The Art of the Exception

Presentation Objective: Discuss the often unappreciated duty of ISOs to negotiate information security exceptions. Understand that organization culture drives maturity……

Barry Davis, CISSP
DSS Chief Information Security Officer

COV Information Security Conference 4/11/2019

Presenter

Barry Davis
CISSO
Virginia Dept. of Social Services
(804) 726-7153

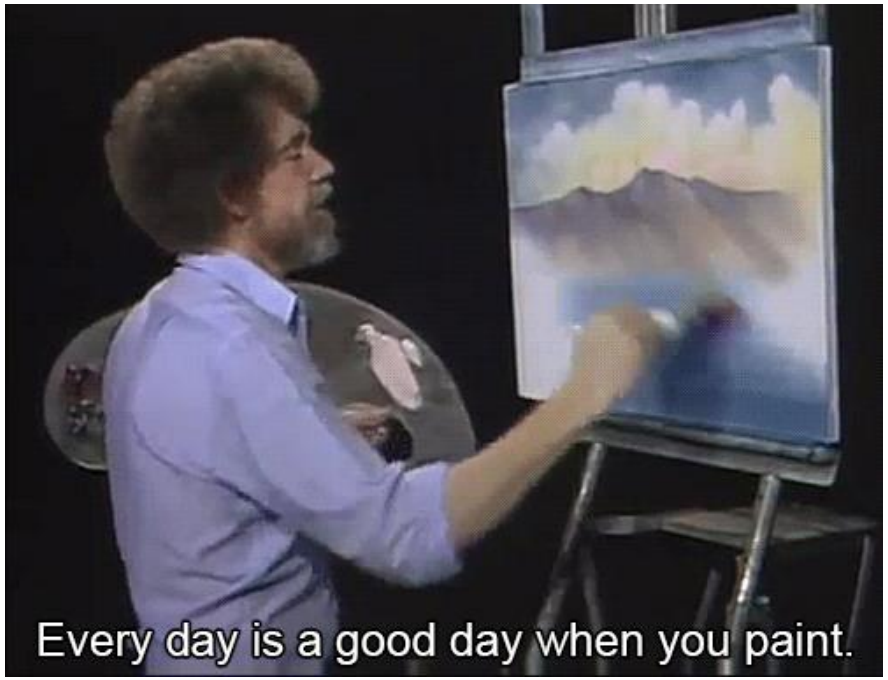
Email: barry.davis@dss.virginia.gov

Agenda

- Introduction
- Lessons from Bob Ross
- The Case for Exception
- The Art of Negotiation (aka Step 1)
- Process pathways (more negotiation)
- A GRC tool
- Next Steps for DSS

Lessons from Bob Ross…

- Made art less intimidating
- Pared painting down to simple steps
- He inspired confidence
- Reminded us that art should be available to everyone



The Case for Exception

- Legacy Applications
- End-of-Life software
- Vendor dependencies
- Password strength
- Baseline deviation
- Discovery…..

"Look around..."

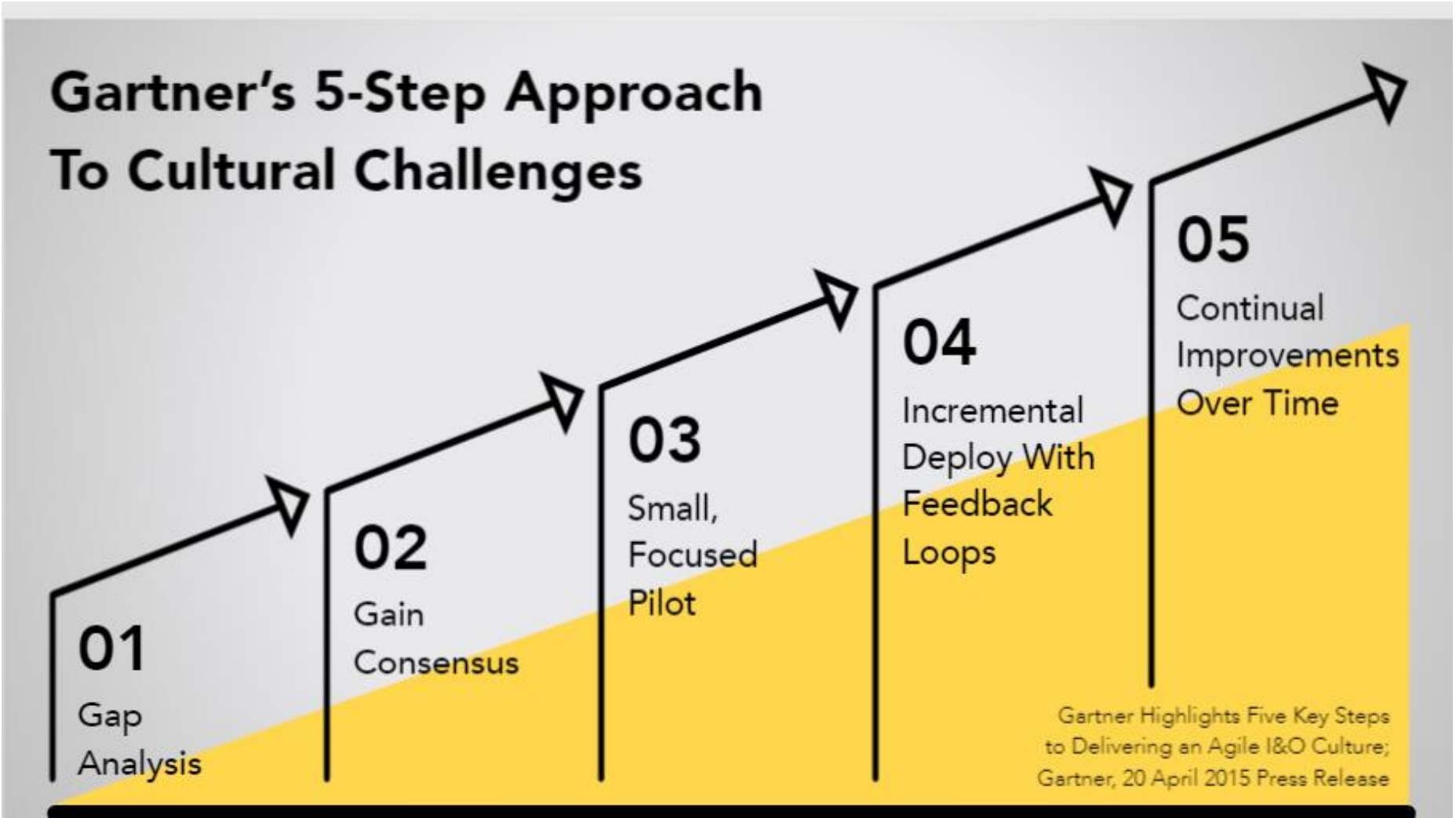
"We don't make mistakes,
just happy little accidents."

Managing Exception Risk (art vs science)

"Let's get crazy"

Exception Management –Culture Change

"I believe talent is just a pursued interest."



Exception Management –Culture Change

"You need the dark in order to show the light."

- Processes confined to ISO organization
- Risks measurement is subjective, not to standards/policies
- Risk capture process not well defined

- Exception process known outside of ISO organization
- Risks measurement is based on organization policy and standards
- Formal process for risk ownership
- Risk is not aggregated or discussed in a risk management forum
- Formal remediation steps or time lines required as part of the process

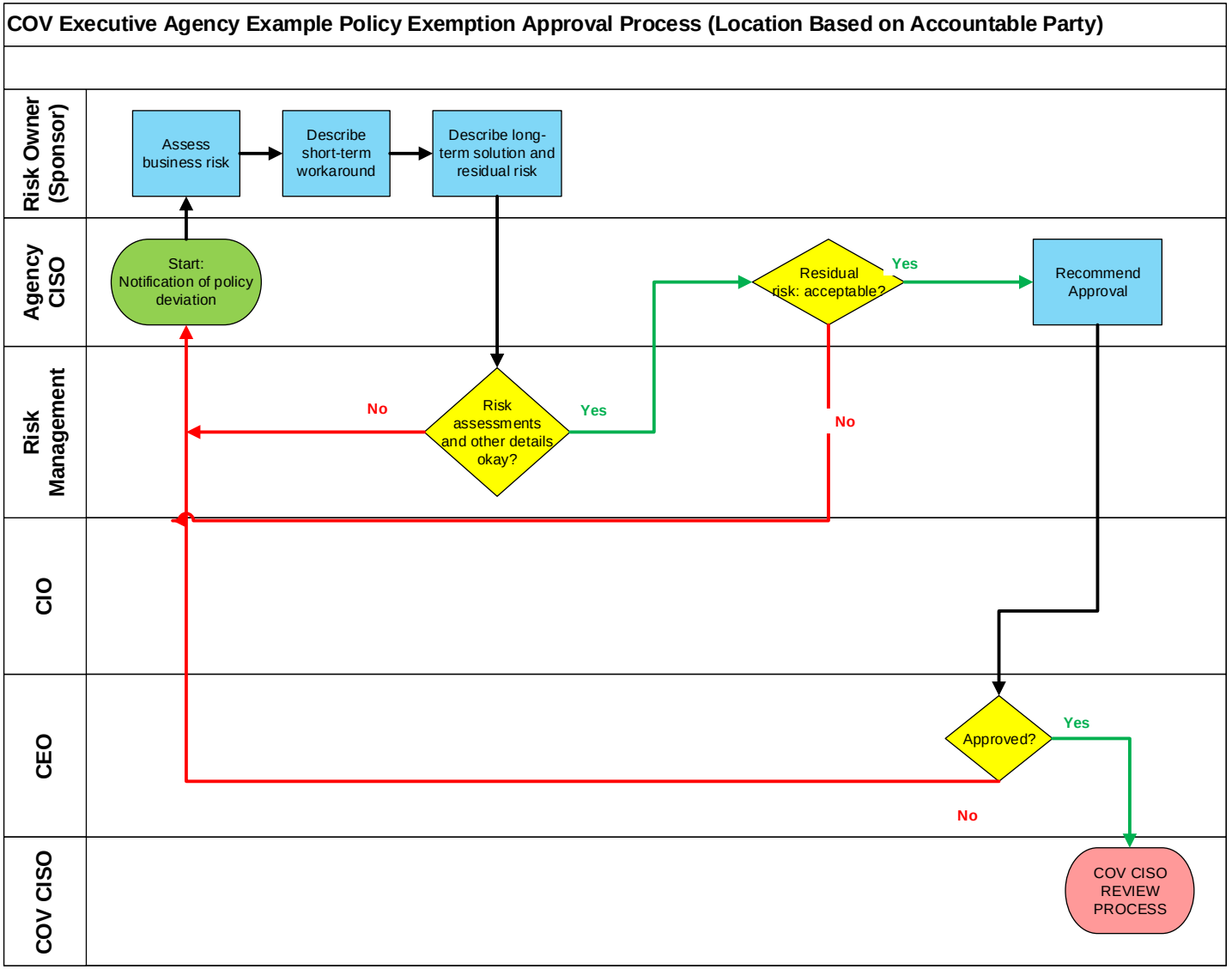
- Exception process is published and followed by peer groups
- Peer organizations have security/risk champions that work with ISO organization to provide required info
- Automated exception review or tracking mechanisms are in place
- Exceptions are discussed in enterprise risk management forums and scored to the organization risk profile, with C-level visibility
- Accounts for combined risk

Compounded Risk

- Multiple exceptions across multiple applications could lead to unacceptable consequences….
  - Exception 1, exception from IDS/IPS that is negatively impacting the application
  - Exception 2, Next week, Firewall exception to allow well-known port traffic from untrusted networks
- A fully mature exception process should account for this combined risk. Each exception should not represent a disconnected IT event.

> “Water's like me. It's laaazy ... Boy, it always looks for the easiest way to do things”

Example Agency Policy Exemption Flow



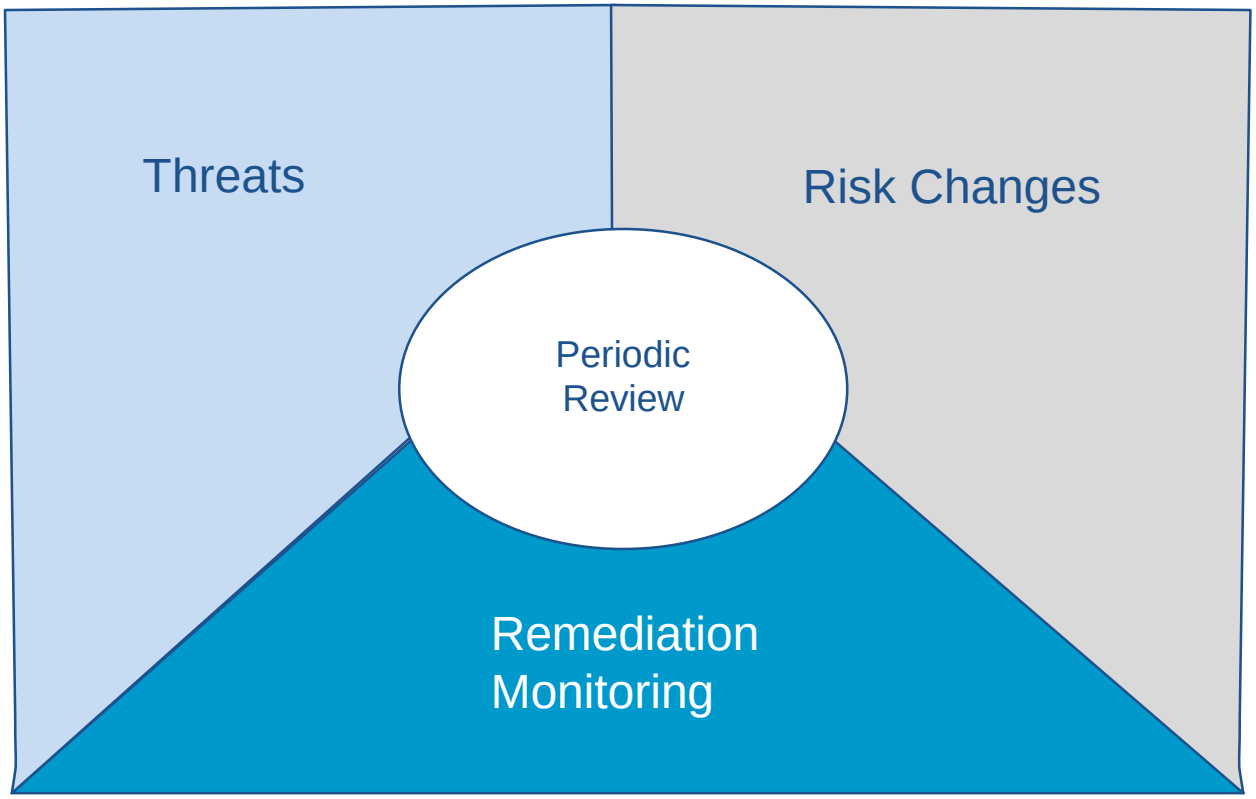
Example Agency Policy Exemption Process

	Detect Policy Deviation	Assess Risk	Agree Short-Term Workaround	Agree Long-Term Solution	Assess Residual Risk	Approve Plan	Approve Residual Risk	Implement Plan
Risk Owner	C	AR	AR	AR	AR	I	R	AR
CISO	AR	C	R	R	C	I	A*R*	R
CRO or Delegate	I	R	C	C	R	AR	R	I
CIO	I	I			I	I	A*R*	I
CEO							A*R*	
Others as Required	C	C	C	C	C			R

Responsible: Person or Function That Is Responsible for Executing the Activity
Accountable: Person or Function That Owns the Activity, Approves Work and Is Held Accountable for It
Consulted: Person or Function That Has Information Relevant to the Activity
Informed: Person or Function to Be Informed of Progress and Results

Note: Only one party can be held accountable for any individual execution step. In the “Approve Residual Risk” column, the party with accountability for approval is linked to the level of the risk.

The R-word



“Look around. Look at what we have……”

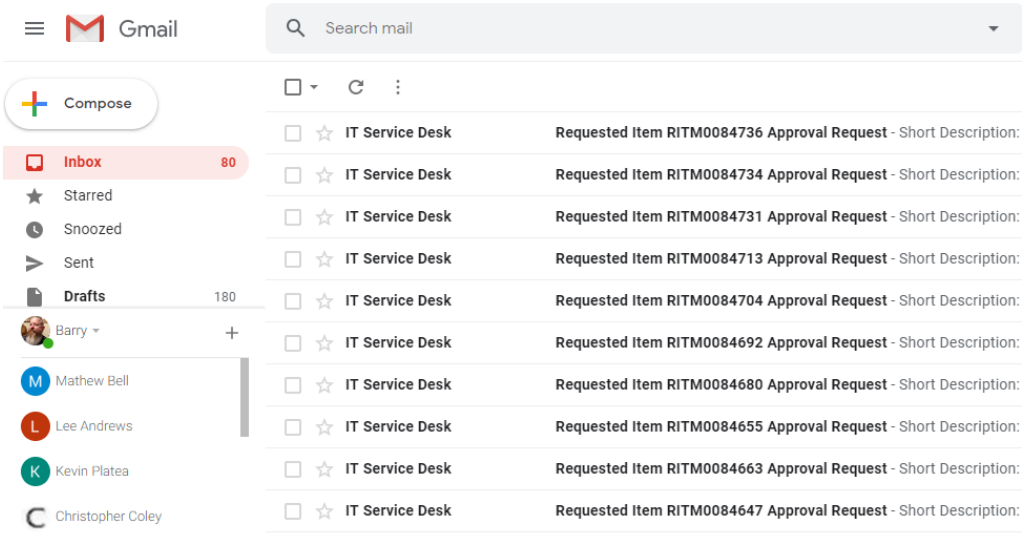
The Other R-Word

- Two main types of Remediation
  - Low Complexity
  - All Others
    - Medium to High complexity
    - Negotiation between Business, IT, Security
    - Unintended Consequences
    - Longer deployment times
    - Security Professionals challenged to provide evidence….
  - Compensating Controls as a stalemate breaker…..

Conclusions

- Keep the process open and transparent
- Establish Policy and Standards
- Establish Procedures & Process Diagrams
- Formalize and recognize the exception process
- Uniformly apply security principles
- Strive for a Risk Aware Culture

Questions & Answers



Thank You!

Artifact Slide

- Sample documents that can be used from this discussion.
- DSS Process Map

Microsoft Word Document

- Sample Swim Lanes

Visio Sample
xception Swim Lan