MITRE ACT Overview

Nate Lee

March 2025

Document Version 3.5

MITRE

Findings are not Risks!

What's the Problem?

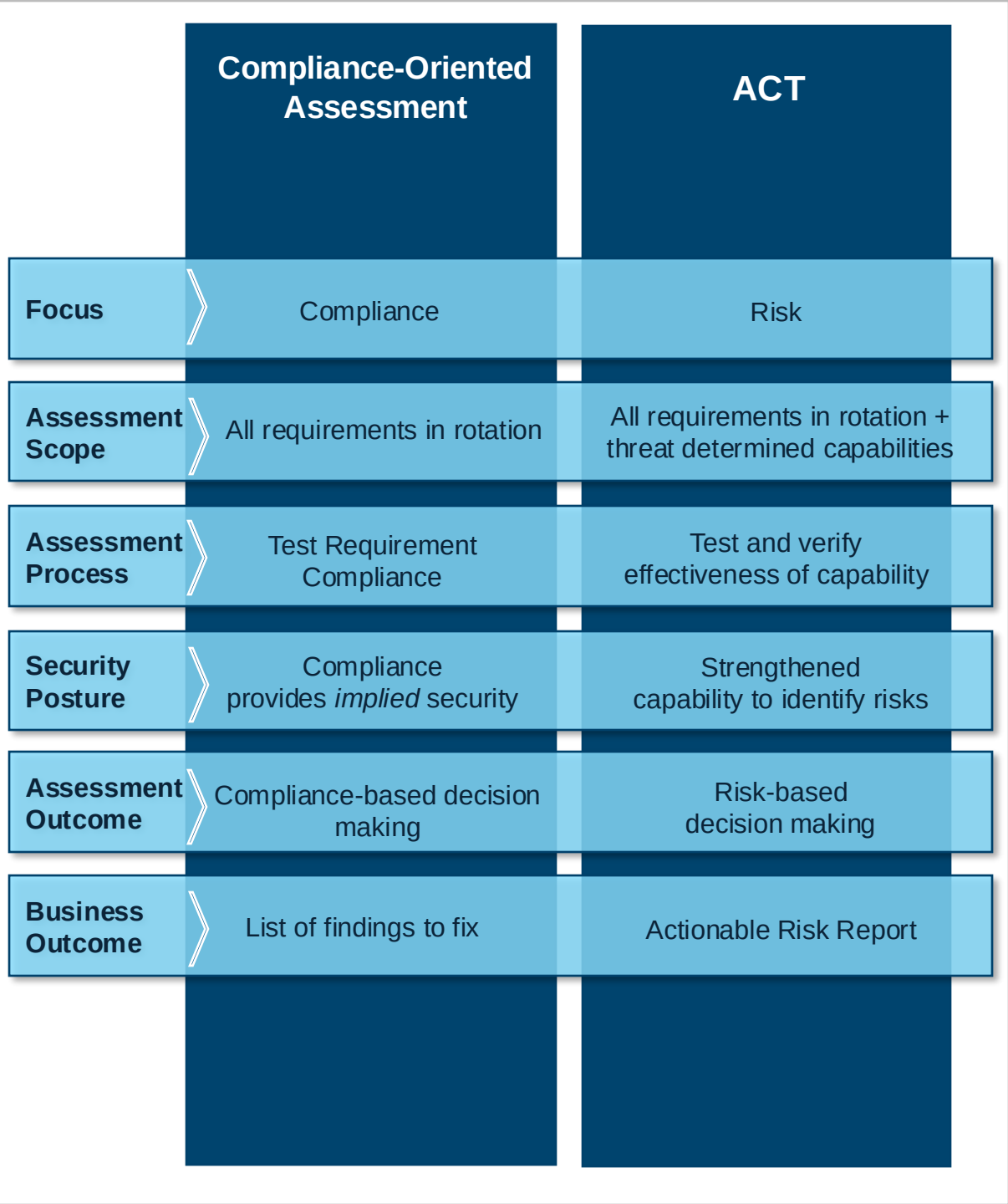
- Many Federal A&A and ATO programs suffer from similar weaknesses:
  1. Low-level *technical findings* handed directly to *less-technical* decision makers.
  2. Decision-makers lack *appropriate framework* for *understanding risk(s)* of findings.
  3. Without risk context, "*close the findings*" is the "*safest*" reaction. Decision-makers are implicitly encouraged to blindly *comply with standards* rather than make *risk-based decisions*.
  4. System complies and closes findings, then system deviates from compliance, resulting in *repeat findings*.
  5. Money and resources are wasted either through *repeat findings* or through *inappropriate compliance*.

What is Adaptive Capabilities Testing (ACT)?

- MITRE ACT is a *Capabilities-focused* assessment framework that encourages and drives *risk-based decision-making* by considering *all available Risk Information Sources*.
  - ACT improves decision-making about limited budgets and resources by identifying which threats to *mitigate* with which defenses, and which risks to *accept* because Capabilities are being satisfactorily provided (i.e, within risk tolerance)
  - ACT can provide the primary input to the Authority to Operate (ATO) process, superseding existing compliance-oriented decision-making frameworks.

ACT vs. Compliance Assessment

- *Risk-driven* rather than *compliance-driven*
  - ACT focuses on risk identification and analysis at the Capability-level and de-emphasizes findings of non-compliance with standards (such as NIST SP 800-53 Security Controls).
- *Capability-oriented* rather than *standard-oriented*
  - Capabilities state objectives, while standards (such as Security Controls) state specific implementation requirements that *might* help meet those objectives.
- Based on multiple *Risk Information Sources (RIS)*
  - ACT considers all available risk data at the time of the assessment, not just the current state of compliance with standards.
- More *understandable* and *actionable*
  - ACT adds context, brings conversation to a higher level, and focuses on helping the reader determine what should be done.



MITRE

Example of ACT's Decision-Making Role

ATT&CK:

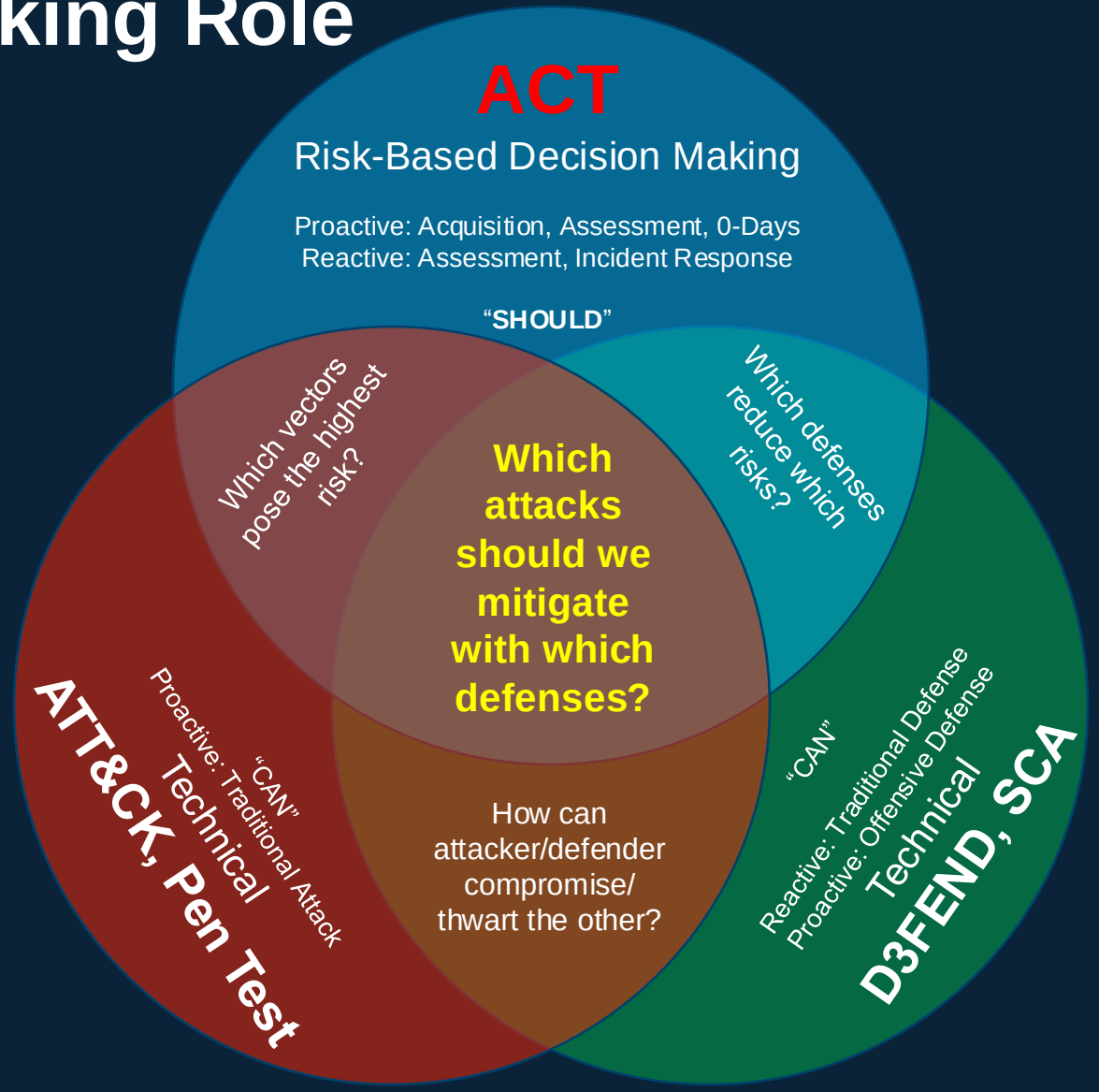
- "What *can* the attacker do to me?" or
- "What *can* I do to my target?

D3FEND:

- "How *can* I protect myself from the attacker?" or
- "How *can* my target protect themselves against me?"

ACT:

- What **should** I do?
- How **should** I spend my limited security budget?



Key Concepts in ACT

- **Security Capability**: defines mission-oriented security objectives
  - Plain-language expressions of mission objectives, which can be fulfilled through compliance (or not!) with various standards
    - All parties can understand the objectives, regardless of role or expertise
    - Provides context for determining whether or not compliance with a standard requirement is appropriate – ”Does compliance help me provide this Capability?”
    - Seldom changed – once defined, they should be applicable regardless of time, Administration, implementation standards, staff, technology, etc.
  - Approximately 18 Capabilities divided into multiple Sub-Capabilities
    - Capabilities are fully customizable by the organization
  - Sub-Capabilities are mapped to various compliance standards (including 800-53 Controls), and vice versa
    - Example: *CRED-02: “Ensure the use of strong credentials”*; maps to at least 27 different Controls from NIST 800-53, as well as various requirements from other standards

Key Concepts in ACT (cont.)

- **Finding:** A statement of non-compliance with a standard
  - Findings are not necessarily negative – they are neutral until evaluated in the Risk Assessment
  - *Example: The minimum accepted password length is 8 characters but should be 12 characters.*

Key Concepts in ACT (cont.)

- **Testing Rigor:** A specification of the required quantity and quality of testing assurance.
  - Goal of Security Assessment is to determine actual compliance with Security Controls and correctness and reliability of Control compliance assertions.
  - Complete testing is impossible. 😳
    - It would require infinite time to completely test all requirements on all system interfaces, functions, modules, *etc*.
  - AO must specify the what kind and how much assurance they require.
    - ACT specifies four Levels of Testing Rigor that provide increasing levels of assurance
  - Assessment Team tailors assessment methods to meet the verification objectives of the chosen Level of Testing.

Testing Rigor Example

Level 1: Assertion Appropriateness

Level 2: Passive Compliance Verification

Level 3: Basic Compliance Verification

Level 4: Advanced Compliance Verification

Category		Description	Note	Level 1	Level 2	Level 3	Level 4	NIST SP 800-53 Assessment Methods		
Type of Testing		This is level of testing Technical or Non-Technical?		*Non-Technical*	*Technical*					
Title		Short description of this level of testing rigor.		Assertion Appropriateness	Passive Compliance Verification	Basic Compliance Verification	Advanced Compliance Verification	Examine	Interview	Test
Typical Use		This level of testing rigor will usually be used for...		*Status Check of Trusted System*	*Initial Form of Ongoing Authorization*	*Tailored-Scope ACT*	*Comprehensive ACT*			
Questions Answered		Does the documentation and configuration indicate a system that ***is likely*** to be acceptably compliant with security requirements? (Examine)		✓	✓	✓	✓	✓		
		Do **pre-existing** testing results and personnel interviews indicate a system that ***is likely*** to be acceptably compliant with security requirements? (Examine, Interview)			✓	✓	✓	✓	✓	
		Does **new** testing confirm the system ***is*** acceptably compliant with a ***sample*** of security requirements? (Test)				✓	✓			✓
		Does **new** testing confirm the system ***is*** acceptably compliant with ***all*** security requirements? (Test)					✓			✓
Goals Achieved		Determine if **assertions** made in documentation and passive data collection are compliant and appropriate. (Examine)		✓	✓	✓	✓	✓		
		Determine if **pre-existing** test results demonstrate that the system adequately complies with security requirements. (Examine)			✓	✓	✓	✓		
		Determine if **personnel** adequately understand the system, the security requirements, and their duties. (Interview)			✓	✓	✓		✓	
		Determine if **assertions** in documentation, **interviews**, and available **pre-existing** system test results are consistent with each other. (Examine, Interview)			✓	✓	✓	✓	✓	
		Determine if **known exploits** (CVEs, 0-days, etc.) are adequately addressed by the system documentation, personnel, and implementation. (Test)				✓	✓			✓
		Determine if the **Core** Controls are adequately implemented by the system. (Test)				✓	✓			✓
		Determine if a **random sample** of the **non-Core** Controls are adequately implemented by the system. (Test)				✓				✓
		Determine if **all non-Core** Controls are adequately implemented by the system. (Test)					✓			✓
Assertions Verified		*Assertion verification summary:*		*Assertions Not Verified*	*Assertions Verified Against **Existing** Test Results*	*Assertions Verified Against **New** Test of **Sample** of Controls*	*Assertions Verified Against New Test of **All** Controls*			
		Interviews			✓	✓	✓		✓	
		Existing Test Results	*NetSparker, Penetration Test, and Previous ACT Security Assessment (see "Tools Used" below).*		✓	✓	✓	✓		
		Known Exploits	*CVEs, 0-days, etc. for components and technologies known to compose the system.*			✓	✓			✓
		Core Controls				✓	✓			✓
		Non-Core Controls				sample	all			✓
Tools Used	Documentation	System Security Plan (SSP), Contingency Plan (CP), Information System Risk Assessment (ISRA), *etc.*		✓	✓	✓	✓	✓		
	Configuration Data	<Tool, *e.g.* InSpec>	*Not considered to be "tests" since they simply collect configuration and status data from the system, which is effectively a collection of assertions that must be verified through testing.*	✓	✓	✓	✓	✓		
		<Tool, *e.g.* DbProtect>		✓	✓	✓	✓	✓		
		<Tool, *e.g.* Nessus>		✓	✓	✓	✓	✓		
		Running Configurations (System)		✓	✓	✓	✓	✓		
	Interviews	Interviews of ISSM, ISSO, App Developers, DB Admins, Network Admins, OS Admins, Mainframe Admin, *etc.*			✓	✓	✓		✓	
	Implementation Data	<Tool, *e.g.* NetSparker>	*Considered to be "tests" since they report actual testing that was performedwithin a reasonable timeframe from this asssessment.*		✓	✓	✓			✓
		Penetration Test			✓	✓	✓			✓
		Previous ACT Security Assessment (Existing Data)			✓	✓	✓	✓		✓
		Vulnerability Assessment Tools (**This Assessment**)	*Vulnerability Assessment performed by the Assessment Team on this assessment.*			✓	✓			✓
System Access Needed		Type of access to the system required to complete testing.		none	none	full	full			

Key Concepts in ACT (cont.)

- **Risk**: A potential failure to adequately meet Security Capability objective(s)
  - Explains what the Findings *mean in context* with other Risk Information Sources (RIS).
    - Findings = "**WHAT?**" Risk = "**SO WHAT?**"
  - 3 types: *Inherent* (direct), *Residual* (indirect), and *Inherited* (from other system(s))
  - Mapped to *Capabilities* instead of implementation standards (*e.g.*, Controls)

Risk Example

This is an example of a **Risk** taken from a real ACT Risk Assessment Report during the recent ACT **Pilot** conducted by MITRE

It shows a risk to the **system** *and* **organization** that arises from ***organizational*** **failures** (in the assessment program)

The Narrative documents the Risk "**story**" – the other cells are supporting metadata.

Risk ID	TST-20210625-R04	**Impact**	High	**Likelihood**	Moderate	**Risk Level**	Moderate
Risk Title	Incorrect information reported in assessment program findings						
Capability	Manage Credentials and Authentication (CRED)	**Sub-Capability ID**	CRED-01	**Sub-Capability Name**	Prevent users from unauthorized access		
Capability	Manage Credentials and Authentication (CRED)	**Sub-Capability ID**	CRED-07	**Sub-Capability Name**	Ensure the reporting of expired, modified, lost, stolen, or revoked credentials		
Capability	Manage and Assess Risk / Operate, Monitor, Asses (RISKOMI)	**Sub-Capability ID**	RISKOMI-06	**Sub-Capability Name**	Implement risk assessment methods and processes		
Capability	Manage Trust for Persons Granted Access (TRUST)	**Sub-Capability ID**	TRUST-09	**Sub-Capability Name**	Unmet TRUST Level		
Potential Event	Incorrect statement(s) or assertion(s) documented in assessment team findings						
Potential Cause ("...caused by...")	Lack of quality control in contract deliverables, lack of sufficient organizational audit of contract deliverables						
Potential Consequence ("...resulting in...")	System stakeholders incorrectly configuring/implementing system components to organizationally defined policies or instructions; repeat findings						
RIS	POA&M - System	**RIS Artifact**	TST POA&Ms Report-5-23-2021	**RIS Artifact Element(s)**	POA&M-3263165, POA&M-3263532, POA&M-3263135		
RIS	ACT Security Assessment Report	**RIS Artifact**	TST_SCA_Report_FINAL_20200813	**RIS Artifact Element(s)**	TST-20200813-F01, TST-20200813-F04, TST-20200813-F05		
Narrative	The 2020 ACT Security Assessment team provided findings that were mapped to incorrect controls and/or contained incorrect requirements. As a result, there may have been incorrect changes to the system, POA&Ms incorrectly documented and closed, and the system is possibly still non-compliant. The documentation and the state of the system were confusing to the current risk assessors. Examples of these problems include: • TST-20200813-F01 incorrectly states an "annual" account review is required, however, 800-53 control states: "Reviews accounts for compliance with account management requirements at least every 90 days for High and Moderate systems or 365 days for Low systems". POA&M-3263165 was created with the wrong corrective action. • TST-20200813-F04 specified an incorrect timeframe (90 days) and should have stated that accounts are required to be disabled after 60 days of inactivity. The finding is also mapped to the wrong 800-53 control which caused POA&M-3263532 to contain incorrection information. • TST-20200813-F05 specified an incorrect password expiration period (90 days) and should have stated that passwords must expire after 90 days per 800-53 requirement which caused POA&M-3263135 to contain incorrect information.						

Risk Example (Narrative)

“The 2020 [SCA] team provided findings that were mapped to incorrect controls and/or contained incorrect requirements. As a result, there may have been incorrect changes to the system, POA&Ms incorrectly documented and closed, and the system is possibly still non-compliant. The documentation and the state of the system were confusing to the current risk assessors. Examples of these problems include: …”

Summary: The SCA team issued findings with incorrect analysis and recommended corrective actions and every party producing and receiving the Finding failed to catch the mistakes. Incorrect POA&Ms were opened, incorrect corrective actions were taken, non-compliant system configurations were pushed to Production, and POA&Ms were closed incorrectly.

This type of systemic organizational failure would not have been caught by the organization’s existing compliance assessments.

Key Concepts in ACT (cont.)

- **Risk Information Source:** An independent source of information about compliance-oriented deficiencies
  - Related *directly or indirectly* to the assessed system
  - Generated by the *system* or the *organization* at-large
  - Generated through *automation* or *manual* processes

  - Examples: [see next slide]

Risk Information Source Examples

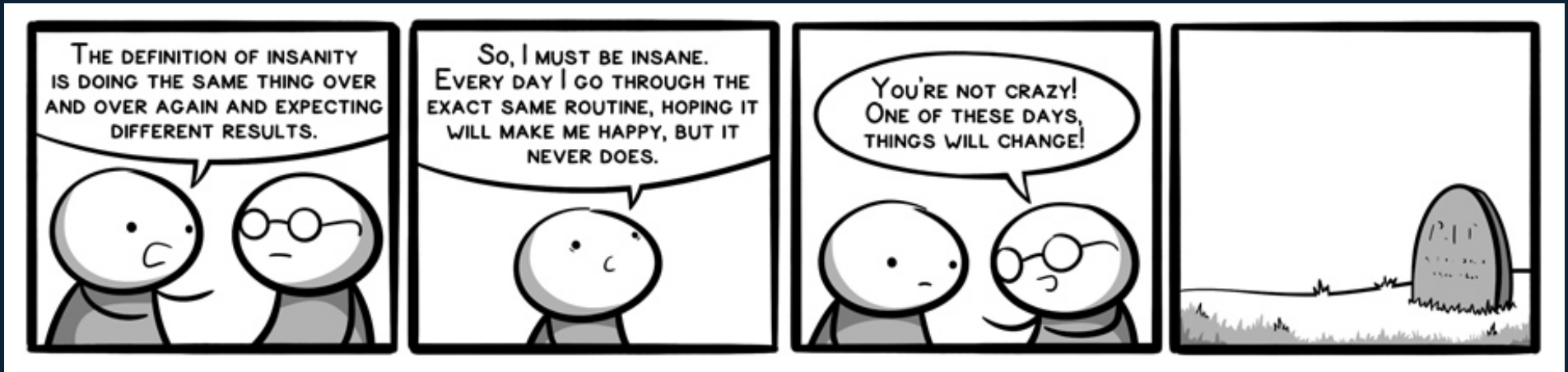
Category	Assessment Type/Standard
Cybersecurity	• Live output from sensors, scans, IDS/IPS, etc. • Security Control Assessment (SCA) (NIST SP 800-53) • High Value Asset Assessment (Pen Test/SAR/Incident Response Evaluation) • Risk and Vulnerability Assessment (RVA) • Cyber Hygiene (CH) • Cyber Resilience Review (CRR) • Information Security Continuous Monitoring Assessment (ISCM)
Physical Security	• DoD 5200.08-R
Financial	• Sarbanes-Oxley Act
Health	• HIPAA
Privacy	• Privacy Act of 1974
Management	• OMB Circular A-123 • Self-Assessment

ACT combines and analyzes *all available RIS's* to inform risk-based decisions.

MITRE

MITRE

“*Insanity* is doing the same thing over and over again expecting different results.”



https://www.buttersafe.com/2015/07/09/definition-of-insanity-comics/

Risk-Based Decision-Making: Context is Key

- Risk-based decision-making is an inherently contextual and qualitative process that uses quantitative data as inputs.
  - A *finding* (of non-compliance) is a neutral state – the *context* of that finding helps to define the risk that it poses (to the system or the organization).
  - Context includes things like:
    - organizational Capabilities
    - organizational directives, business needs, mission objectives
    - findings from other assessment types, risk posture of related or interconnected systems
    - real-world events (0-days, politics, etc.)
  - ACT collects and analyzes disparate-yet-related quantitative data, then guides the decision-maker through a repeatable and well-defined process that uses quantitative metrics and qualitative judgments to make informed and defensible risk-based decisions.

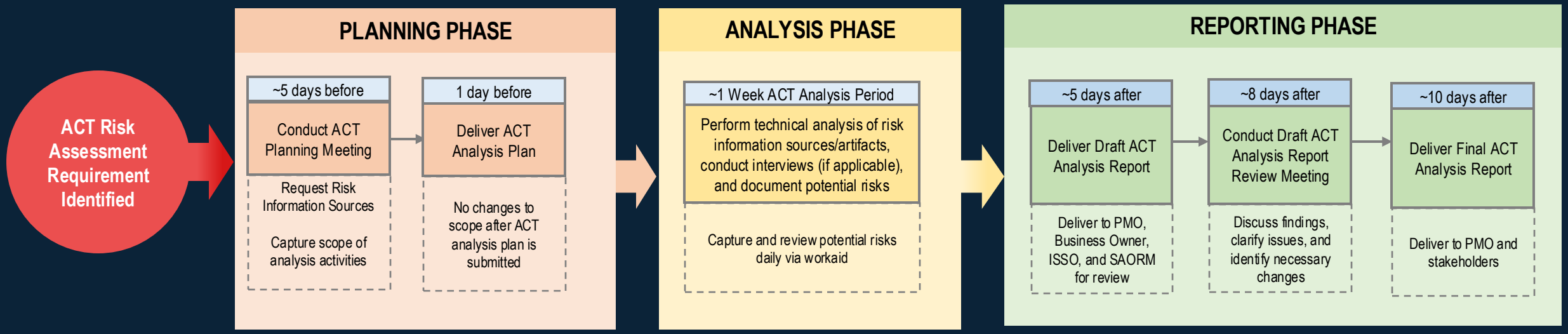
Context Comes from Multiple Parties

- **ACT Risk Assessment Team:**
  - Assesses all systems in your organization, giving them broad knowledge of compliance and risk trends across the organization without having deep knowledge of individual systems
  - Identifies potential risks that consider not only the target system but also other related systems and the organization's Capabilities and mission objectives
- **System Team:**
  - Has deep knowledge of the target system, enabling detailed understanding of pros and cons of implementing risk mitigation at the system level
- **Decision Maker (*e.g.*, Authorizing Official):**
  - Has ultimate responsibility for successful execution of mission objectives and organizational Capabilities, and determines organization's risk tolerance
  - Considers inputs from System Team and Risk Assessment Team to determine disposition of each risk (accept or mitigate) based on organizational risk tolerance and objectives

How Else Can ACT Help Federal Agencies?

- **Identify the next SolarWinds**: ACT enables and encourages “outside of the box” risk-based assessment that looks beyond the target system to its environment, interconnections, providers, etc. ACT is designed to identify non-obvious but important risks, such as the situation (homogenization of Federal networks) that contributed to the SolarWinds breach.
- **Information Sharing**: By encouraging and enabling systems to share risk data within their organization, and organizations to share with other organizations within Departments and across the Federal Government, better decisions can be made faster and more intelligently.
- **Cost Savings**:
  - Making intelligent risk-based decisions about compliance reduces the cost (in dollars and resources) of “configuration jitter” between assessments with conflicting requirements.
  - Information Sharing brings the collective wisdom of all Federal security programs to each participating system and organization, greatly increasing reuse.

ACT *Manual* Risk Assessment Workflow Overview



- ACT provides fast, efficient, flexible, ongoing Risk Assessment and facilitates risk-based decision-making.
- *Manual* ACT Risk Assessment can be fully executed in about 20 business days. *Automated* ACT Risk Assessment should eventually be executable in minutes.
- ACT supports Ongoing Authorization, ATO, CDM, and other risk based decision-making processes.

Risk Scoring

Risk Scoring: Example

1. Qualitative Risk **Levels** are defined with Score ranges:

Risk Level Ranges		
Weighted Risk Level	Range	Spread
Low	1 to 19	20
Moderate	20 to 49	30
High	50 to 89	40
Critical	90+	∞

2. Risk Score **Modifiers** are determined:

Score Modifiers: Misc.		
Category	Type	Value
Information Type	PII	5
	PHI	5
	LES	10
	Financial	5
Missing RIS	MOUs	2
	CP	3
	SSP	10
System Criticality	NatSec	50
	NEF	50
	PMEF	10
	MEF	5
...		

Score Modifiers: Impact / Likelihood Matrix				
Likelihood of Occurrence	Impact Severity			
	Low	Moderate	High	Critical
Low	1	5	10	20
Moderate	5	30	40	50
High	10	40	70	90
Critical	20	50	90	120

3. Risk **Score** is Calculated:

Risk Score Calculations						
Risk ID	Likelihood/Severity	Sys Info Types	System Criticality	Missing RIS Types	Total Risk Score	Risk Level
Risk 01	High/Mod = 40	PHI=0, PII=5, LES=10, $=5	PMEF=10	MOUs=2, CP=3	75	High
Risk 02	Low/Low = 1	PHI=0, PII=5, LES=10, $=5	PMEF=10	MOUs=2, CP=3	36	Moderate
Risk 03	Crit/Low = 20	PHI=0, PII=5, LES=10, $=5	PMEF=10	MOUs=2, CP=3	55	High
Risk 04	High/High = 70	PHI=0, PII=5, LES=10, $=5	PMEF=10	MOUs=2, CP=3	105	Critical
				HVA System Risk Score:	271	

The sum of the Risk Scores is the System's overall Risk Score.

The Modifier values can be changed at any time, resulting immediately in new Scores across all Risks and all Systems with no re-analysis required.

Risk Scoring: Uses

- **Rank-order Systems**
- **Rank-order Risks within a system**
- **Immediately identify and prioritize important systems when “hot topics” arise**
- **Compare similar Risks across systems to understand causes and impacts**
- **Understand how Risks are affecting Security Capabilities, Compliance Requirements, other systems, etc.**

Person Name

email@address

(###) ###-####

Nate Lee

nlee@mitre.org

(530) 628-3533

Person Name

email@address

(###) ###-####

Backup Slides

MITRE

ACT Development Roadmap

Goal: Mature organization's ability to make risk-based decisions about compliance-oriented issues by building an organizational security culture that encourages and rewards decisions to comply (or not) with standards based on holistic understanding of organization's risk posture, mission, and objectives.

Near-Term Improvements (Date TBD)

Objective: Lay technical groundwork and initiate preliminary culture change.

- **Culture Change:**
  - Define and validate initial set of Capabilities for organization (building on existing CDM Capabilities).
  - Begin socializing and considering Capabilities and Risks-vs-Compliance in various decision and assessment flows.
  - Understand current ATO decision-making process as it will relate to ACT.
- **Risk Information Sources (RIS):**
  - Identify currently available RISs and their formats.
  - Identify gaps in current RIS coverage - what other RISs are needed?
  - Prototype workaid that automates RIS ingestion and rough risk identification (reduces manual work by human SME).
- **Risk Identification & Scoring:**
  - Define/update Risk Scoring Methodology and scale for organization based on historical data and mission objectives.
  - Perform mock Risk Assessments of several systems based on currently-available RIS data.

Mid-Term Improvements (Date TBD)

Objective: Obtain buy-in from organization leadership, begin rollout of ACT culture and processes

- **Culture Change:**
  - Develop and provide ACT education to all relevant organization personnel.
  - Issue appropriate policy/directives and execute changes to various dashboards, reports, decision-making processes, etc. to formally shift organization to an “ACT culture” of risk-based decision making.
- **Risk Information Sources (RIS):**
  - Define standards for RIS data to ensure that it is machine-parsable (acceptable formats) and mappable (tagged, grouped, harmonized, *etc*.).
  - Begin development of secure and centralized RIS data repository.
  - Deploy tools/processes that implement new RISs to fill gaps in required RIS data coverage.
  - Develop and deploy v1.0 workaid that automates RIS ingestion and generates mostly-reliable preliminary risks (reduces manual work by human SME).
- **Risk Identification & Scoring:**
  - Execute Pilot Program of Risk Assessments of several organization systems based on available RIS data.
  - Validate and test ACT value by making ATO decisions for Pilot systems using ACT Risk Assessment data as primary input.

Long-Term Improvements (Date TBD – "Utopia")

Objective: Fully support and execute automated Ongoing Authorization.

- **Culture Change:**
  - Group, Organization, and Federal cultures are fully mature: Capabilities-oriented Risk-based decision-making is the norm.
  - ATO decisions are made based on ACT Risk Assessments, which are automated and performed frequently based on whatever RIS data is available at that time.
- **Risk Information Sources (RIS):**
  - All RIS data is machine-parsable and fully standardized (tagged, harmonized, homogenized, mapped, *etc*.).
  - All RIS data is securely stored in centralized and connected repositories.
  - All RIS data is accurately parsed and mapped by automated tool.
- **Risk Identification & Scoring:**
  - Automated tools perform "good enough" risk identification and analysis requiring acceptably low human SME intervention (metrics TBD).

ACT Automation Roadmap

Goal: Reduce cost of assessments and multiply effectiveness of every security dollar by supporting automated risk-based Ongoing Authorization.

Near-Term Automation Improvements (Date TBD)

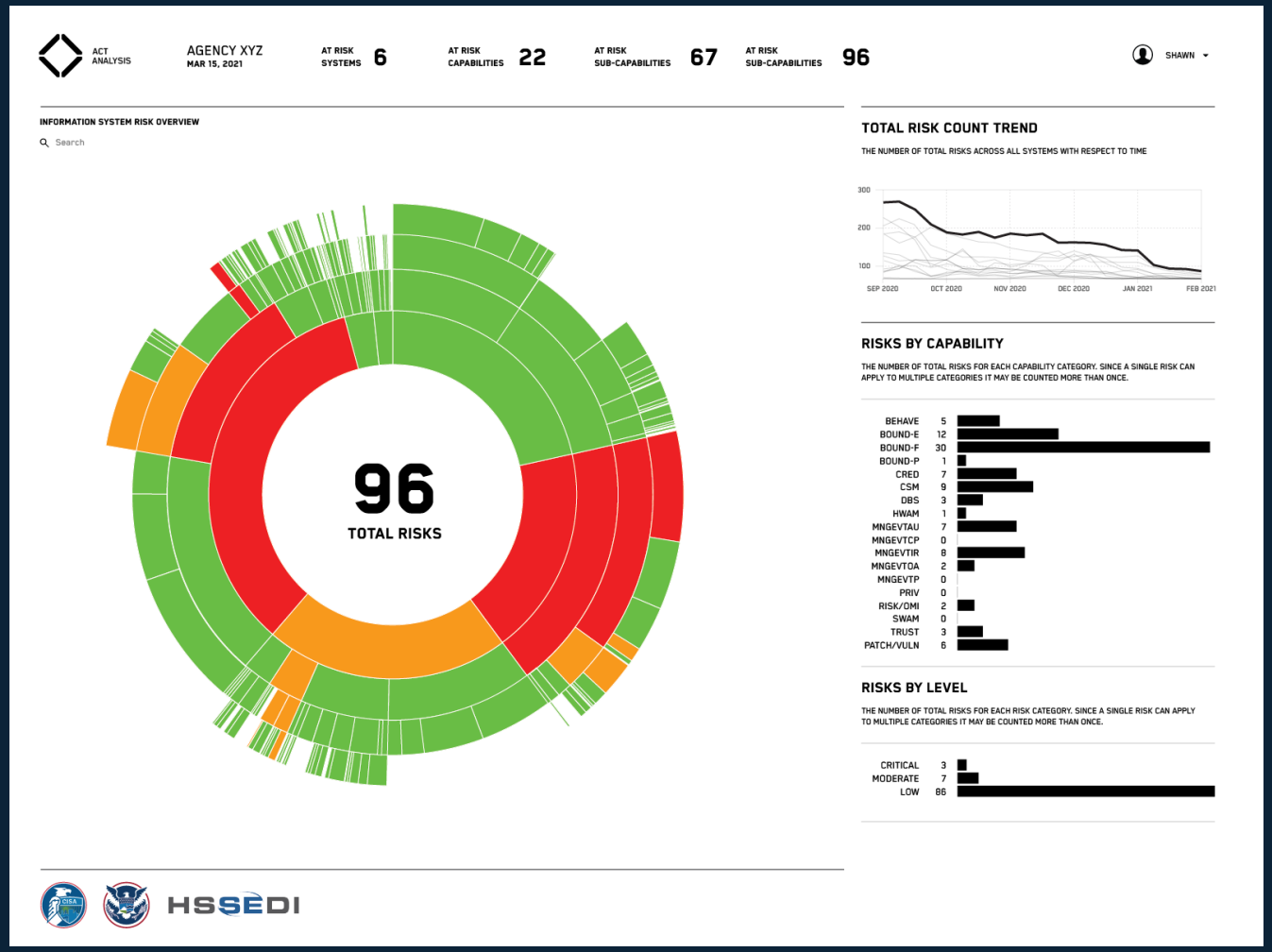
Risk Assessment Work Aid - Rudimentary (requires human processing)

- RIS Mapping: Rudimentary mapping of RIS data to each other: sort, group, correlate
  - Automatically analyze and group potentially related RIS Artifact Elements (e.g. Findings) to reveal potential Risks.
    - Human can add/edit/delete as appropriate.
- Risks: Rudimentary potential risk identification
  - Aid the human in identifying which potential Risks are pertinent.
- Risk Assessment Report (RAR): Outputs rough risk data to be used by human SME to create RAR.
- Dashboard: outputs data to be manually input to Dashboard.

Near-Term Automation Improvements (Date TBD)

System-Level Dashboard - Rudimentary

- Shows risk data broken down by risk categories
  - Inherent/Inherited/Residual
  - Capabilities/Sub-Capabilities
  - Cause/Effect/Consequences
- Shows risk data by risk status
  - Open / Accepted / Transferred / Mitigated



Mid-Term Automation Improvements (Date TBD)

- **Risk Assessment Work Aid - Improved** (requires human verification and edit)
  - RIS Mapping: Improved RIS data mapping.
  - Risks: Improved potential risk identification.
  - Outputs Dashboard-ready and RAR-ready risks and related data.
  - Dashboard: automatically updates Dashboards.
- Dashboards:
  - **System Level Dashboard – Improved**
    - Adds risk status over time, other metrics as requested
  - **Organization-Level Dashboard – Rudimentary**

Long-Term Automation Improvements (Date TBD - “Utopia”)

- **Risk Assessment Work Aid - Mature** (requires human sanity-checking)
  - RIS Mapping: Trustworthy and comprehensive RIS data mapping
  - Risks: Trustworthy and mostly-pertinent risk identification
  - RAR: Outputs near-complete RAR - needs human polish
  - Dashboard: automatically updates Dashboards.
- Dashboards:
  - **System Level Dashboard – Mature**
  - **Organization-Level Dashboard – Improved-to-Mature**
  - **Federal Government Dashboard – Rudimentary-to-Mature**