4: Managed. The organization has an effective approach to meeting the objective.				LEVEL 3: Defined. The organization has a documented, detailed approach to meeting the objective, and regularly measures the compliance.				LEVEL 2: Repeatable. The organization has a well-measured approach to meeting the objective, but it is not consistently repeatable and well-documented. The organization has not regularly measured its progress.				LEVEL 1: Established. The organization has an initial, incomplete, or reactive approach to meeting the objective.			
#	FUNCTIONAL AREA	SECURITY OBJECTIVE	NIST FRAMEWORK MAPPING	DEFINITION/OBJECTIVE	RELEVANT CONTROL ACTIVITIES IN PLACE	LEVEL 1: Established		LEVEL 2: Repeatable		LEVEL 3: Defined		LEVEL 4: Managed		LEVEL 5: Optimized		ROADMAP (What steps will the agency take in the next 12 months to improve its posture?)	CHALLENGES TO IMPLEMENTATION
						PATTERN CONTROLS	% OF AGENCY AT LEVEL 1	PATTERN CONTROLS	% OF AGENCY AT LEVEL 2	PATTERN CONTROLS	% OF AGENCY AT LEVEL 3	PATTERN CONTROLS	% OF AGENCY AT LEVEL 4	PATTERN CONTROLS	% OF AGENCY AT LEVEL 5		
2.1	Identity	Primary ID Confidentiality		Describe the appropriate security of primary ID information and approved sharing and define conditions with respect to storage and access. Include the requirements of HIPAA, Texas Business & Commerce Code, and agency confidentiality policies that include and expand upon regulatory and legal requirements for applicability.	Privacy Policies document		Privacy policy considered when determining the classification of data.	Privacy policy established and documented.	Applicable privacy standards and regulations are incorporated into the organization's security program.			The organization's structure, processes, and personnel are clearly defined.	Privacy is protected by the organization's security program.				
2.2	Identity	Data Classification	IDA-APS	Data classification provides a framework for managing data and information resources based on their value to the organization, critical functional value, and impact of loss on other operations. To apply the appropriate levels of protection or restriction to data and information resources, primary, critical, operational, and privacy considerations, data, whether electronic or physical, must be classified. The data owner should consult with the Information Security Organization and list categories in the classification of data (Restricted, Confidential, Agency Internal, or Public). Description of data classification information shall cover the expected level of identification or distribution of all the organization's information resources that they are intended to access in criticality to the business and that protection can be applied commensurate with the security importance.	Data classification policies and procedures document		Data classification policies and procedures are defined and repeatable. Access to information, sensitive and important, distributed parts of the organization have appropriate protection and classification.	Data classification policies and procedures are defined and repeatable. Access to information, sensitive and important, distributed parts of the organization have appropriate protection and classification.	The organization's data classification policies are defined with applicable regulations and the organization's mission requirements. The organization's data classification policy is reviewed and updated as appropriate. Data owners have been classified for their information.			Data is managed by technology that restricts classification or access data is created. Automated classification is used to categorize classified data in the organization. Data classification maintains a continuous, proactive and preventive handling appropriate matrix.	Data is managed by an information technology that restricts classification or access data is created. Automated classification is used to categorize classified data in the organization. Data classification maintains a continuous, proactive and preventive handling appropriate matrix.				
2.3	Identity	Critical Information Resource Inventory	IDA-APS	The organization has not been inventoried for applications, hardware and data. Owner of the data, application and data is unaccountable.	The organization has not been inventoried for applications, hardware and data. Owner of the data, application and data is unaccountable.		The organization has policies for performing inventory that are not consistently followed. Inventory is performed manually and error-prone. Management does not have multiple reviews of the organization's inventory and considers the matter	The organization has policies for performing inventory that are not consistently followed. Inventory is performed manually and error-prone. Management does not have multiple reviews of the organization's inventory and considers the matter	Critical data has been inventoried. The organization has identified data assets for all data centers and types of information systems with respect to the full, critical, sensitive data and system inventory that are not consistently updated. Management does not include all assets of the system from regulatory, compliance, legal, business, and investment.			Critical data has been inventoried, tabulated, and classified according to a business value of hardware, services, data, and software.	Regulatory, compliance and investment value are included in the organization's data classification matrix.				



Security Plan Template in GRC Platform

Navigation Menu <<
Agency Security Plan Attestations: 561918

0 of 0 Completed Options ▾

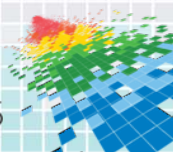
Font family | Font Size | **B** *I* U ABC x¹ x₂ | 

▼ General Information

Agency:	Fake State Agency	Number of Agency FTEs:	[Provide the number of full-time equivalent employees] <input type="text" value="12,574"/>
Dedicated Security Staff:	[Indicate the number of FTEs dedicated to information security, cybersecurity, or network security.] <input type="text" value="11"/>	Dedicated Security Budget:	[Provide the percentage of the IT budget dedicated to security.] <input type="text" value="1.5"/> %
Regulatory Drivers:	[Describe internal/external regulatory drivers (e.g., TAC 202, NIST, HIPAA) that might also be driving completion of the agency security plan template.] <input style="width: 100%;" type="text" value="HIPAA, IRS Pub 1075, FERPA, CJIS, "/>		

▼ Security Objectives
| Add New | Lookup | View All |

Obj. #	Security Objective	Relevant Control Activities in Place	% of Agency at Lvl 0	% of Agency at Lvl 1	% of Agency at Lvl 2	% of Agency at Lvl 3	% of Agency at Lvl 4	% of Agency at Lvl 5	
2.1	Privacy & Confidentiality	Privacy policies are defined and processes are in place to safeguard client personally identifiable information.	0 %	50 %	25 %	25 %	0 %	0 %	✕
2.10	Security Assessment and Authorization/ Technology Risk Assessments		40 %	60 %		20 %	0 %	0 %	✕
2.11	External Vendors and Third Party Providers		0 %	0 %	30 %	40 %	30 %	0 %	✕
2.12	Enterprise Architecture, Roadmap & Emerging Technology		100 %	0 %	0 %	0 %	0 %	0 %	✕
2.13	Secure System Services, Acquisition and Development		100 %	0 %	0 %	0 %	0 %	0 %	✕



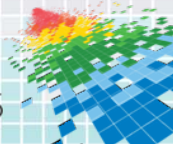
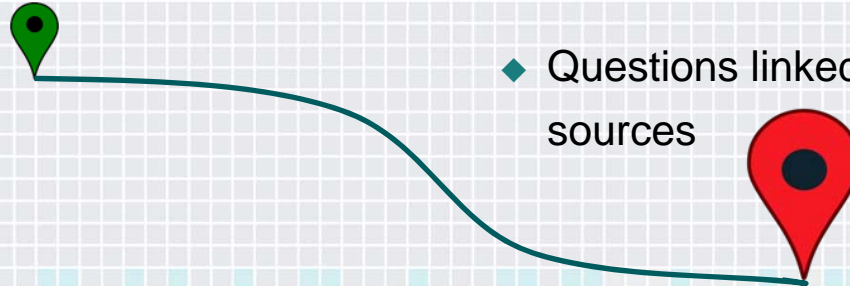
Risk Assessment

Issues

- ◆ Outdated MS Access system
- ◆ Mainly Excel spreadsheets
- ◆ No way to roll up overall risk for an organization

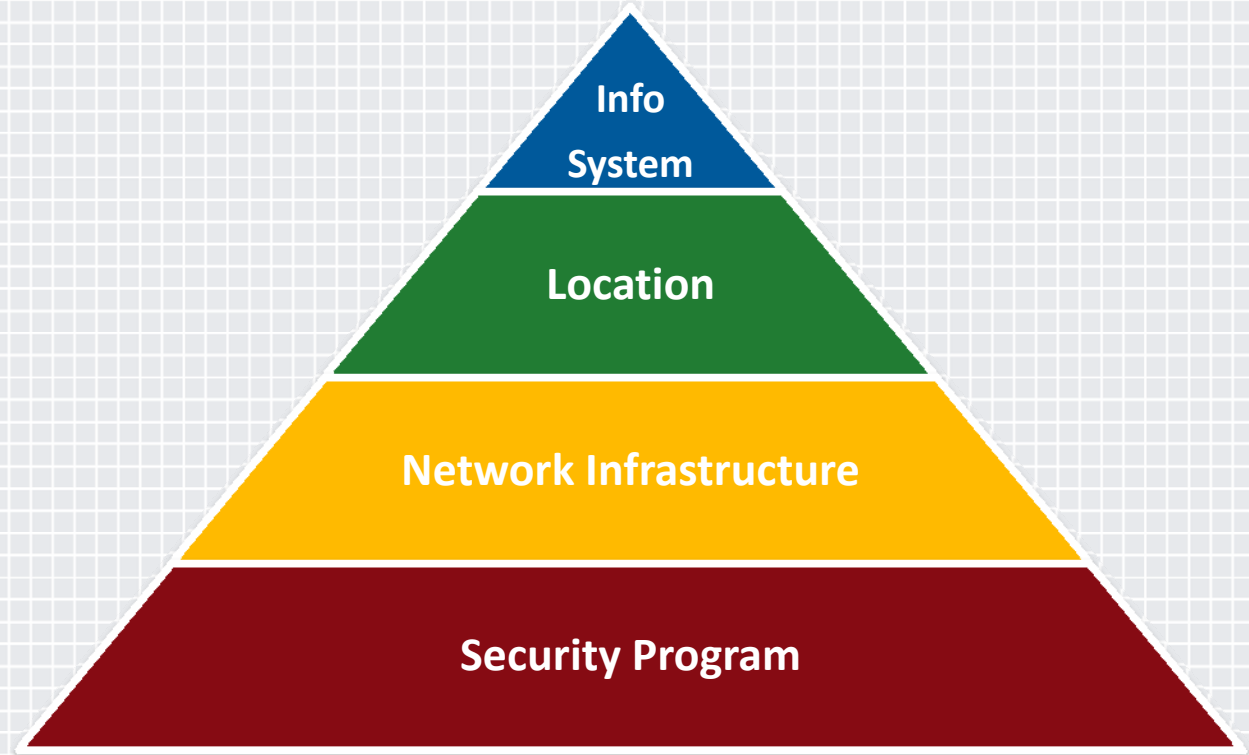
Solution

- ◆ Risk assessment capability through the GRC platform
- ◆ Targeted questionnaires to the people who know the status of controls
- ◆ Can roll up to the overall organization
- ◆ Questions linked to different authoritative sources



Risk Assessable Units

Break assessments
down by component
so questions are
only answered once.



Security Categorization



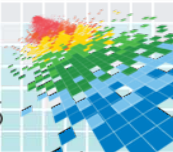
▼ Information Types						
Information Type	Availability Rating	Availability Special Considerations	Confidentiality Rating	Confidentiality Special Considerations	Integrity Rating	Integrity Special Considerations
<u>Criminal Incarceration</u>	Low	There may be cases (e.g. emergency bulletins affecting prisoner health and/or safety) in which emergency dissemination of information regarding life-threatening situations is delayed for excessive periods. Such cases can result in a high availability impact level.	Low		Moderate	In some cases (e.g., instructions regarding a need to isolate a prisoner from the general prison population for personal safety reasons), the unauthorized modification or destruction of criminal incarceration information can result in loss of human life a high impact potential.

▼ Security Category	
Recommended Security Category:	Moderate
Override Justification:	Category Override:
Additional Documentation:	

Criminal Incarceration

**Availability – Low
Confidentiality – Low
Integrity - Moderate**

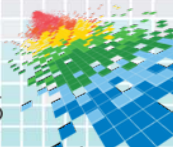
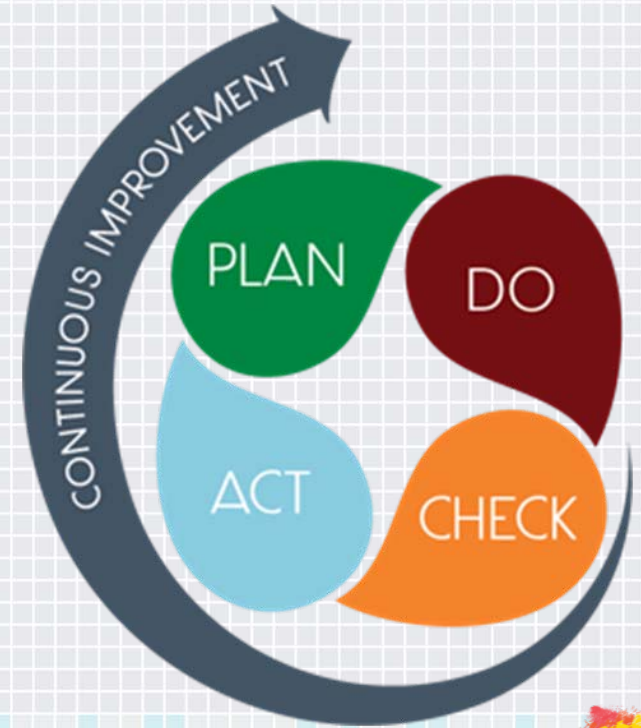
Moderate



Framework Instrumentation

Steps to successful application

- ◆ Figure out:
 - ◆ where you are
 - ◆ where you are going
 - ◆ who belongs in your army
- ◆ Select a framework
- ◆ Develop tools to normalize and share information and link day to day work to your overall objectives



Contact Us

Eddie Block

- ◆ Eddie.Block@Dir.texas.gov

Nancy Rainosek

- ◆ Nancy.Rainosek@Dir.texas.gov

