



# **IRS/FTA CSO Conference**



## **Enterprise**

### **Security Self Assessment**

**March 8, 2007**

**Timothy R. Blevins , KDOR Chief Information Officer**

1



## **Securing the Enterprise Outline of Presentation**

**Kansas ITEC Security Council**

**Purpose and Membership**

**Information Security Self-Assessment**

**IT Security HW, SW and Security  
Services Contract**

2



## Securing the Enterprise ITEC Security Council Purpose

The Information Technology Security Council shall:

Address information technology security issues and provide policy, standards, guidelines, or procedural recommendations to the Information Technology Executive Council;

Initiate and recommend security specifications for statewide contracts for common information technology requirements from suppliers qualified by the Division of Purchases.

Review proposed programs and projects referred by Chief Information Technology Officers and make recommendations regarding the appropriateness of security measures, technologies used, compliance with policy and standards, conformity with the Kansas State Technical Architecture and resource estimates;

Provide guidance to the Kansas State Technical Architecture Security Subcommittee regarding security aspects of the architecture;

3



## Securing the Enterprise ITEC Security Council Purpose

The Information Technology Security Council shall:

Contribute to and support the Strategic Information Management Plan and the annual Information Technology Plan;

Promote coordination and cooperation among state organizations' for effective integration and use of information technology security;

Promote and coordinate Quality Assurance of IT security processes and practices;

Promote and coordinate IT security audits throughout the enterprise;  
Address information technology security resource management issues at the request of the ITEC and make recommendations thereon.

4



## **ITEC Security Council Security Self-Assessment 27 Agencies that participate**

**Adjutant General's Dept.  
Information Network of Kansas  
Judicial Administration  
Juvenile Justice Authority  
Kansas Attorney General's Office  
Kansas Bureau of Investigation  
Kansas Corporation Commission  
Kansas Dept of Administration  
Kansas Dept of Agriculture  
Kansas Dept of Commerce  
Kansas Dept of Corrections  
Kansas Dept of Education  
Kansas Dept of Health & Environment  
Kansas Dept of Labor**

5



## **ITEC Security Council Security Self-Assessment 27 Agencies that participate continued**

**Kansas Dept of Revenue  
Kansas Dept of Social & Rehabilitation Services  
Kansas Dept of Transportation  
Kansas Dept of Wildlife & Parks  
Kansas Dept on Aging  
Kansas Highway Patrol  
Kansas Insurance Department  
Kansas Lottery  
KPERS  
Legislative Admin Services / LPA / Reviser of Statutes  
Office of the Secretary of State  
Office of the State Treasurer  
State Historical Society**

6



## Securing the Enterprise Information Security Self-Assessment

### BACKGROUND:

The Security Council decided in January 2003 that an enterprise-wide IT security risk assessment was necessary.

Subcommittee researched different possibilities and settled on the National Institute of Standards and Technology (NIST) questionnaire as contained in NIST Special Publication 800-26, *Security Self-Assessment Guide for IT Systems*. Subcommittee started with the 255 questions in the questionnaire and pared it down to a more manageable 170 questions.

This was developed for Federal agencies to use and includes references to :  
*GAO Federal Information Systems Controls Audit Manual (FISCAM)*,  
NIST Pub 800-14, *Generally Accepted Principles and Practices for Security Information Technology*,  
NIST Pub 800-18, *Guide for Developing Security Plans for IT Systems*,  
and NIST Pub 800-30, *Risk Management Guide for IT Systems*. 7



## Securing the Enterprise Information Security Self-Assessment

### BACKGROUND:

**Questionnaire was sent to ITAB Members August, 2003.**

**16 Agencies responded**

**ITEC established Policy 4310 effective July 22, 2004 requiring annual completion. Board of Regents to develop a similar survey.**

**Questionnaire was sent to ITAB members in August, 2004.**

**All 27 non-regents institutions responded -Last on Nov 10th**

**Results Spreadsheet with individual and comparative results sent out to all 27 respondents on 2/25/05**



## Securing the Enterprise Information Security Self-Assessment Next Steps

### **Security Council recommends a twofold goal for agencies:**

For those that scored less than 2.0 for any critical element, improve to a minimum of 2.0 for each critical element. ( written policies/procedures)

For those that scored at or above 2.0, to work towards scoring a minimum of a 3. ( Implementing the policies into standard use)

### **Items for Security Council to address collectively**

Focus on Contingency Planning, Security Awareness-Training and Education, Incident Response Capability, and Audit Trails

### **Internal and 3rd Party Audits**

Integrate results of the assessments

9



## Securing the Enterprise Information Security Self-Assessment Summary of Results

### **Significant overall improvement from 2003 to 2004**

#### **Recall rating key:**

- 0 - No policy or established practice**
- 1 - No written policy, but an informal practice**
- 2 - Written Policy/Procedure**
- 3 - Written Policy/Procedures implemented and in standard use**
- 4 - Policy/Procedure fully integrated and reviewed and tested**

**2003- Overall average from 1.6 to 3.0 on the 33 critical elements**

**2004- Overall average from 1.9 to 3.3 on the 33 critical elements**

**2003- 10 critical elements below 2.0 for 2003**

**2004- Only 1 critical element averaged below 2.0**

10

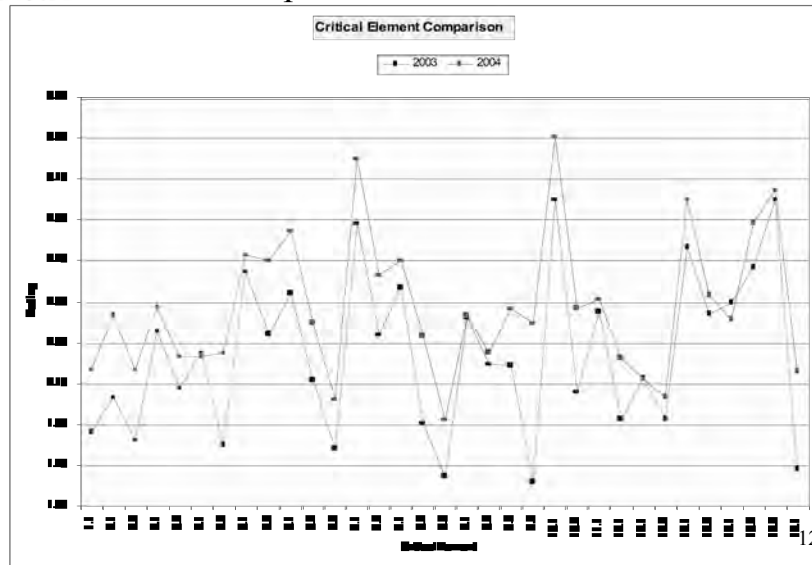


## Securing the Enterprise Information Security Self-Assessment Sample Comparative Results 2003-2004

| Self-Assessment |         |         |        |  |  |  |  |  |
|-----------------|---------|---------|--------|--|--|--|--|--|
|                 | 2003    | 2004    |        |  |  |  |  |  |
|                 | Overall | Overall |        | Question   |  |  |  |  |
| Element         | AVG     | AVG     | Change | 1. Risk Management   |  |  |  |  |
| 1.1.1           | 2.12    | 2.60    | 0.48   | 1.1.1 Is the current system configuration documented, i    |  |  |  |  |
| 1.1.2           | 1.71    | 1.83    | 0.13   | 1.1.2 Are risk assessments performed and documented        |  |  |  |  |
| 1.1.3           | 1.29    | 1.67    | 0.37   | 1.1.3 Has a mission/business impact analysis been co       |  |  |  |  |
| 1.1             | 1.86    | 2.17    | 0.30   | 1.1 Critical Element: Is risk periodically assessed?       |  |  |  |  |
|                 |         |         |        | 2. Review of Security Controls                             |  |  |  |  |
| 2.1.1           | 2.12    | 2.40    | 0.28   | 2.1.1 Has the system and all network boundaries been       |  |  |  |  |
| 2.1.2           | 1.65    | 2.17    | 0.52   | 2.1.2 Are tests and examinations of controls routinely r   |  |  |  |  |
| 2.1             | 2.03    | 2.43    | 0.40   | 2.1. Critical Element: Have the security controls of the   |  |  |  |  |
|                 |         |         |        |  |  |  |  |  |
| 2.2.1           | 1.82    | 2.17    | 0.34   | 2.2.1 Is there an effective and timely process for reporti |  |  |  |  |
| 2.2             | 1.82    | 2.17    | 0.34   | 2.2. Critical Element: Does management ensure that c       |  |  |  |  |



## Securing the Enterprise Information Security Self-Assessment Comparative Results 2003-2004





**Kansas 2007**  
**ITEC Security Council Security Self-Assessment**

Last Presentation was August 2006

Next Steps from that presentation have been done:

We tailored the new SSA to meet state requirements

Piloted new SSA, refined as necessary and used in Fall 2006

Emailed out the new SSA to 27 agencies

Extended the deadline one full month

13



**ITEC Security Council Security Self-Assessment**  
**Differences from prior years**

Quantum jump in complexity from last year

NIST making changes in response to Federal Information Security Act (FISMA)

3 NIST documents were used to form the spreadsheet:

800-53 (Rev 1) Recommended Controls for Federal Information

800-53A (2PD) Guide for Accessing the Security Controls

800-26 (Rev 1) Guide for Assessments and Reporting Form

In 2005 we had 16 major control areas , 33 critical elements, and 170 individual controls.

In 2006, 17 major controls areas, 152 individual controls, and 542 specific questions or procedures.

14



## ITEC Security Council Security Self-Assessment Results have been tabulated

| State of Kansas Information Technology Security Self-Assessment for 2006 |                      |
|--|----------------------|
| 17 Control Groups  |                      |
| Security Control   | All Agencies Average |
| 1. Access Control  | 2.58                 |
| 2. Awareness and Training  | 2.47                 |
| 3. Audit and Accountability  | 1.84                 |
| 4. Certification, Accreditation, & Security Assessments                  | 2.04                 |
| 5. Configuration Management  | 2.46                 |
| 6. Contingency Planning  | 2.17                 |
| 7. Identification and Authentication                                     | 2.73                 |
| 8. Incident Response   | 1.78                 |
| 9. Maintenance   | 2.20                 |
| 10. Media Protection   | 2.46                 |
| 11. Physical and Environmental Protection                                | 2.59                 |
| 12. Planning   | 2.42                 |
| 13. Personnel Security   | 2.48                 |
| 14. Risk Assessment  | 1.74                 |
| 15. System and Services Acquisition                                      | 2.26                 |
| 16. System and Communications Protection                                 | 2.33                 |
| 17. System and Information Integrity                                     | 2.63                 |



## ITEC Security Council Security Self-Assessment Intro Worksheet

| Control Group   | Control Area | Control Area | Control Area | Control Area | Control Area | Control Area | Control Area | Control Area | Control Area |
|---|--------------|--------------|--------------|--------------|--------------|--------------|--------------|--------------|--------------|
| Control Group   | Control Area | Control Area | Control Area | Control Area | Control Area | Control Area | Control Area | Control Area | Control Area |
| 1. Access Control                                       | 1.1          | 1.2          | 1.3          | 1.4          | 1.5          | 1.6          | 1.7          | 1.8          | 1.9          |
| 2. Awareness and Training                               | 2.1          | 2.2          | 2.3          | 2.4          | 2.5          | 2.6          | 2.7          | 2.8          | 2.9          |
| 3. Audit and Accountability                             | 3.1          | 3.2          | 3.3          | 3.4          | 3.5          | 3.6          | 3.7          | 3.8          | 3.9          |
| 4. Certification, Accreditation, & Security Assessments | 4.1          | 4.2          | 4.3          | 4.4          | 4.5          | 4.6          | 4.7          | 4.8          | 4.9          |
| 5. Configuration Management                             | 5.1          | 5.2          | 5.3          | 5.4          | 5.5          | 5.6          | 5.7          | 5.8          | 5.9          |
| 6. Contingency Planning                                 | 6.1          | 6.2          | 6.3          | 6.4          | 6.5          | 6.6          | 6.7          | 6.8          | 6.9          |
| 7. Identification and Authentication                    | 7.1          | 7.2          | 7.3          | 7.4          | 7.5          | 7.6          | 7.7          | 7.8          | 7.9          |
| 8. Incident Response                                    | 8.1          | 8.2          | 8.3          | 8.4          | 8.5          | 8.6          | 8.7          | 8.8          | 8.9          |
| 9. Maintenance  | 9.1          | 9.2          | 9.3          | 9.4          | 9.5          | 9.6          | 9.7          | 9.8          | 9.9          |
| 10. Media Protection                                    | 10.1         | 10.2         | 10.3         | 10.4         | 10.5         | 10.6         | 10.7         | 10.8         | 10.9         |
| 11. Physical and Environmental Protection               | 11.1         | 11.2         | 11.3         | 11.4         | 11.5         | 11.6         | 11.7         | 11.8         | 11.9         |
| 12. Planning  | 12.1         | 12.2         | 12.3         | 12.4         | 12.5         | 12.6         | 12.7         | 12.8         | 12.9         |
| 13. Personnel Security                                  | 13.1         | 13.2         | 13.3         | 13.4         | 13.5         | 13.6         | 13.7         | 13.8         | 13.9         |
| 14. Risk Assessment                                     | 14.1         | 14.2         | 14.3         | 14.4         | 14.5         | 14.6         | 14.7         | 14.8         | 14.9         |
| 15. System and Services Acquisition                     | 15.1         | 15.2         | 15.3         | 15.4         | 15.5         | 15.6         | 15.7         | 15.8         | 15.9         |
| 16. System and Communications Protection                | 16.1         | 16.2         | 16.3         | 16.4         | 16.5         | 16.6         | 16.7         | 16.8         | 16.9         |
| 17. System and Information Integrity                    | 17.1         | 17.2         | 17.3         | 17.4         | 17.5         | 17.6         | 17.7         | 17.8         | 17.9         |
| Please complete the following information               |              |              |              |              |              |              |              |              |              |
| Agency Name   |              |              |              |              |              |              |              |              |              |
| System Name and Title                                   |              |              |              |              |              |              |              |              |              |

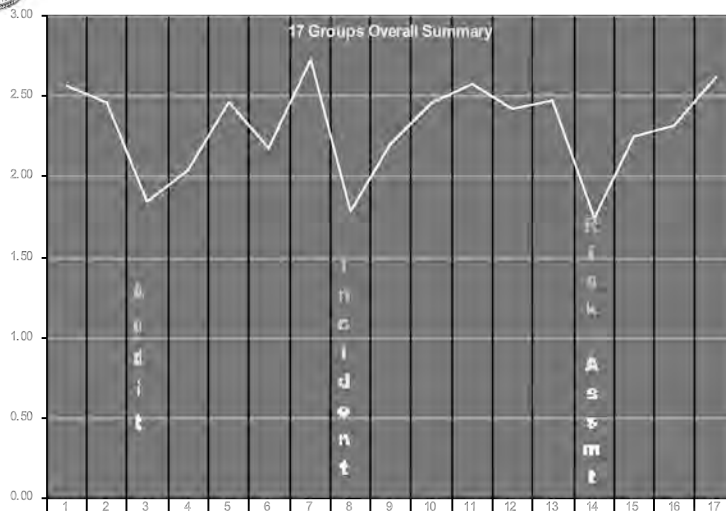


## ITEC Security Council Security Self-Assessment SSA 26-1 Worksheet Line 302...

| Security Control  | Rating | Enter in Column C:<br>Comments or Cross References to Policies / Procedures | Col D:<br>Initials of<br>Person<br>Completing |
|---|--------|---|---|
| <b>2. Awareness and Training</b> <span style="float: right;">Class: Optional</span><br>Organizations must: (i) ensure that managers and users of organizational information systems are made aware of the security risks associated with their activities and of the applicable laws, executive orders, directives, policies, standards, instructions, regulations, or procedures related to the security of organizational information systems; and (ii) ensure that organizational personnel are adequately trained to carry out their assigned information security-related duties and responsibilities. |        |   |   |
| Enter in Col. B for each control, (AC-1.1AC-12 etc.):<br>0- We do not do at all<br>1- We have an Informal Practice Only<br>2- We have written Policy or Procedures<br>3- We have Written Policy & Procedures Implemented<br>4- We have Written Procedures Reviewed & Tested<br>n/a- It is not applicable for us   |        |   |   |
| <b>AT-1 Security Awareness and Training Policy and Procedures</b><br><b>Control:</b> The organization develops, documents, and periodically reviews/updates: (i) a formal, documented, security awareness and training policy that addresses purpose, scope, roles, responsibilities, management commitment, coordination among organizational entities, and compliance; and (ii) formal, documented procedures to facilitate the implementation of the security awareness and training policy and associated security awareness and training controls.   |        |   |   |
| <b>AT-1.1</b><br>Examine organizational records or documents to determine if security awareness and training policy and procedures: (i) exist, (ii) are documented, (iii) are disseminated to appropriate elements within the organization, (iv) are periodically reviewed or responsible parties within the organization; and (v) are updated when organizational threat indicators require updates.   |        |   |   |
| <b>AT-1.2</b><br>Examine the security awareness and training policy to determine if the policy adequately addresses purpose, scope, roles, responsibilities, management commitment, coordination among organizational entities, and compliance.   |        |   |   |
| <b>AT-1.3</b><br>Examine the security awareness and training procedures to determine if the procedures are sufficient to address all areas identified in the security awareness and training policy and all associated security awareness and training controls.  |        |   |   |



## ITEC Security Council Security Self-Assessment Results have been tabulated





## **ITEC Security Council Security Self-Assessment Observations**

The 2006 SSA is far more granular than previous ones. Due to turnover, some agency evaluators were seeing the SSA for the first time.

As expected, the overall scores were somewhat lower than previous years.

There were some significant outliers in the rankings reported by some agencies.

Three control groups overall average were below 2.00- Audit and Accountability, Incident Response, and Risk Assessment.

19



## **ITEC Security Council Security Self-Assessment Recommendations for 2007**

Conduct training sessions for the evaluators to help ensure consistency of scoring, and interpretation of what the 0-4 levels entail.

Ensure agencies without written security policies adopt at a minimum the state default policy. This would result in some scores coming up to the 2.0 level.

For those agencies that scored less than 2.0 for any major control, their goal should be to improve to a minimum 2.0 for each control. The score of 2.0 was selected because written policies are generally considered as essential in developing an organized system of security in an agency.

The Council believes an agency which completes the necessary steps in developing a written policy or procedure examines important security issues, and in time, is more likely to move their score higher by implementing the policy (3.0) and then solidly integrating it into the agency (4.0).

20



## ITEC Security Council Security Self-Assessment Recommendations for 2007

For those agencies that scored at or above 2.0 for each major control to work toward scoring a minimum 3.0. This would indicate that the written policies/procedures have been implemented and in standard use.

The Security Council has recently developed an Incident Response Protocol which will help in the Incident Response area.

Modify the 2006 SSA to include the 15 additions from the final version of 800-53 just released in December.

Include the questions or procedures from 800-53A to be released in March .

21



## ITEC Security Council Security Self-Assessment Results have been tabulated



22



Securing the Enterprise

# Kansas ITEC Security Council

23



## **CSO Conference**



**Kansas Statewide Security Contract**  
**March 7, 2007**

24



## **IT Security Hardware, Software and Related Security Services Contract Award-RFP 07745**

### **Contract Background**

ITEC Security Council started work on the RFP -April 2004

RFP issued on October 20 and closed on December 1, 2004

30 Technical Responses evaluated by December 31, 2004

Cost Proposals evaluated by January 12, 2005

Security Council unanimously approves recommendations and empowers PNC to negotiate with 7 vendors -January 13

Conference calls with vendors completed by January 28

Preliminary contract awards dated February 10 and posted on website on February 23

ITEC Security Council briefed -February 24

25



## **IT Security Hardware, Software and Related Security Services Contract Award-RFP 07745**

### **Key Contract Features:**

**Period of Contract February 10, 2005 through February 9, 2007**

**Option to renew for two one year periods**

**All state, regents, county and local units of government can purchase off of this contract as well as K-12 education organizations**

**Will provide tracking of expenditures under the contract**

26



## **IT Security Hardware, Software and Related Security Services Contract Award-RFP 07745**

### **Key Category Features:**

#### **11 Categories**

**Firewalls**

**VPNs**

**IDS**

**IPS**

**Wireless ( No award)**

**Virus Management**

**Authentication and Authorization**

**Encryption**

**Hard Authentication (Tokens)**

**Tools**

**Services**

27



## **IT Security Hardware, Software and Related Security Services Contract Award-RFP 07745**

### **Key Features:**

#### **Tools**

**Vulnerability Scanning**

**Patch Management,**

**Monitoring and Log Analysis,**

**Workstation Policy Assurance**

**Spam Management**

**Web Filtering**

#### **Services**

**Security Planning and Design**

**Vulnerability Assessment**

**Penetration Testing**

**Network and Server monitoring**

**End User Security**

**Technical Security Training**

**Managed Security Services**

28



## **IT Security Hardware, Software and Related Security Services Contract Award-RFP 07745**

### **Key Vendor Features:**

#### **Preliminary Award (Now)**

**Fishnet -HW/SW/Services**

**ISG Technology - HW/SW/Services**

**World Wide Technology -HW/SW/Services**

**McAfee HW/SW through Fishnet or SW through LAR**

**Symantec HW/SW through ISG and WWT**

#### **Purchasing working on additional awards**

**Symantec for Services**

**Qwest for Services**

**IBM for HW/SW/Services**

29



## **IT Security Hardware, Software and Related Security Services Contract Award-RFP 07745**

### **Key Features:**

**Can order Trend, Patchlink, Surf Control, Websense, Archer  
Technologies, Insystek off of LAR with SHI**

**Qualys can be ordered through Fishnet**

**Red Siren through Qwest**

#### **Task Order (TO) Process for Services**

**Send TO to all vendors on contract award**

**Can select which one you want, not necessarily the low bidder**

30



## **IT Security Hardware, Software and Related Security Services Contract Refresher**

### **BACKGROUND**

**March 2006 -Security Council starts discussing additions to be added to the contract**

**April - Subcommittees develop suggested new product categories**

**May - Security Council approves recommendations**

**June - Purchasing determines only currently approved vendors under the original 07745 contract are eligible for refresher and only for those categories for which they were approved at that time**

**This reduces field to 3 vendors and letters sent requesting them to make offerings for the new additions by end of July**

**August – Responses evaluated – Security Council unanimously approves recommendation to add all new offerings to the contract**

**September – Purchasing works on Addendum # 2 to 07745**

**October – Addendum # 2 published to website**

31



## **IT Security Hardware, Software and Related Security Services Contract Refresher**

### **NEW ADDITIONS**

**Category 4- IPS: Web Session Security Appliances**

**Fishnet- Imperva, F5, Crossbeam ISG-Cisco WWT- Cisco, Symantec**

**Category 6- Virus Management: Spyware Detection/Removal**

**Fishnet- Webroot ISG- Cisco WWT- Cisco, Symantec**

**Category 7 Authentication & Authorization**

**Secure E-mail: ISG- Cisco (Fishnet and WWT opt out)**

**Secure Remote Access: Fishnet –F5 ISG-Cisco (WWT opt out)**

**Identity Management: ISG- Cisco (Fishnet and WWT opt out)**

**Secure Instant Messaging: Fishnet- Akonix ISG-Cisco (WWT opt out)**

**Category 8- Encryption: Encryption for mobile devices**

**Fishnet –Utimaco (ISG and WWT not eligible)**

**Category 10 –Tools Subcat A-Vulnerability Scanning**

**Web Programming Applications Security: Fishnet- SpyDynamics**

**WWT- SOW-Symantec (ISG Opt out)**

32



## **IT Security Hardware, Software and Related Security Services Contract Refresher**

### **KDOR Plans to use refresher:**

#### **Secure Remote Access:**

- F5 FirePass SSL VPN appliance

No additional client software- just need browser

Policy enforcement for AV, Firewall, Quarantine Automatic Integration for Remediation

Support Host and Portal Access, Application tunnels, Citrix, etc, Lotus Notes

#### **Laptop Encryption:**

- Utimaco

SafeGuard Easy –Full disk Encryption ( Sector level, pre-boot authorization)

Can also encrypt USB Drives, external hard drives,

#### **Wireless Connectivity**

- Cellular Wireless Cards