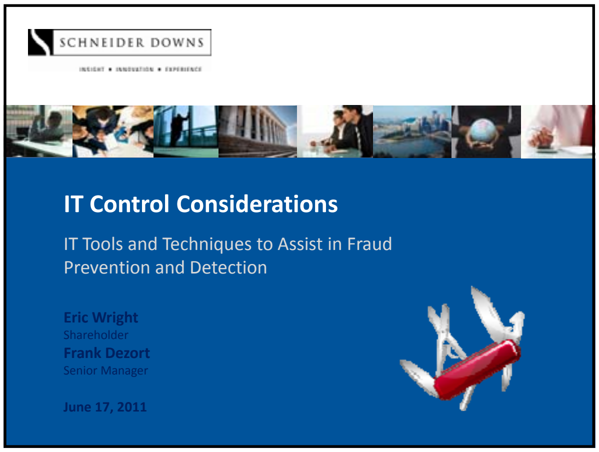


SCHNEIDER DOWNS

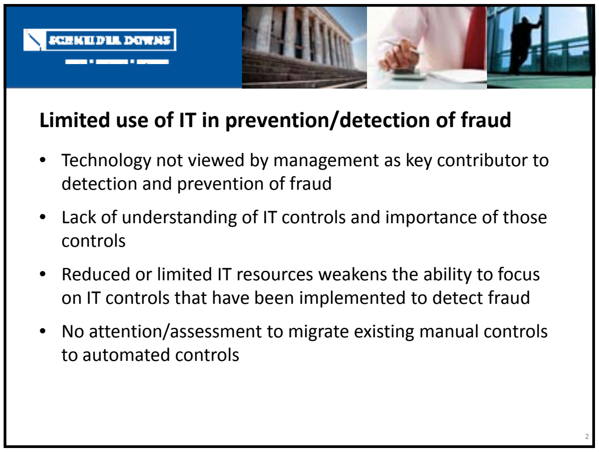
INSIGHT • INNOVATION • EXPERIENCE

IT Control Considerations

IT Tools and Techniques to Assist in Fraud Prevention and Detection

Eric Wright
Shareholder
Frank Dezort
Senior Manager

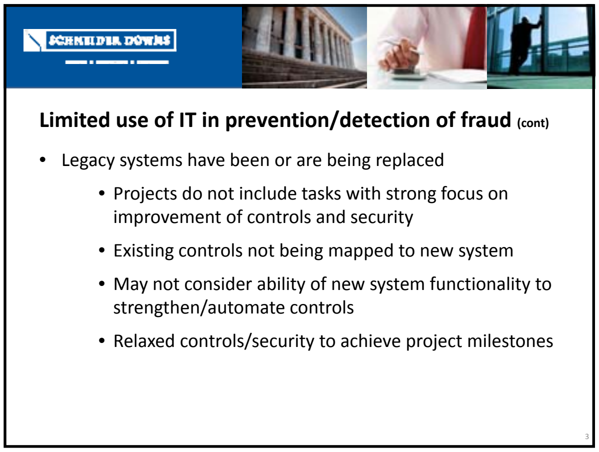
June 17, 2011



Limited use of IT in prevention/detection of fraud

- Technology not viewed by management as key contributor to detection and prevention of fraud
- Lack of understanding of IT controls and importance of those controls
- Reduced or limited IT resources weakens the ability to focus on IT controls that have been implemented to detect fraud
- No attention/assessment to migrate existing manual controls to automated controls

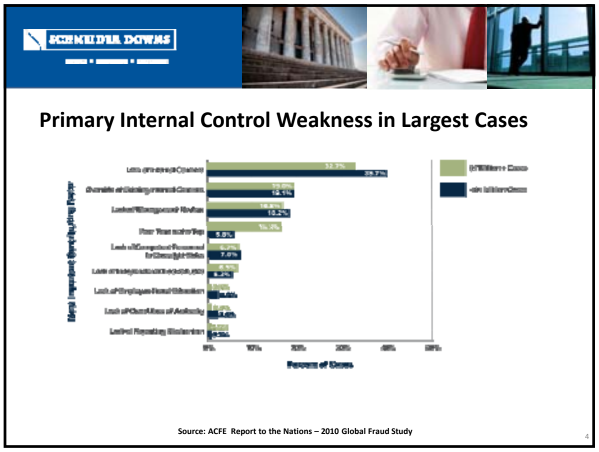
2



Limited use of IT in prevention/detection of fraud (cont)

- Legacy systems have been or are being replaced
  - Projects do not include tasks with strong focus on improvement of controls and security
  - Existing controls not being mapped to new system
  - May not consider ability of new system functionality to strengthen/automate controls
  - Relaxed controls/security to achieve project milestones

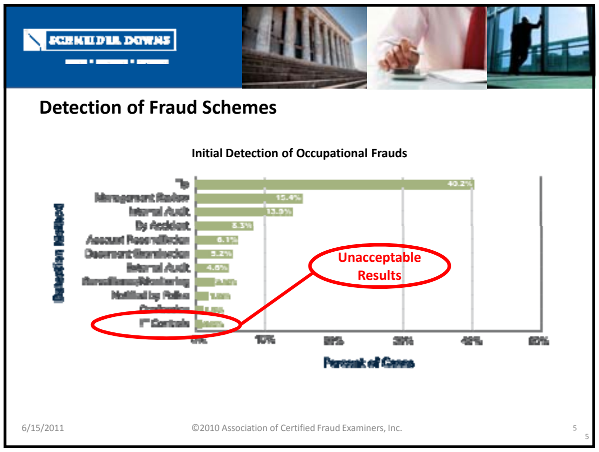
3



Primary Internal Control Weakness in Largest Cases

Source: ACFE Report to the Nations – 2010 Global Fraud Study

4



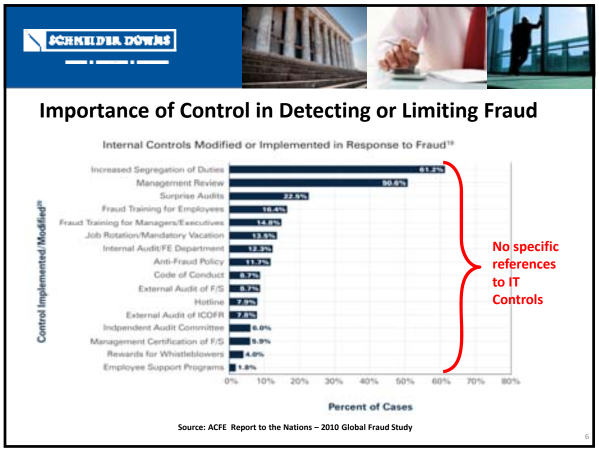
Detection of Fraud Schemes

Initial Detection of Occupational Frauds

Unacceptable Results

6/15/2011 ©2010 Association of Certified Fraud Examiners, Inc. 5

5



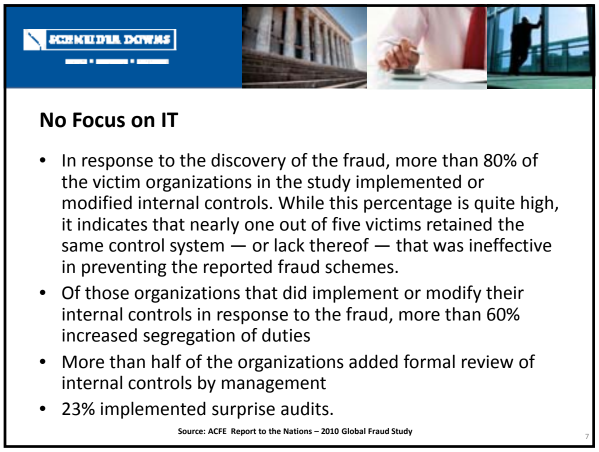
Importance of Control in Detecting or Limiting Fraud

Internal Controls Modified or Implemented in Response to Fraud[19]

No specific references to IT Controls

Source: ACFE Report to the Nations – 2010 Global Fraud Study

6

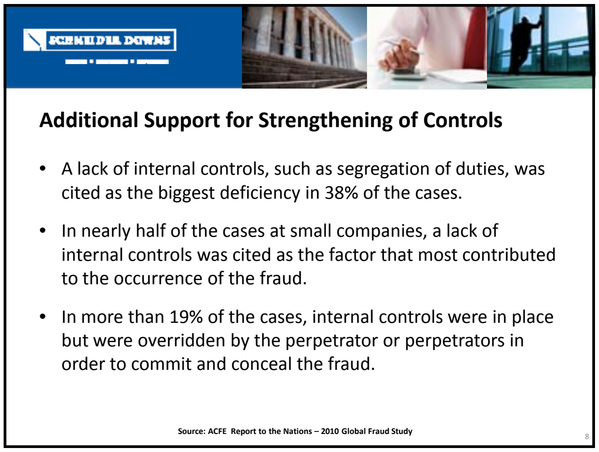


No Focus on IT

- In response to the discovery of the fraud, more than 80% of the victim organizations in the study implemented or modified internal controls. While this percentage is quite high, it indicates that nearly one out of five victims retained the same control system — or lack thereof — that was ineffective in preventing the reported fraud schemes.
- Of those organizations that did implement or modify their internal controls in response to the fraud, more than 60% increased segregation of duties
- More than half of the organizations added formal review of internal controls by management
- 23% implemented surprise audits.

Source: ACFE Report to the Nations – 2010 Global Fraud Study

7

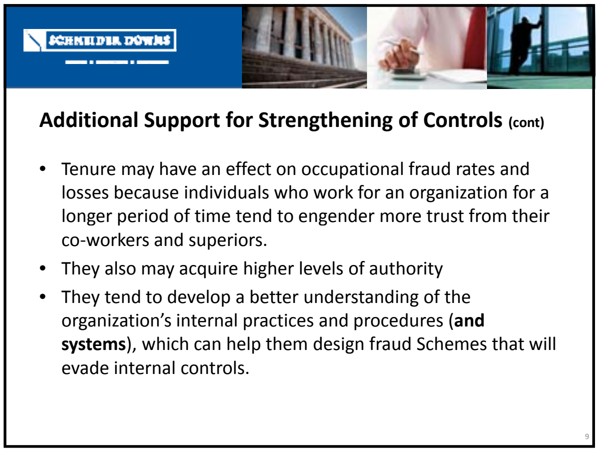


Additional Support for Strengthening of Controls

- A lack of internal controls, such as segregation of duties, was cited as the biggest deficiency in 38% of the cases.
- In nearly half of the cases at small companies, a lack of internal controls was cited as the factor that most contributed to the occurrence of the fraud.
- In more than 19% of the cases, internal controls were in place but were overridden by the perpetrator or perpetrators in order to commit and conceal the fraud.

Source: ACFE Report to the Nations – 2010 Global Fraud Study

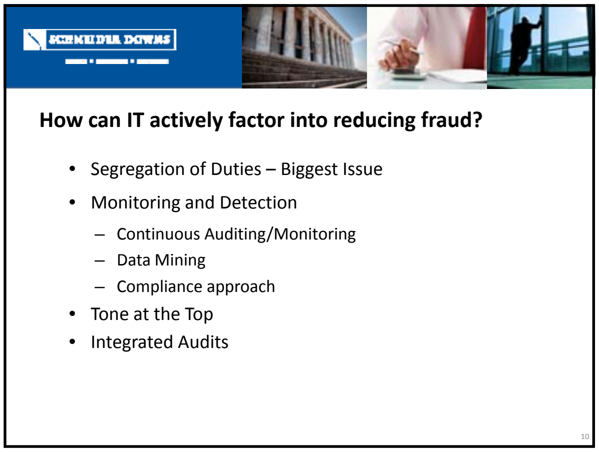
8



Additional Support for Strengthening of Controls (cont)

- Tenure may have an effect on occupational fraud rates and losses because individuals who work for an organization for a longer period of time tend to engender more trust from their co-workers and superiors.
- They also may acquire higher levels of authority
- They tend to develop a better understanding of the organization's internal practices and procedures (**and systems**), which can help them design fraud Schemes that will evade internal controls.

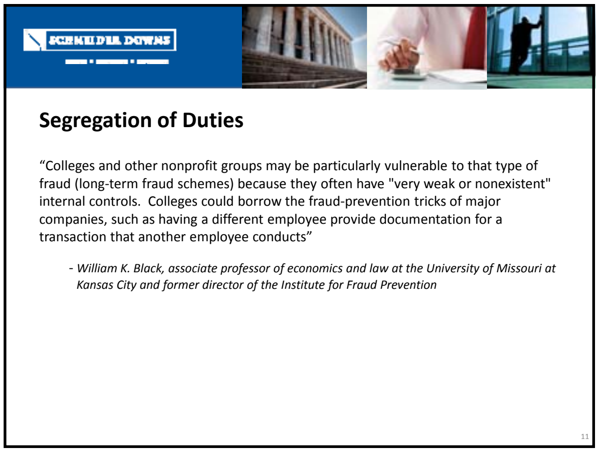
9



How can IT actively factor into reducing fraud?

- Segregation of Duties – Biggest Issue
- Monitoring and Detection
  - Continuous Auditing/Monitoring
  - Data Mining
  - Compliance approach
- Tone at the Top
- Integrated Audits

10

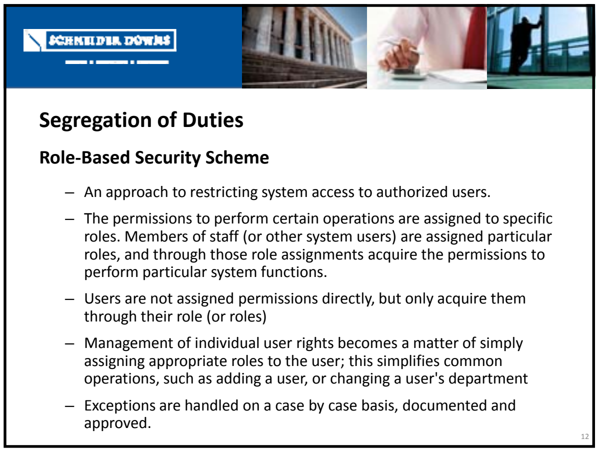


Segregation of Duties

“Colleges and other nonprofit groups may be particularly vulnerable to that type of fraud (long-term fraud schemes) because they often have "very weak or nonexistent" internal controls. Colleges could borrow the fraud-prevention tricks of major companies, such as having a different employee provide documentation for a transaction that another employee conducts”

- William K. Black, associate professor of economics and law at the University of Missouri at Kansas City and former director of the Institute for Fraud Prevention

11



Segregation of Duties

Role-Based Security Scheme

- An approach to restricting system access to authorized users.
- The permissions to perform certain operations are assigned to specific roles. Members of staff (or other system users) are assigned particular roles, and through those role assignments acquire the permissions to perform particular system functions.
- Users are not assigned permissions directly, but only acquire them through their role (or roles)
- Management of individual user rights becomes a matter of simply assigning appropriate roles to the user; this simplifies common operations, such as adding a user, or changing a user's department
- Exceptions are handled on a case by case basis, documented and approved.

12

Define security roles

Close the Books Process

Defined Roles Transactions	Enter and Post JE	G/L Setup	Comments
Close the Books			
Closing Transactions			
Posting Journal Entries	X	X	
Approving Journal Entries	X	X	Compensating control for approval is a manual control residing outside of App
Generate Reoccuring Journal Entries	X	X	
Initiation of Reversing Entries	X	X	
Closing Maintenance			
Closing Accounting Periods		X	
Update Foreign Currency Rate Table		X	
Maintain Chart of Accounts		X	
Access to Direct G/L Posting		X	
Setup Calendar Year		X	

Approval of Roles	
CFO Signature:	Date:
IT Manager Signature:	Date:

Review of the "Xs" in a column to determine if SOD issues exist

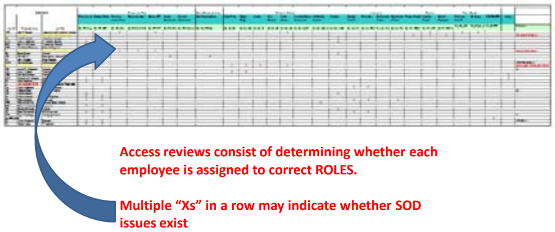
Define security roles

Payroll Process

Defined Roles Transactions	Process Payroll	Approve Payroll	Maintain Employees
Payroll			
Payroll Transactions			
Enter Hourly Payroll	X		
Enter Salary Payroll	X		
Process Payroll	X		
Approve Payroll		X	
Print Checks / Generate ACH File	X		
Transmit ACH File to Bank	X		
Payroll Maintenance			
Maintains Employee Records			X
Approves Wage and Salary Increases			X

Approval of Roles	
CFO Signature:	Date:
IT Manager Signature:	Date:

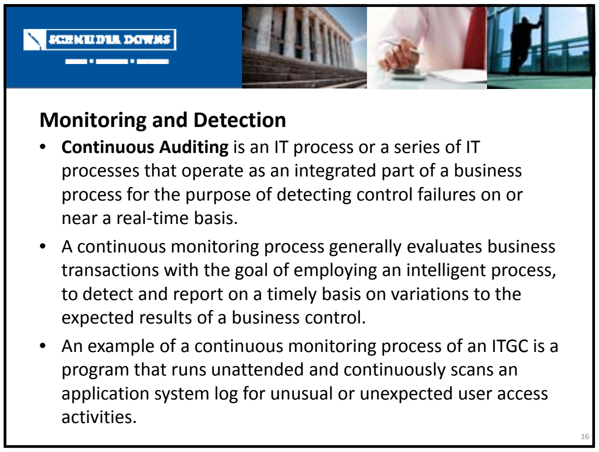
Add employees to roles



Access reviews consist of determining whether each employee is assigned to correct ROLES.

Multiple "Xs" in a row may indicate whether SOD issues exist

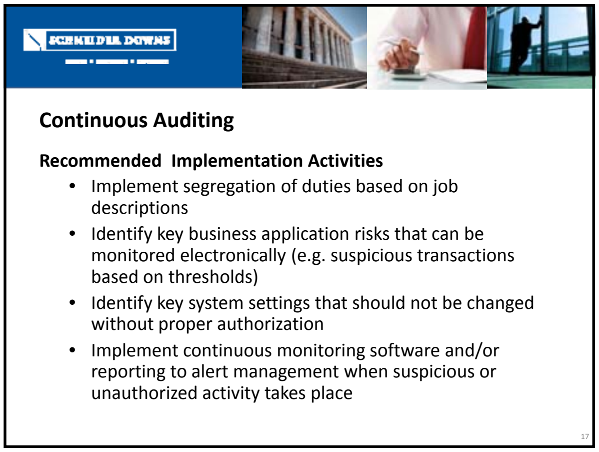
Includes "SUPER" or "ADMIN" access roles



Monitoring and Detection

- **Continuous Auditing** is an IT process or a series of IT processes that operate as an integrated part of a business process for the purpose of detecting control failures on or near a real-time basis.
- A continuous monitoring process generally evaluates business transactions with the goal of employing an intelligent process, to detect and report on a timely basis on variations to the expected results of a business control.
- An example of a continuous monitoring process of an ITGC is a program that runs unattended and continuously scans an application system log for unusual or unexpected user access activities.

16

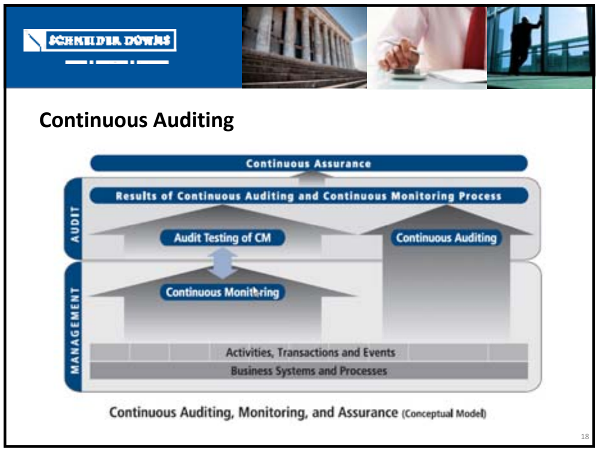


Continuous Auditing

Recommended Implementation Activities

- Implement segregation of duties based on job descriptions
- Identify key business application risks that can be monitored electronically (e.g. suspicious transactions based on thresholds)
- Identify key system settings that should not be changed without proper authorization
- Implement continuous monitoring software and/or reporting to alert management when suspicious or unauthorized activity takes place

17

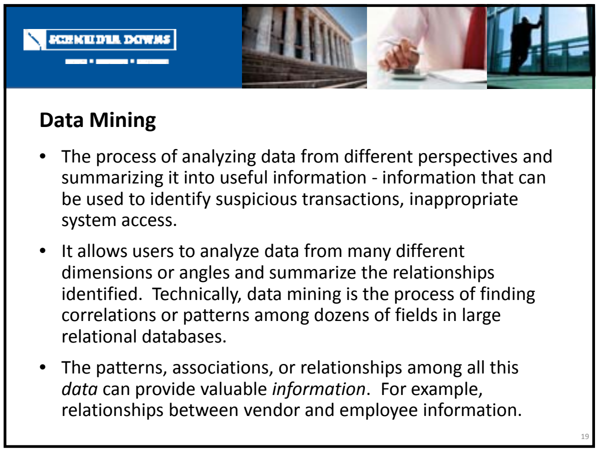


Continuous Auditing

Continuous Assurance
Results of Continuous Auditing and Continuous Monitoring Process
AUDIT
Audit Testing of CM
Continuous Auditing
MANAGEMENT
Continuous Monitoring
Activities, Transactions and Events
Business Systems and Processes

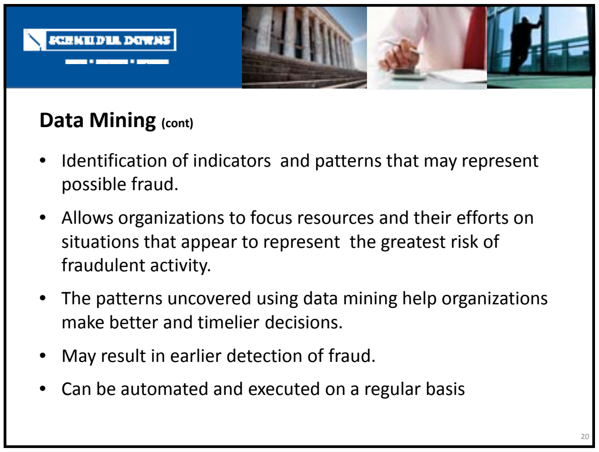
Continuous Auditing, Monitoring, and Assurance (Conceptual Model)

18



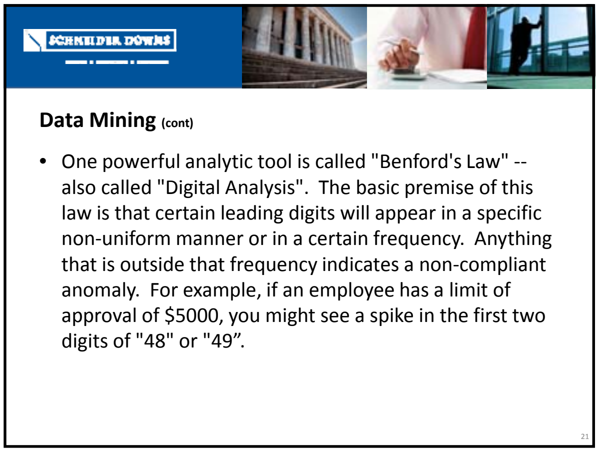
Data Mining

- The process of analyzing data from different perspectives and summarizing it into useful information - information that can be used to identify suspicious transactions, inappropriate system access.
- It allows users to analyze data from many different dimensions or angles and summarize the relationships identified. Technically, data mining is the process of finding correlations or patterns among dozens of fields in large relational databases.
- The patterns, associations, or relationships among all this *data* can provide valuable *information*. For example, relationships between vendor and employee information.



Data Mining (cont)

- Identification of indicators and patterns that may represent possible fraud.
- Allows organizations to focus resources and their efforts on situations that appear to represent the greatest risk of fraudulent activity.
- The patterns uncovered using data mining help organizations make better and timelier decisions.
- May result in earlier detection of fraud.
- Can be automated and executed on a regular basis



Data Mining (cont)

- One powerful analytic tool is called "Benford's Law" -- also called "Digital Analysis". The basic premise of this law is that certain leading digits will appear in a specific non-uniform manner or in a certain frequency. Anything that is outside that frequency indicates a non-compliant anomaly. For example, if an employee has a limit of approval of $5000, you might see a spike in the first two digits of "48" or "49”.

SCHNEIDER DOWNS

Data Mining Examples

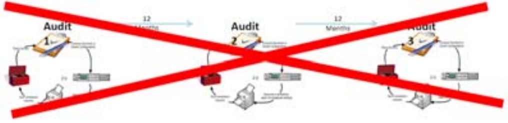
- Payroll
- Grade Changes

- Procurement
- Travel Expenses

SCHNEIDER DOWNS

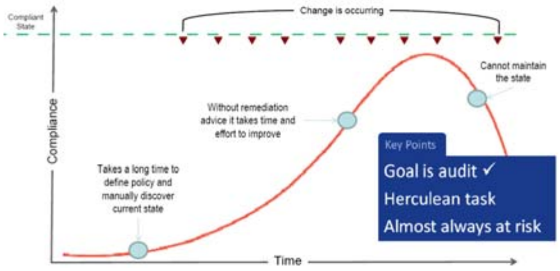
Compliance Approach

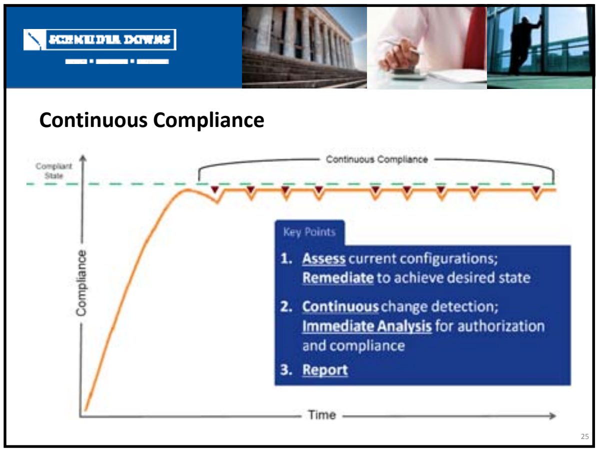
- Compliance viewed as:
  - Necessary evil
  - Projects rather than a culture of leading practices
  - A milestone rather than an approach
  - A checkbox rather than a strategy
  - Discreet steps versus a continuous process
  - Development of programs specifically to pass a compliance audit



SCHNEIDER DOWNS

Static Compliance Model

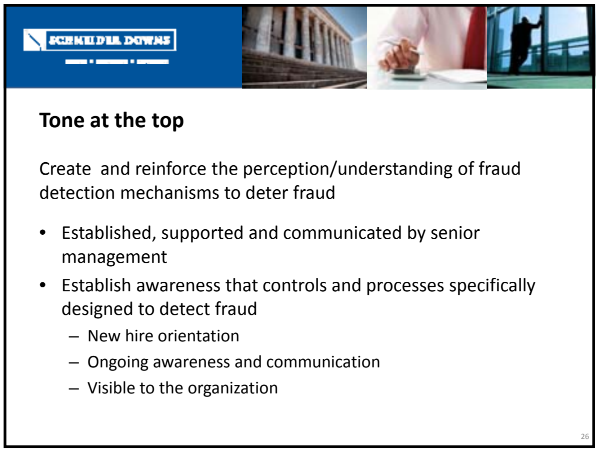

Compliant State
Change is occurring
Compliance
Time
Takes a long time to define policy and manually discover current state
Without remediation advice it takes time and effort to improve
Cannot maintain the state
Key Points
Goal is audit ✓
Herculean task
Almost always at risk



Continuous Compliance

Key Points

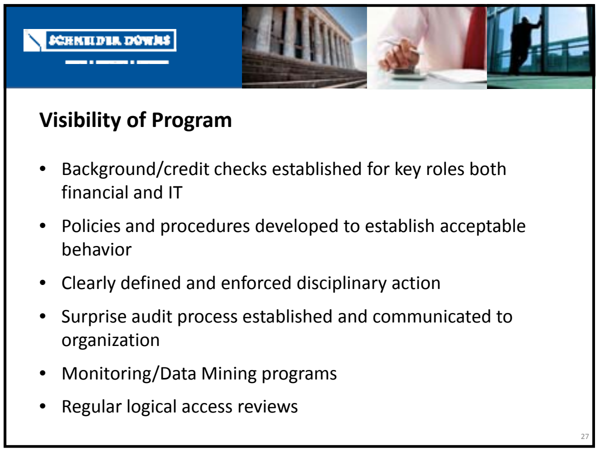
1. **Assess** current configurations; **Remediate** to achieve desired state
2. **Continuous** change detection; **Immediate Analysis** for authorization and compliance
3. **Report**



Tone at the top

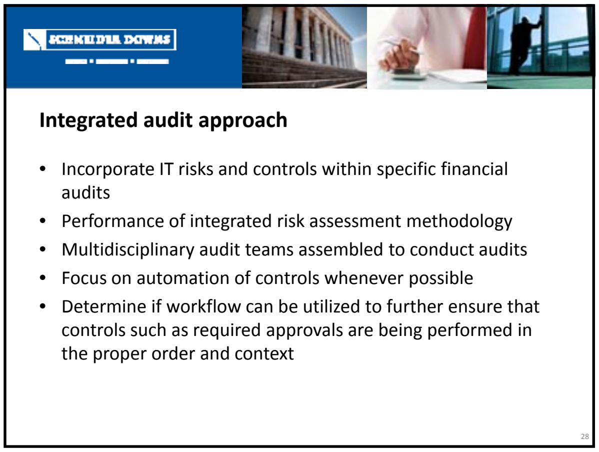
Create and reinforce the perception/understanding of fraud detection mechanisms to deter fraud

- Established, supported and communicated by senior management
- Establish awareness that controls and processes specifically designed to detect fraud
  - New hire orientation
  - Ongoing awareness and communication
  - Visible to the organization



Visibility of Program

- Background/credit checks established for key roles both financial and IT
- Policies and procedures developed to establish acceptable behavior
- Clearly defined and enforced disciplinary action
- Surprise audit process established and communicated to organization
- Monitoring/Data Mining programs
- Regular logical access reviews



Integrated audit approach

- Incorporate IT risks and controls within specific financial audits
- Performance of integrated risk assessment methodology
- Multidisciplinary audit teams assembled to conduct audits
- Focus on automation of controls whenever possible
- Determine if workflow can be utilized to further ensure that controls such as required approvals are being performed in the proper order and context