



# *Tailoring OCTAVE*

Johnathan Coleman, CISSP, CISM

[jc@SecurityRiskSolutions.com](mailto:jc@SecurityRiskSolutions.com)

[jpc@cert.org](mailto:jpc@cert.org)

843-442-9104

## Common OCTAVE Difficulties

- Too many Workshops
- Methodology too difficult to follow
- Too generic/not domain specific
- Some processes are tricky to get right

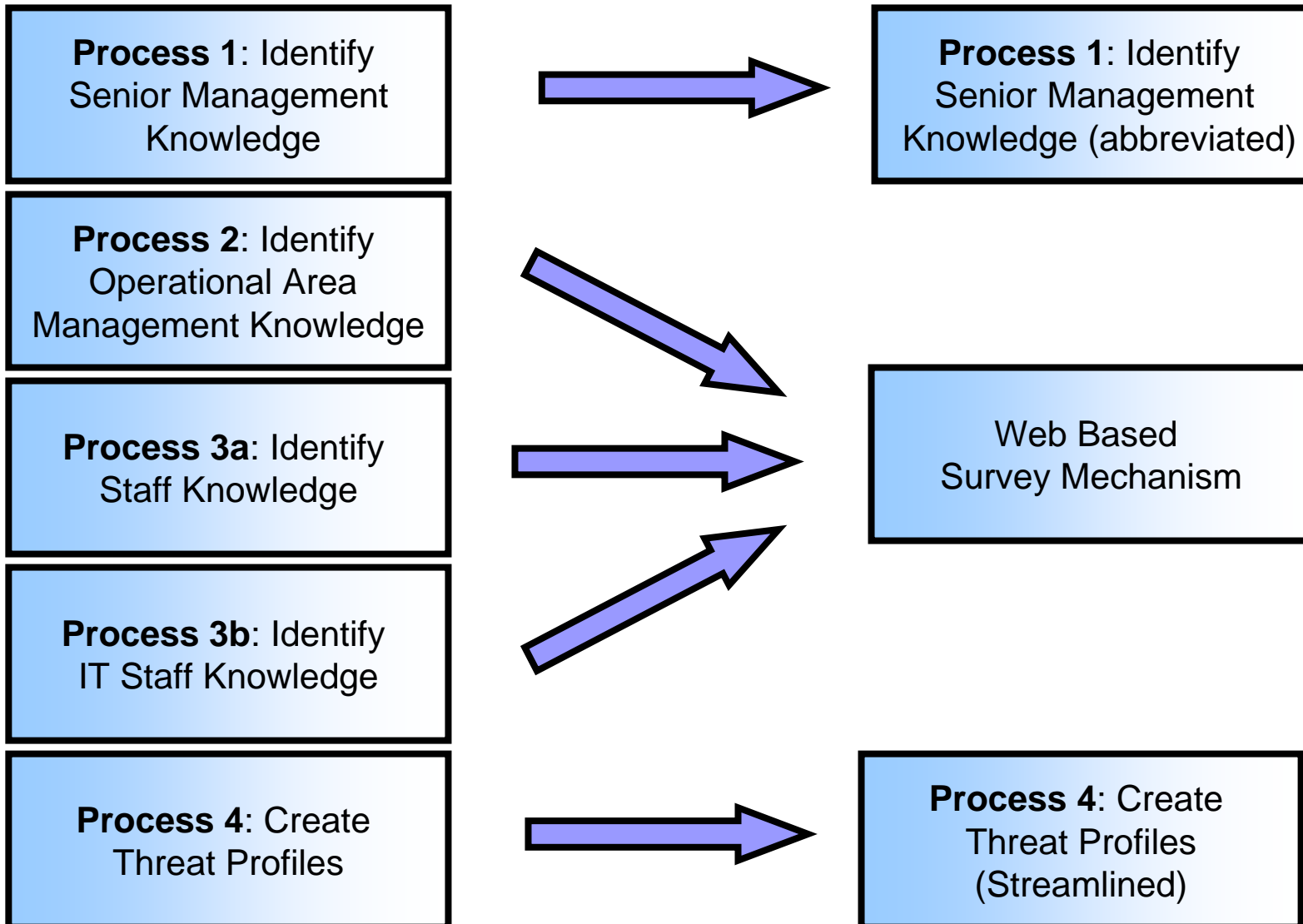
## Tailoring Opportunities

- Streamline to reduce number of workshops
- Support methodology with intuitive tools
- Include HIPAA/DoD requirements
- Simplify certain workshop activities

## Streamline methodology to reduce number of workshops

- Use an interdisciplinary, inter-hierarchical Analysis Team to provide knowledge in place of conducting all Phase 1 workshops.
- Streamline Senior Managers' Workshop to:
  - Reduce to an hour
  - Maintain SM Support and solidify commitment
  - Obtain necessary approval/sign-off for key activities (e.g. Risk Evaluation Criteria)
- **RESULT:** 1 x 1 hour Senior Managers' Knowledge Elicitation Workshop replaces 4 x multi-hour workshops

# Reduce number of Phase 1 workshops



## Web Based Survey Mechanisms

- Knowledge Elicitation Workshop time is not necessary
- OCTAVE Catalog of Practices Survey reaches a broader audience thereby:
  - Results are less refutable
  - Overall security awareness in organization is increased
  - Can be conducted concurrently with other Phase 1 and Phase 2 activities (reduces overall time needed to complete OCTAVE)
  - Easily repeatable and creates a benchmark for measurement of future efforts
- Web survey needs to capture contextual user comments (replaces workshop discussion) for use in Process 8 (Current Protection Strategies and Organizational Vulnerabilities)
- Analysis Team takes HIPAA Metrics Survey (also serves as a compliance gap analysis and allows for HIPAA specific reports to be created)

## Simplify Process 4 (Analysis Team Activity)

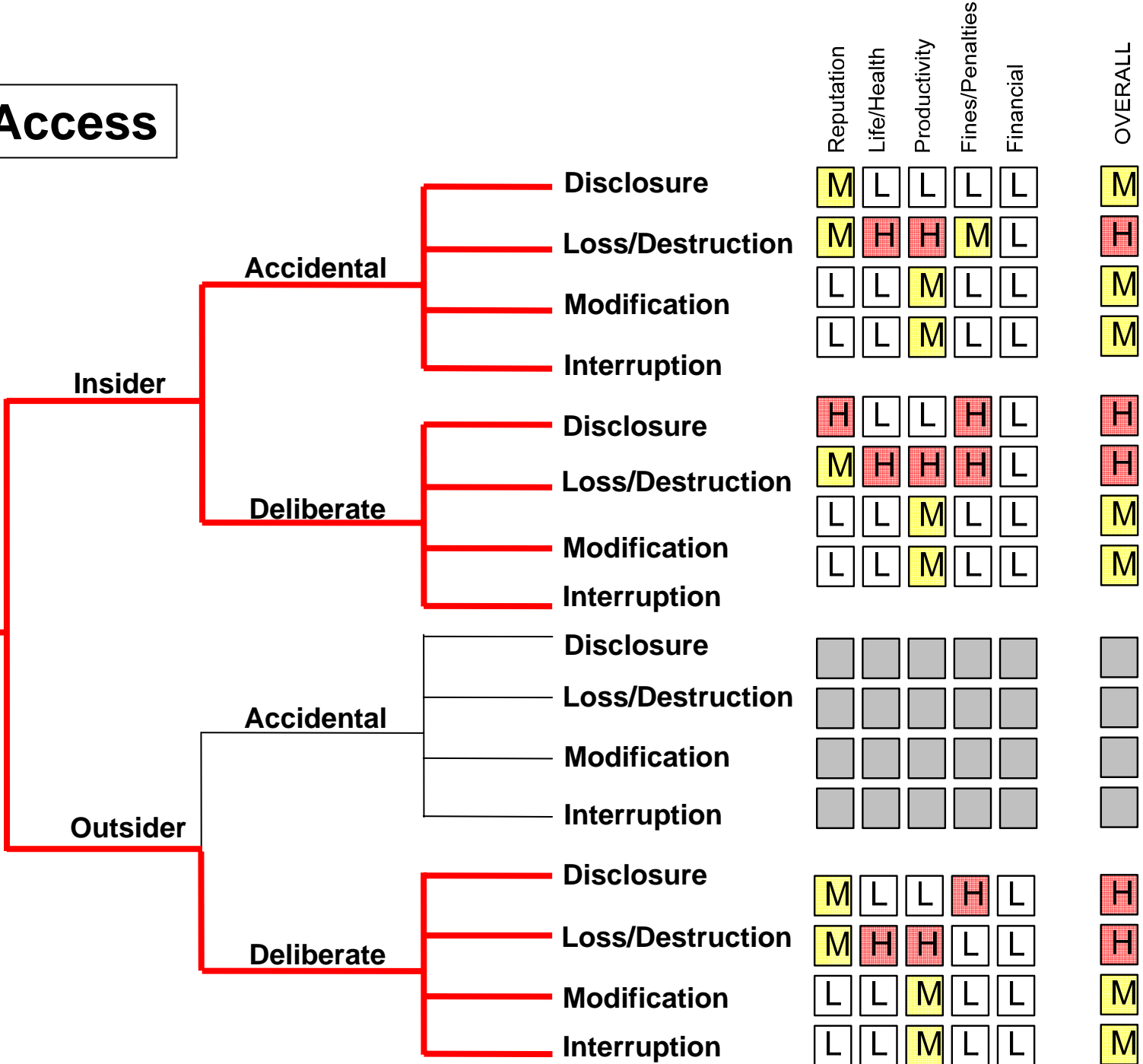
- Create Threat Profiles at same time as identifying threats to assets (reduces paperwork, threats are identified in a more logical sequence, will later serve to simplify Process 7).
- Only Identify Threats for Critical Assets
- Limit Security Requirements activity to *“Select Most Important Security Requirement”*

## Simplify Process 7

- Activity 7.1: *“Identify the Impact of Threats to Critical Assets”* is no longer necessary - it is completed as a byproduct of using the modified threat trees created in Process 4.
- Activity 7.2: *“Create Risk Evaluation Criteria”* - pre-populated and provided to Senior Management in Process 1 for discussion and approval.
- Activity 7.3: *“Evaluate the Impact of Threats to Critical Assets”* - becomes the only Process 7 activity to be completed. Modified threat trees simplify the process and make it more logical to follow.

# Network Access

# Asset



## Simplify Process 8

- Use results from web survey to create “stop-light” status of readiness in each of the 18 Catalogue of Practice Categories:
  - Creates a benchmark against which to measure improvement
  - Easy visual reference for Executive Summary Reports
  - Provides an ideal way to drive prioritization for development of protection Strategies (previously left to the discretion of the Analysis Team which can lead to confusion)
- Use modified Threat Trees to Score or Prioritize development of mitigation plans

# Catalogue Of Practices Stop-Light Status

Strategic						Operational											
1. Sec. Training	2. Sec.Strategy	3. Sec. Management	4. Sec. Policy & Reg	5. Coll Sec Mgmt	6. Cont.Planning	7. Phys Sec. P & P	8. Physical Access Cont.	9. Mon. & Audit Phys Sy.	10. Sys. & Nw. Mgt.	11.Sys. Admin Tools	12. Mon & Audit IT Sy.	13. Authent. & Auth	14.Vuln. Mgt.	15. Encryption	16. Sy. Arch. & Design	17. Incident Mgt.	18. General Staff Pract.
G	Y	G	G	G	R	G	G	Y	Y	G	G	Y	G	Y	G	R	G

## Other Tailoring Considerations

- Supplement Phase 2 with:
  - System Security Checklists (especially for systems that cannot be scanned)
  - Physical Security Reviews
- Options for Overall Sequence of Activities:
  - Parallel tracks:
    1. Web Survey => Stop-Light Status => Protection Strategies
    2. SM Workshop => Threat Profiles => Mitigation Plans
    3. Phase 2 Assessment => Action Items

# Thanks!

For more detailed information refer to handout:  
OCTAVE Mapping