



TEXAS
Health and Human
Services

GUARD₄® your ASSETS

A Realistic Approach to
Risk Assessments for State Agencies

John Skaarup, Stan Hogan, and Steven Pryor

Agenda



TEXAS
Health and Human
Services

- The Research
- The Frameworks/Models
- The Realization
- The Solution
- The GU₄ARD





Research

Talking with our peers

- No consistent risk assessment approach
- Extensive controls / lack of resources
- Inability to:
 - accurately assess controls
 - track and monitor findings



TEXAS
Health and Human
Services



Research

Talking with our peers

- Asset Management: insufficient / unreliable
- Compliance fog (what does TAC 202 really require?)
- Agencies working in very tall, concrete reinforced, nuclear-resistant, silos (with blinders on)



TEXAS
Health and Human
Services



Research

Talking with our peers

- Change only comes through audit, fines, or breaches
- *"That's not my job - that's something that the IT people do"*



TEXAS
Health and Human
Services



Research

Risk Management Tools

- Limited use of enterprise risk management / risk assessment tools
- Easy to use tools are either insufficient or require considerable and costly customization (thus making them neither easy nor cheap)



TEXAS
Health and Human
Services



Research

Risk Management Tools

- Private sector tools do not easily translate to government
- Quality tools are unaffordable
- Dedicated resources or professional services are required to manage and maintain the tools



TEXAS
Health and Human
Services

Frameworks/Models



TEXAS
Health and Human
Services





Realization

Change is necessary

- Low-to-no cost
- A simple risk model / framework to follow
- Defensible risk methodology



TEXAS
Health and Human
Services



Realization

Change is necessary

- Ability to handle multiple security catalogs and categorizations
- Timely assessment of controls
- Ability to generate required security documents:
 - Security Assessment Report (SAR)
 - System Security Plan (SSP)



TEXAS
Health and Human
Services



Realization

Change is necessary

- Dashboard with analytics
- Common and exportable data
- Ability to assess contracts, contractors, and vendors



TEXAS
Health and Human
Services



Realization

Change is necessary

- Documentation of findings and corrective actions
- Addressing control weaknesses and vulnerabilities in applications



TEXAS
Health and Human
Services



Realization

Really, we only need two things

1. Ability to make informed decisions based on identified risk
2. Capability to provide a reasonable level of assurance to the organization



TEXAS
Health and Human
Services



TEXAS
Health and Human
Services



Introducing GU₄ARD

- Government
- Utility for
- Agency
- Risk
- Determination

GU₄ARD



TEXAS
Health and Human
Services

DEMONSTRATION

GU₄ARD



TEXAS
Health and Human
Services

- Built by Texas HHS Security staff
- Intended *not only for our organization* but for all state agencies
- Scalable from the smallest to the largest agencies
- Is free and available to any state agency**

***Important: Texas HHS cannot provide support for implementation, updates, troubleshooting, and/or maintenance*



TEXAS
Health and Human
Services

Discussion



End Credits



TEXAS
Health and Human
Services

- John Skaarup, CISSP
DADS Information Security Officer
- Stan Hogan, MBA, CISA, CRISC
HHS Director of Information Security Assurance
- Steven Pryor, MS, CISSP, CEH, PMP
HHS Senior Security Analyst



TEXAS
Health and Human
Services

Thank you

infosecurity@hhsc.state.tx.us



TEXAS
Health and Human
Services

References

- <http://www.johnsaunders.com/papers/riskcip/riskconference.htm>
- [IT Risk Assessment: Quantitative and Qualitative Approach - Proceedings of the World Congress on Engineering and Computer Science 2008 WCECS 2008, October 22 - 24, 2008, San Francisco, USA](#)