Socializing your Risk Assessment Information with the C-Suite

@2013 JCPenney. All rights reserved.

Formulating a Risk Assessment Approach

- Ongoing and continuous process
- Conduct “in person” audits
- Gather knowledge and understanding
- Ensure complete audit universe

@2013 JCPenney. All rights reserved.

Vetting your Findings

- Provide audit universe and assessment tool to team with plenty of lead time prior to bringing audit team together
- Use sources and resources to clarify thoughts prior to meeting with team
- Trust your assessment tool
- Don’t get stuck in the weeds

@2013 JCPenney. All rights reserved.

Risk Assessment Template for 2014 Audit Planning - TeamRisk Scoring Model

Input Values	Description
1	NA
2	1=NA, Assess from 2 (Inconsequetial-Rare) to 10 Significant-Almost Certain)
3	
4	
5	
6	
7	
8	
9	
10	

Likelihood	Impact: Insignificant	Minor	Moderate	Major	Significant
Almost Certain	5	6	8	9	10
Likely	4	5	7	8	9
Possible	3	4	6	7	8
Unlikely	2	3	5	6	7
Rare	2	2	4	5	6

Overall Scoring Thresholds			
10	38	Green	Low
38	52.5	Yellow	Medium
52.5	100	Red	High

Entity Color Legend

- Deleted for 2014
- New for 2014
- Something Changed

Auditable Entities

Area	Category	Subcategory	Staffing Area Audit Team Inputs: Regulatory/ Legal Compliance	Fraud Ethic	Value Chain (Operational Risks)	Financi	People	Information Technolog	Overall Score	Tier	Comments - For Risk Factors Rated 9 or 10, or Overall Scores i High Range, note specific risk considerations that contributed t assessment score.
IT	Operations	Asset Management	5	5	5	5	5	5	50.00	Medium	
IT	Operations	Change Control	5	5	6	5	6	5	53.75	High	
IT	Operations	Data Centers	8	4	4	4	5	4	52.76	High	
IT	Operations	Call Centers	4	4	5	4	4	8	52.76	High	
IT	Operations	Desktop Management	9	1	1	1	1	1	61.43	High	
IT	Operations	Disaster Recovery	8	8	8	8	8	8	80.00	High	

Presenting your findings

- Risk rank your selected findings
- Develop a proposed time line for addressing identified items
- Share your findings with IT partners prior to meeting with Executive Leadership
- Keep discussion at a high level

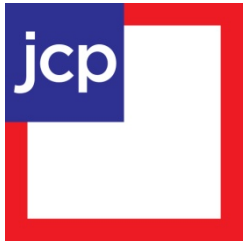
@2013 JCPenney. All rights reserved.

Developing a Partnership

- Meet with IT partners on a regular basis
- Engage in open dialogue
- Partnership has to be two-sided
- The ultimate goal is the betterment of the Enterprise and not an opportunity for “gotcha”

]

@2013 JCPenney. All rights reserved.



Risk Partnership

© 2012 jcpenney. All rights reserved. Proprietary and Confidential

Inputs into the Risk Management Roadmap

- Inputs into the roadmap include:
  - Business and IT Strategic Roadmap
  - IT Tactical Plan for that year
  - Verizon DBIR and other state of security reports
  - Results of assessments and audits

- Internal Audit meets quarterly with IT Executives to discuss
  - Audit remediation
  - Areas in need of security review

IT partners with Internal Audit for Board Reporting

- IT notes key risks for the coming year
- Inherit and Residual Risk are calculated to produce mitigation plan

IT Threat Assessment

ID	Threat Category	Threat	Description	Vulnerability	Risk	Likelihood	Impact	Controls	Additional Steps for Mitigation
11	Internal Non-Malicious	Availability of Excess Privileges	Elevated privileges throughout the architecture (database, network and system areas) are not properly managed	Lack of traceability on system modifications	Misuse of privileges or unintended of modification of data			-Quarterly Access Reviews for PCI/SOX applications -Password Vault for admin access on Windows and some Unix systems for PCI/SOX applications	-QAR for all systems -Password Vault for all admin access
12	Internal Non-Malicious	Control Maturity Regression	Organization transformation has caused some regression in security controls due to unclear roles	Undocumented controls/unclear ownership	Systems and/or applications not adequately controlled or no longer compliant			-General security awareness and some targeted training	-Implementation of an Information Security Management System (ISMS) to control security holistically -Targeted security awareness for managers responsible for technical areas -Exception-based reporting

Legend

Likelihood		Impact	
Certain		Catastrophic	
Likely		Major	
Possible		Moderate	
Unlikely		Minor	
Remote		Insignificant	

Items in italics are in process or complete

Things to watch in Board discussion

- Make sure to report on key victories and how you have lowered your risk profile
- Sometimes less really is more
  - Too much detail and techno speak can confuse the discussion
  - Three or four slides are usually sufficient for a good discussion
- Your Internal Audit partner can be your best friend in these meetings, make sure you have shared the presentation with them

The day to day partnership

- IT Risk Management and Internal Audit meeting formally on a weekly basis
- Daily informal conversations are had between the leads
  - Discuss upcoming audits
    - Where and what to audit
    - Timing of audits
    - Initial findings
  - Partnering opportunities
  - What is happening in the rumor mill
- We meet together with our external audit