RSAConference2019
Asia Pacific & Japan
Singapore | 16–18 July | Marina Bay Sands

SESSION ID: SDS-W02

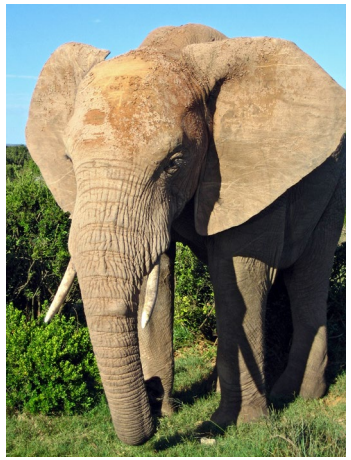
An Object-Oriented Approach to Information Security Policy Management

Cuneyt Karul, Ph.D., CISSP, CISM, RESILIA

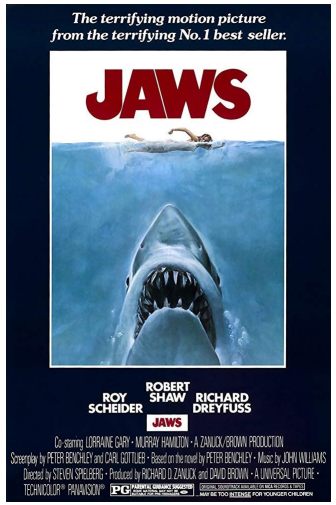
Director, Information Security & Compliance
BlueCat Networks

What is the most dangerous animal in the world?

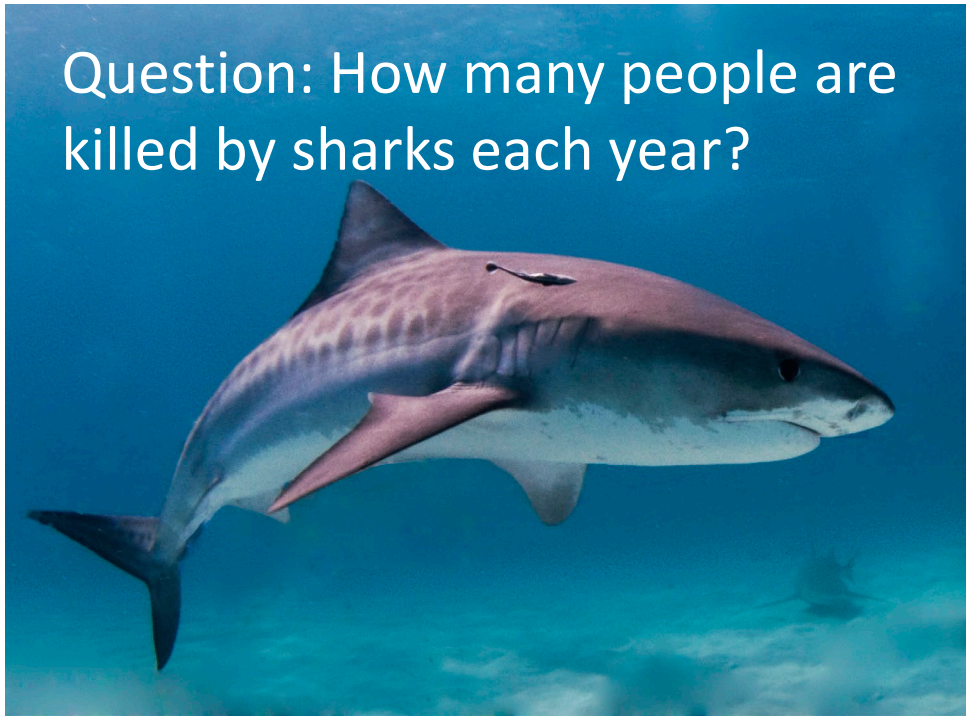
- Lion
- Elephant
- Bear
- Snake
- Shark



Shark?



Jaws (1975)
Jaws 2 (1978)
Jaws 3D (1983)
Jaws: The Revenge (1987)



SHARK WEEK

Discovery (1988 -)

SHARKFEST

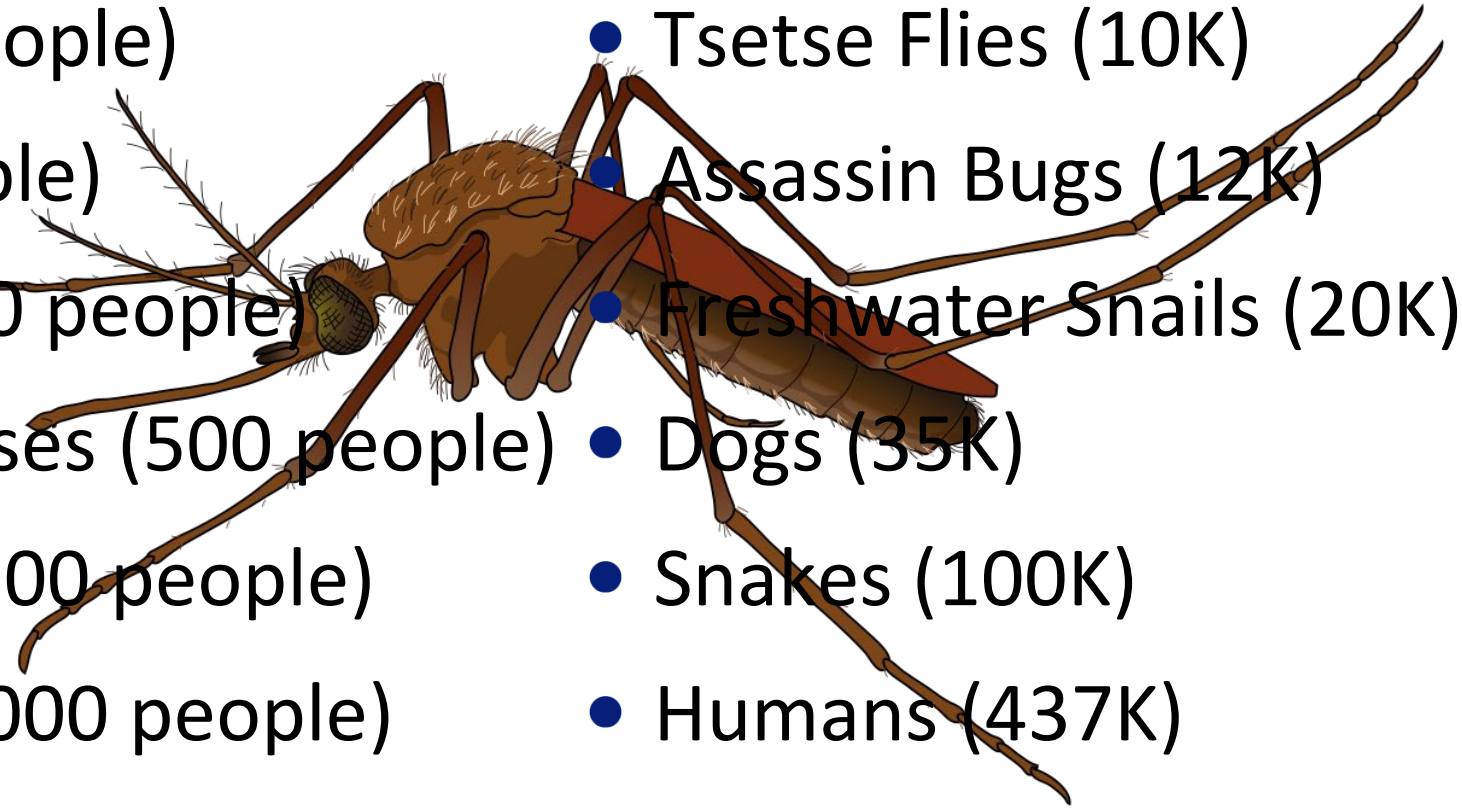
NatGeo (2013 -)

Sharknado (2013) + 7 more

BLUECAT

How many people are killed by animals annually?

- Sharks (6 people)
- Wolves (10 people)
- Lions (22 people)
- Elephants (500 people)
- Hippopotamuses (500 people)
- Tapeworms (700 people)
- Crocodiles (1,000 people)
- Ascaris Roundworms (4.5K)
- Tsetse Flies (10K)
- Assassin Bugs (12K)
- Freshwater Snails (20K)
- Dogs (35K)
- Snakes (100K)
- Humans (437K)



Mosquitoes (750K)

Are we focusing on the real Threats?

What makes the news?

- Quantum computers will break encryption. Civilization will collapse!
- Heartbleed, ShellShock, Meltdown, Spectre, Zombieload, LogJam, Freak, and many other named CVEs
- Facebook vulnerability, WhatsApp spyware, Huawei backdoors, etc.
- State-sponsored cyber attacks

What is the real threat?

- We keep falling for phishing and social engineering
- Human error
- Weak authentication
- Organizations don't have a strategy
- **We don't always create and enforce the right policies**

Are we focusing on the real Solutions?

What is hot?

- Artificial Intelligence
- Homomorphic encryption
- Quantum encryption
- Blockchain
- Zero Trust Network
- Cloud Security
- Bug Bounty Programs

What actually works?

- Awareness Training
- Multifactor Authentication
- Defense in Depth
- Email Hygiene
- Change Management
- Encryption
- **Policies, Standards, Procedures**

RSAConference2019
Asia Pacific & Japan

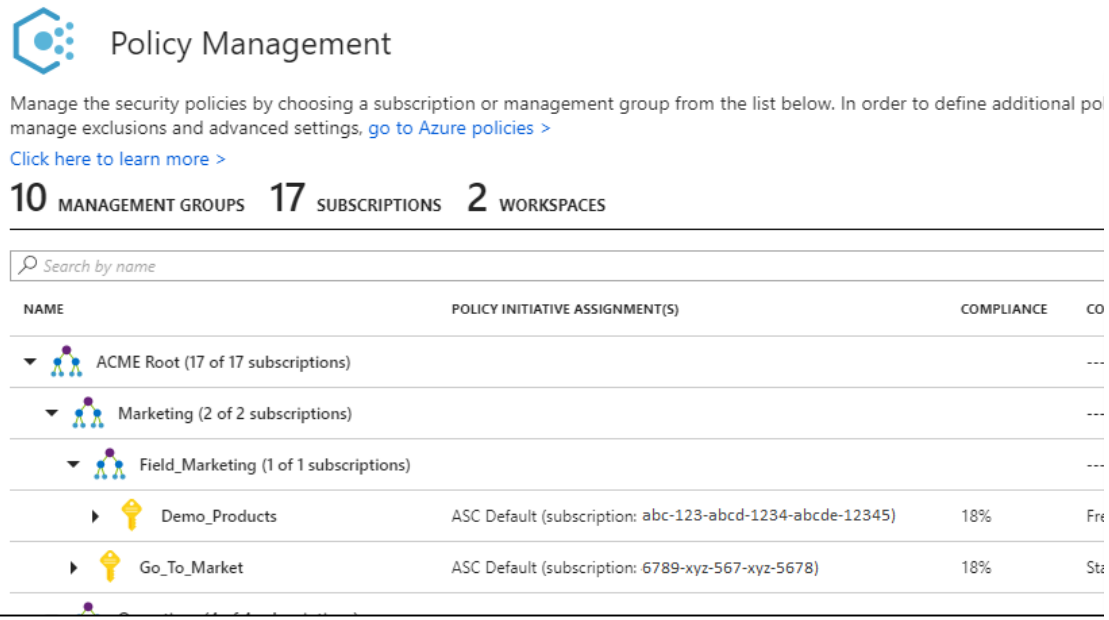
Information Security Policy Management

A Brief Overview

What is an Information Security Policy?

- Overall intention and direction as formally expressed by management (*ISACA*)
- Strategic tool used to dictate how sensitive information and resources are to be managed and protected (*ISC2*)
- A set of criteria for the provisioning of security services (*NIST*)
- A document that outlines specific requirements or rules that must be met (*SANS*)
- A definition of what it means to be secure for a system, organization, or other entity (*Wikipedia*)

Security Policy may mean different things

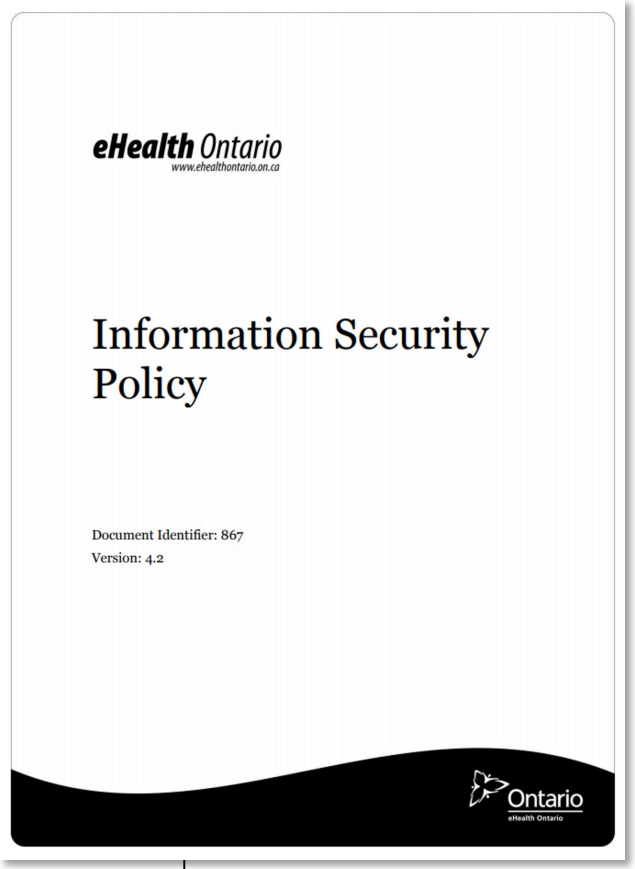


A Java Security Policy:

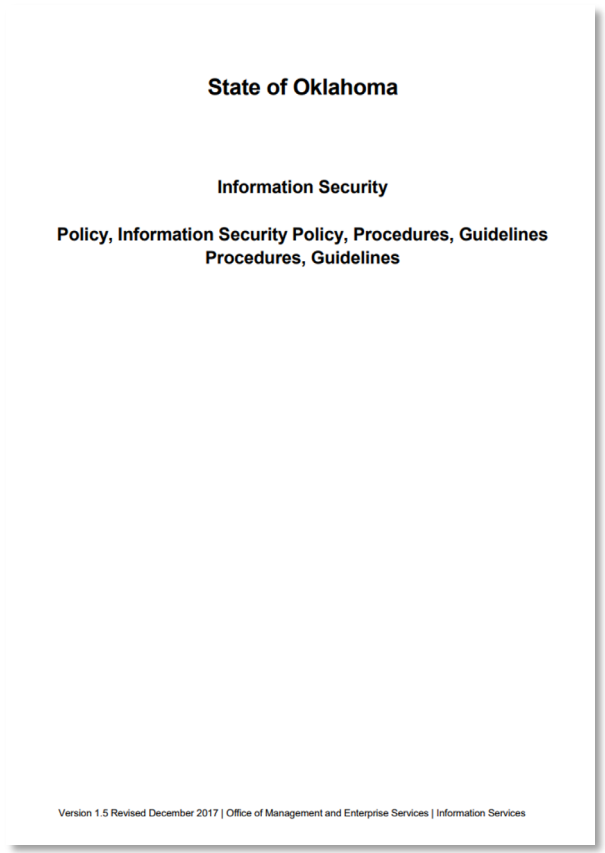
```
policy.url.1=file:${java.home}/lib/security/java.policy
policy.url.2=file:${user.home}/.java.policy
```

Example

```
  grant signedBy "Duke" {
      permission java.io.FilePermission "/tmp/*", "read,write";
  };
  grant {
      permission java.util.PropertyPermission "java.vendor", "read";
  };
```

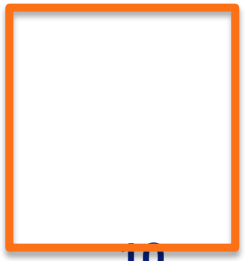


17 pages



94 pages

Where do Policies fit in a Security Program



Policies, Standards, Procedures & Guidelines

Information Security Policy Framework

- What do we use Policy Framework for?

RSAConference2019
Asia Pacific & Japan

Challenges of Information Security Policy Management

Defining the Problem

Information Security Policy Framework

- Challenges

Do we have all the policies we need to satisfy auditors, certification authorities & customers?

Does our organization effectively use our policies? Do members understand and comply?

Can we keep them up-to-date as fast as our organization changes?

Challenges

Inform & Control Outcome

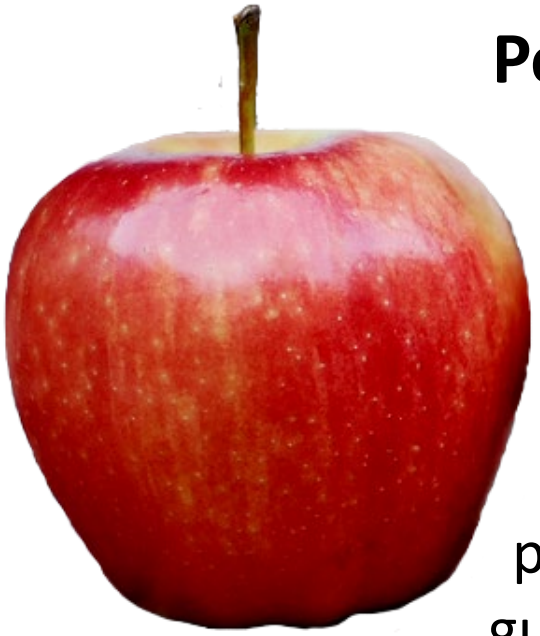
- Too many policies to read
- Confusing, potentially conflicting information
- Long documents in legal jargon
- Hard to find specific information
- Hard to verify compliance
- Diverse audience with different expectations

Challenges

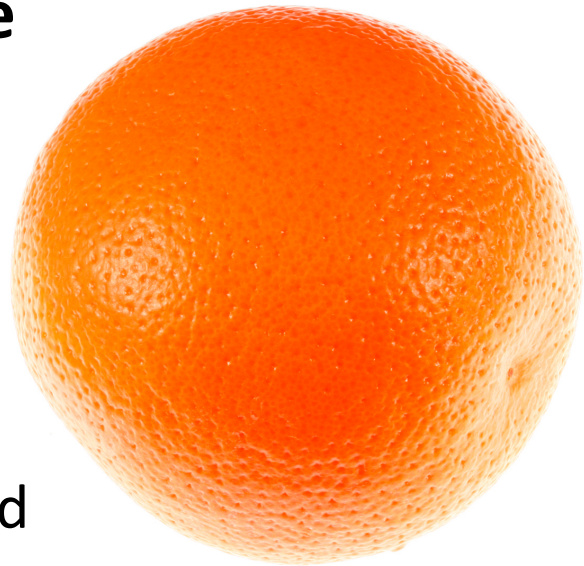
Align with Business Goals

- Business and technology change fast, very hard to keep up
- Different content requires different owners and skill sets
- Some documents change more often than others
- Requires resources to maintain policies
- Uneven requirements (locations, business units, platforms)

What goes into a policy, standard and procedure?



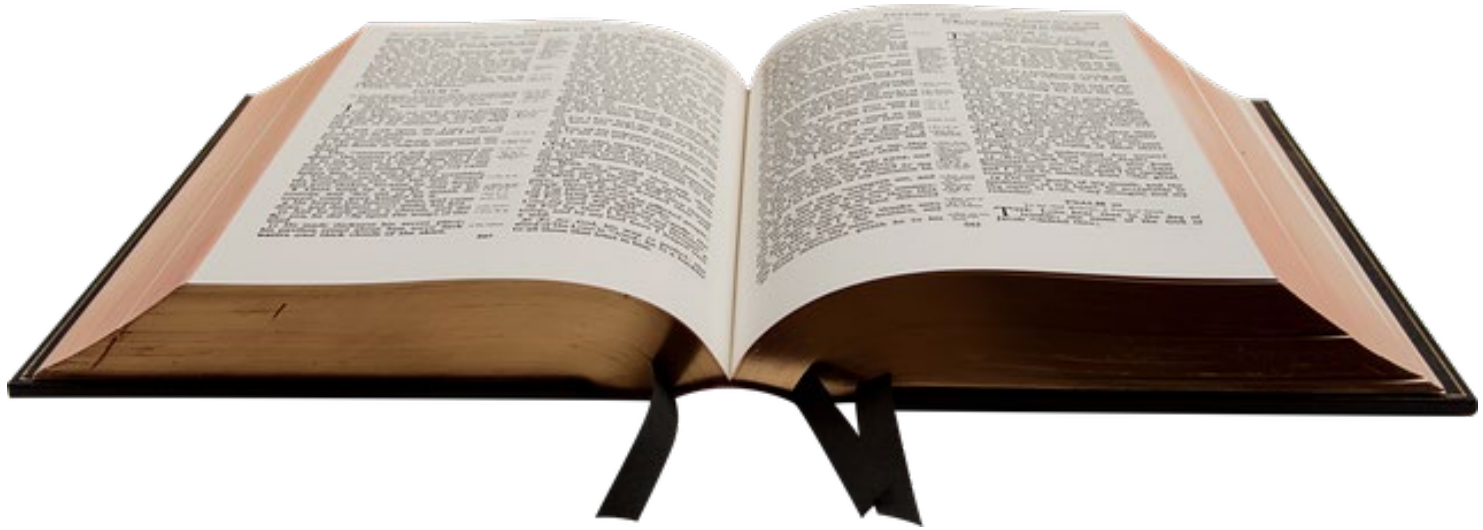
Policy ≠ Standard ≠ Procedure



Most policies are a mixture of policies, standards, procedures and guidelines, making them even harder to manage and consume.

Why is it challenging?

We are trying to fit an increasingly complex, non-linear, and multi dimensional body of knowledge into a linear document, and expecting lay people to understand and comply with it.



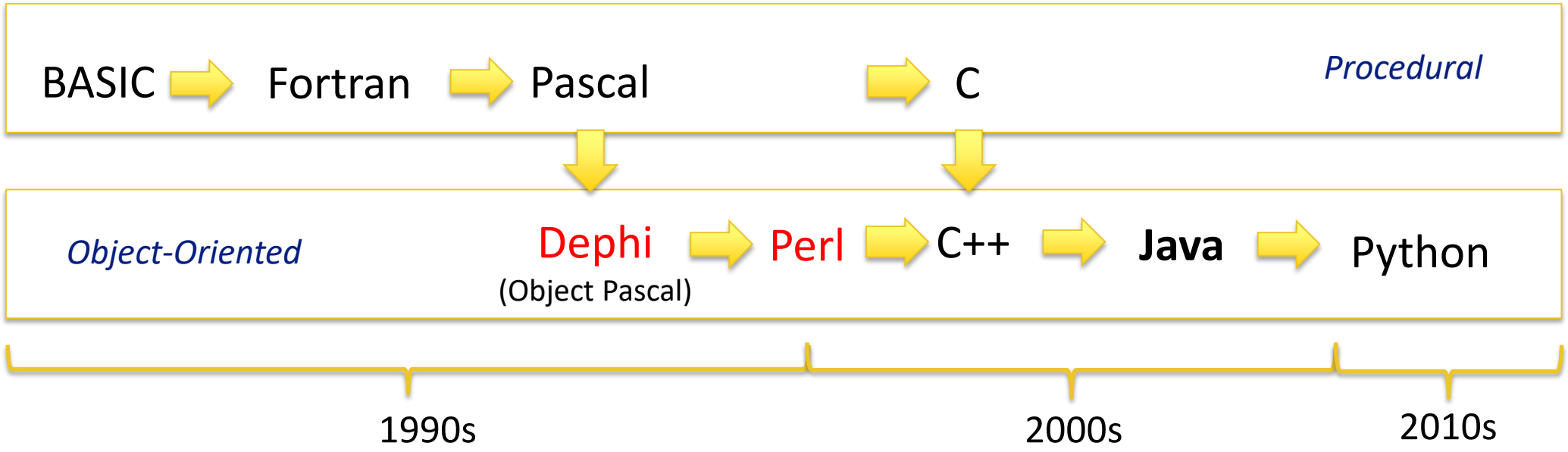
RSAConference2019
Asia Pacific & Japan

Object-Oriented Approach to the Rescue

A Very Short Summary of Object-Oriented Design

Foreword

- This is not a complete overview of Object-Oriented Design
- Not all concepts are transferable to policy framework
- My journey from procedural to object-oriented paradigms:



Why Object Oriented Approach?

- We evolved to understand our surroundings as objects
- Comes more natural to people, computers don’t care
- Better suited to address certain problems than others
- It is an approach, not a technology
- Helps isolate problems into manageable bits
- Helps prevent reinventing the wheel
- Encourages (or forces) structure

Basics

Class: **Cat**
Properties (data)
- breed
- color
- age
- sex
- name

Methods (action)
- run
- sleep
- jump

Encapsulation
(Data hiding)

Instances of Class Cat

Object: **fluffy**
Properties (data)
- breed: short haired English Blue
- color: bluish gray
- age: 6
- sex : female

Object: **midnight**
Properties (data)
- breed: unknown
- color: black
- age: 6
- sex : male

Interface
- Toilet Trainable
- Domestic
- Walkable

Inheritance

Organism

Animal

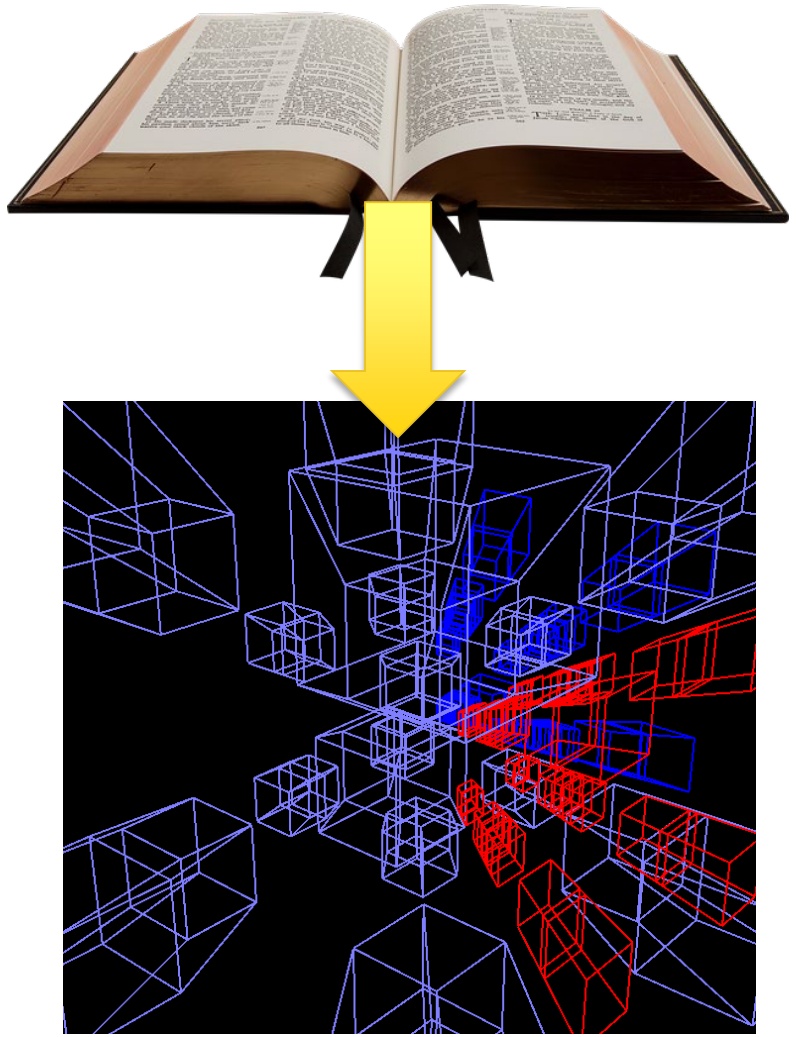
Cat

Dog

Cat ≠ Dog
Cat & Dog are related

Major benefits

- Decrease complexity
- Encapsulation helps prevent unintended conflicts
- Ability to work in parallel
- Imposes structure
- Offers multiple ways to reuse (inheritance, delegation, composition)



RSAConference2019
Asia Pacific & Japan

Putting It Together

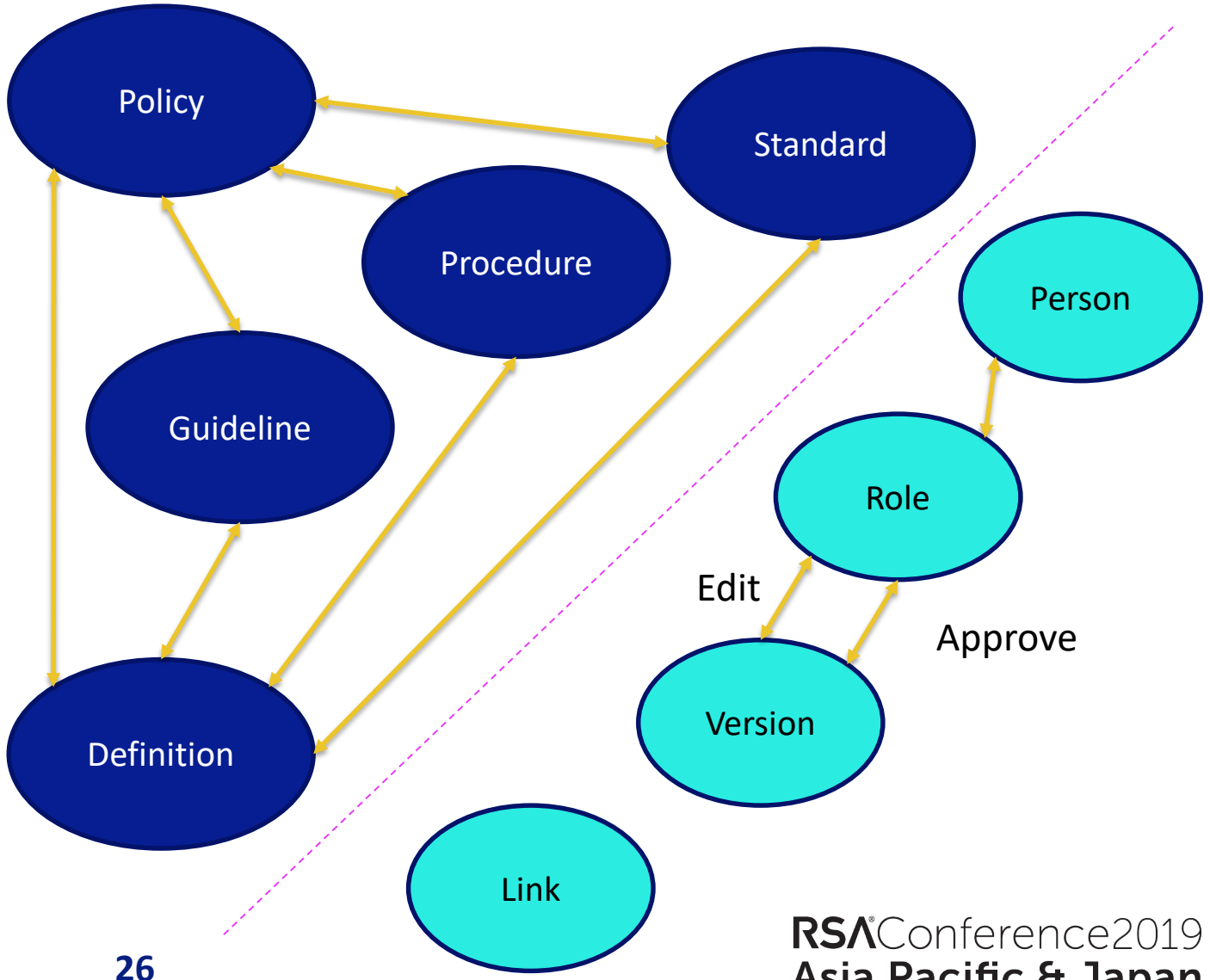
Reevaluating the Policy Framework

Step 1: Define Classes

- Determine
  - Goals
  - Audience
  - Differences
  - Commonalities
  - Owner
- Define
  - Structure
  - Content

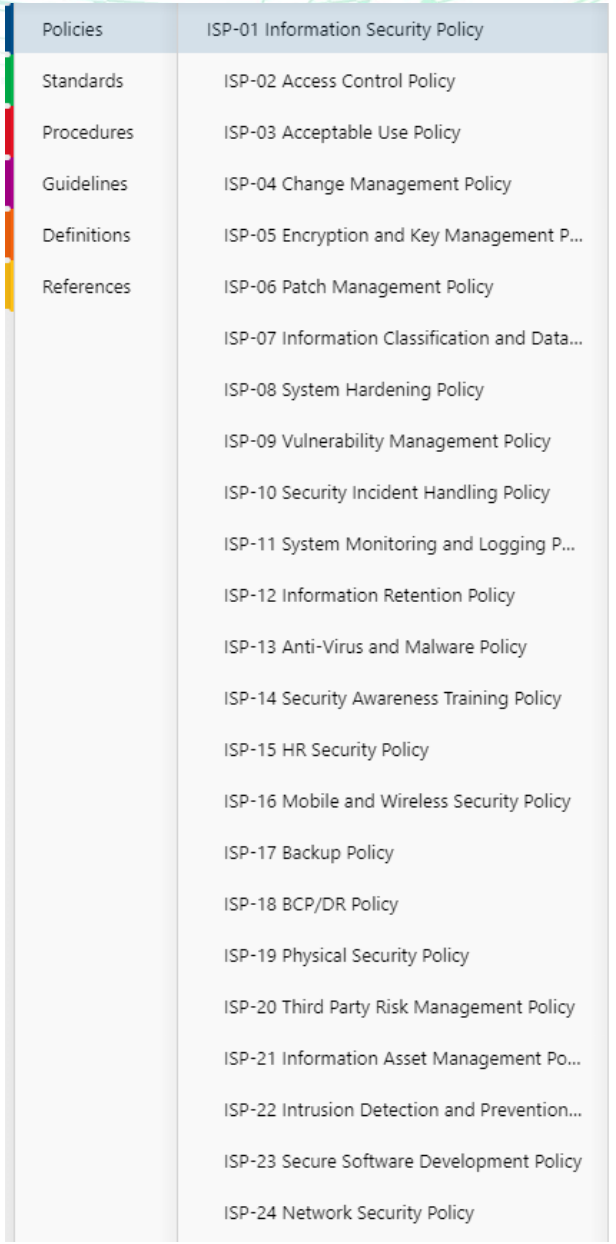
Step 2: Define Relationships

- How policies, standards, procedures, and guidelines are related to each other
- Do we need supporting classes?
  - External Reference Link
  - Person/Role
  - Version
  - Locale



Step 3: List Policies

- How many policies do we need?
  - ISACA says no more than 2 dozen
  - Each with a short policy statement
- What policies are you asked for?
  - Customers, your organization, certifications
- What policies do you currently have?
  - Can they be divided into multiple policies?
  - Can some content be moved elsewhere?
  - Are they concise and clear?



Step 4: Design Policy Class

- What are the Policy class properties?
- What information is “must have”?
- What information can we keep elsewhere?
- Can you convert your existing policies into this format?
- Do you need more (or less) fields?

	BLUECAT
Policy Name	**Security Incident Handling Policy**
Policy Number	ISP-10 v1.0
Policy Statement	Timely reporting and handling of Information Security Incidents is crucial for BlueCat's business. All suspected Information Security incidents must be reported to the Information Security Officer as outlined in ISR-03 Information Security Incident Procedure. Security Incidents involving physical security, such as natural disasters, lengthy outages, acts of terror and violence must be reported to Crisis Management Team (email: groups-cmt@bluecatnetworks.com).
Rationale	The purpose of this Policy is to establish the Information Security reporting and notification requirements for BlueCat.
Related Policies, Standards and Procedures	This policy extends ISP-01 Information Security Policy ISR-03 Information Security Incident Procedure.
Responsibilities and Policy Details	Information Security Officer is responsible to log all reported Information Security Incidents, classify them based on their severity, gather a response team to respond and escalate when needed. All BlueCat employees are responsible to report suspected Information Security incidents to the ISO.

Revisiting OO Basics for Policy Class

Class: **Policy**
Properties (data)
- name
- number
- statement
- rationale
- related details

Methods (action)
- update
- approve

Encapsulation
(Data hiding)

Instances of Class Policy

Object: **ISP-10**
Properties (data)
- name: Security Incident Handling
- number: ISP-10 v1.0
- statement: <content>
- rationale: <content> …

Object: **ISP-23**
Properties (data)
- name: Secure Software Development
- number: ISP-23 v1.1
- statement: <content>
- rationale: <content> …

Interface
- Versionable
- Viewable
- Requires Approval

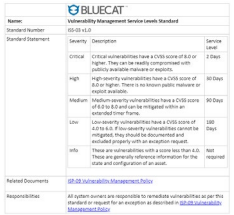
Inheritance

Page

Document

Policy

Standard



Policy ≠ Standard
Policy & Standard are related

Step 6: Create Instances of Policy Class

- Create/move parent Information Security Policy to establish scope, roles, and other top level entities
- Move your existing policies into your new structure
- Identify content to move to other policies, standards, or procedures
- Identify, move, and link definitions

Example: Encryption and Key Management Policy – Links to related documents

Related Policies, Standards and Procedures	This policy extends ISP-01 Information Security Policy ISS-02 Encryption Standard ISR-01 Customer Data Handling Procedure FIPS 140-2 Security Requirements for Cryptographic Modules Standard

Step 7: Design Standard Class

- Standards should provide measurement for compliance
- They will change more often than policies
- They should be unambiguous, precise, and consistent
- They often don't need executive approval

Example:

Password Strength Requirements
(Part of Password Standard)

1) be a minimum of 8 characters;
2) cannot be one of the last 10 previous passwords used;
3) contain characters from three of the following five categories:

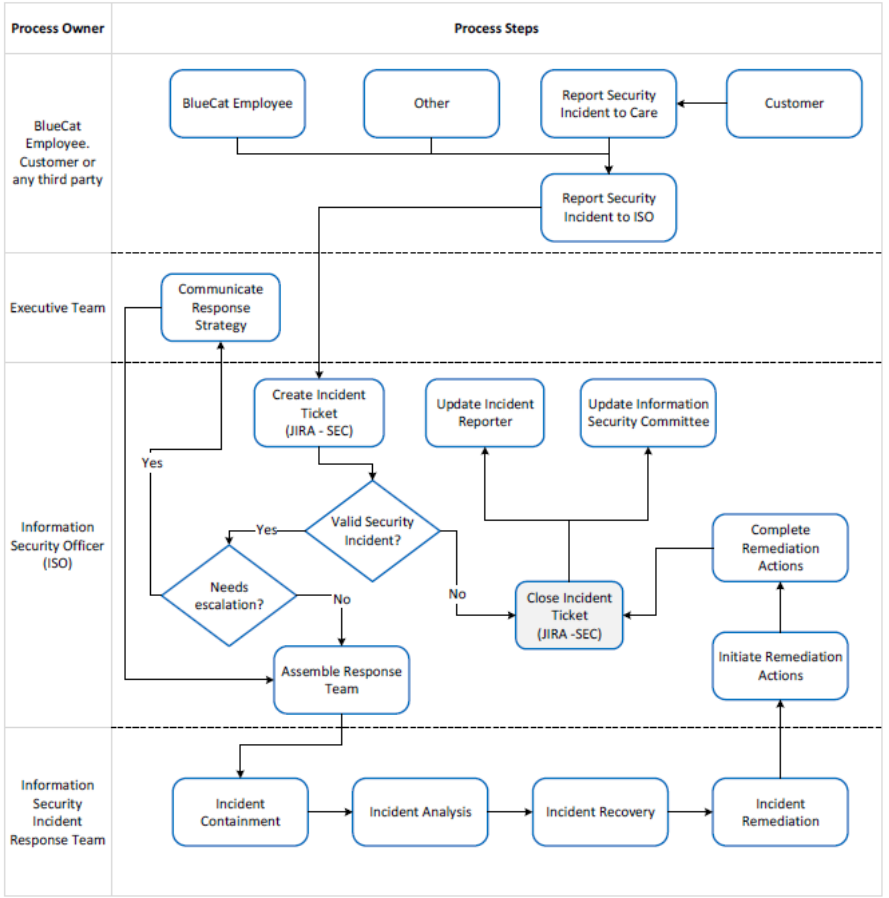
- Uppercase characters of European languages (A through Z, with diacritic marks, Greek and Cyrillic characters)
- Lowercase characters of European languages (a through z, sharps, with diacritic marks, Greek and Cyrillic characters)
- Base 10 digits (0 through 9)

…

Step 8: Design Procedure Class

- Procedures provide step by step instructions to compliance
- They are often created and maintained by Business Units
- In many cases, linking to an existing document works best
- Procedures may contain sensitive information not meant to be distributed
- They tend to have concurrent versions (e.g. hardening guide for Windows, Linux, Mac)

IS Incident Process Map

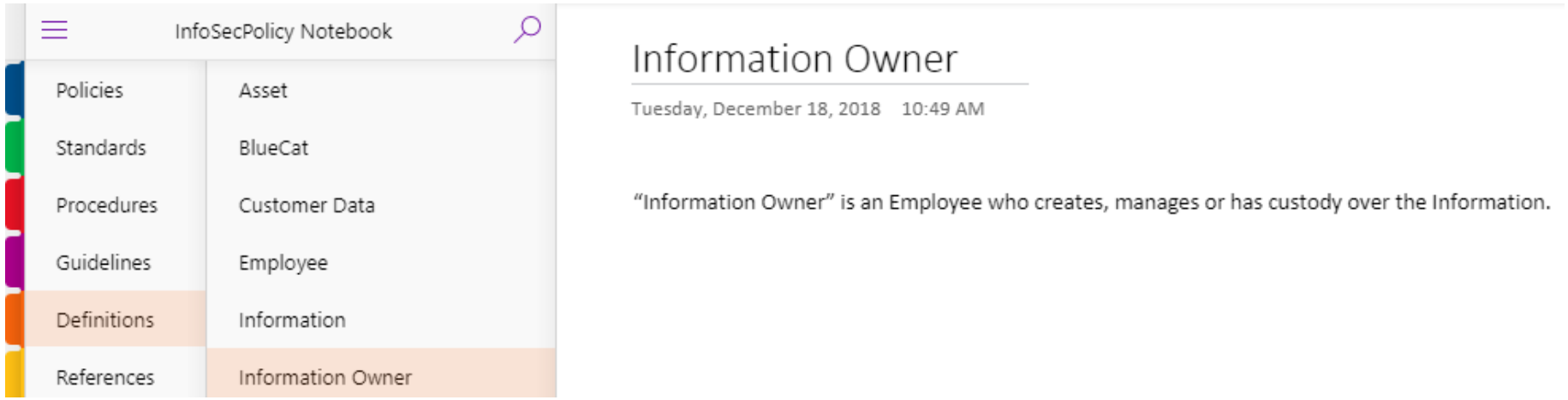


Step 9: Design Guideline Class

- Guidelines are discretionary
- They are often created and maintained by Business Units
- In many cases, linking to an existing document works best
- They tend to change frequently
- They tend to be large documents in free form

Step 10: Design Definition Class

- Help prevent duplicate and inconsistent data (optional)
- They are referred from policies, standards, procedures, and guidelines as a link
- They should be reviewed regularly to ensure that they are accurate and up-to-date



A Simple Policy Framework Template

- Example object *properties* (fields) for a minimalist policy framework template:

Policy	
PK **PK**	**Policy Number** **Version**
	Policy Name **Statement** **Rationale** Related Documents Details and Responsibilities History Approval **Published**

Standard	
PK **PK**	**Standard Number** **Version**
	Standard Name **Statement** Related Documents Details and Responsibilities History Approval **Published**

Procedure	
PK **PK**	**Procedure Number** **Version**
	Procedure Name Content Link to Document

Guideline	
PK **PK**	**Guideline Number** **Version**
	Guideline Name Content Link to Document

Definition	
PK	**Definition Name**
	Content

RSAConference2019
Asia Pacific & Japan

Implementation Notes

Practical Aspects of Implementing the Policy Framework

High Level Requirements

Must Have

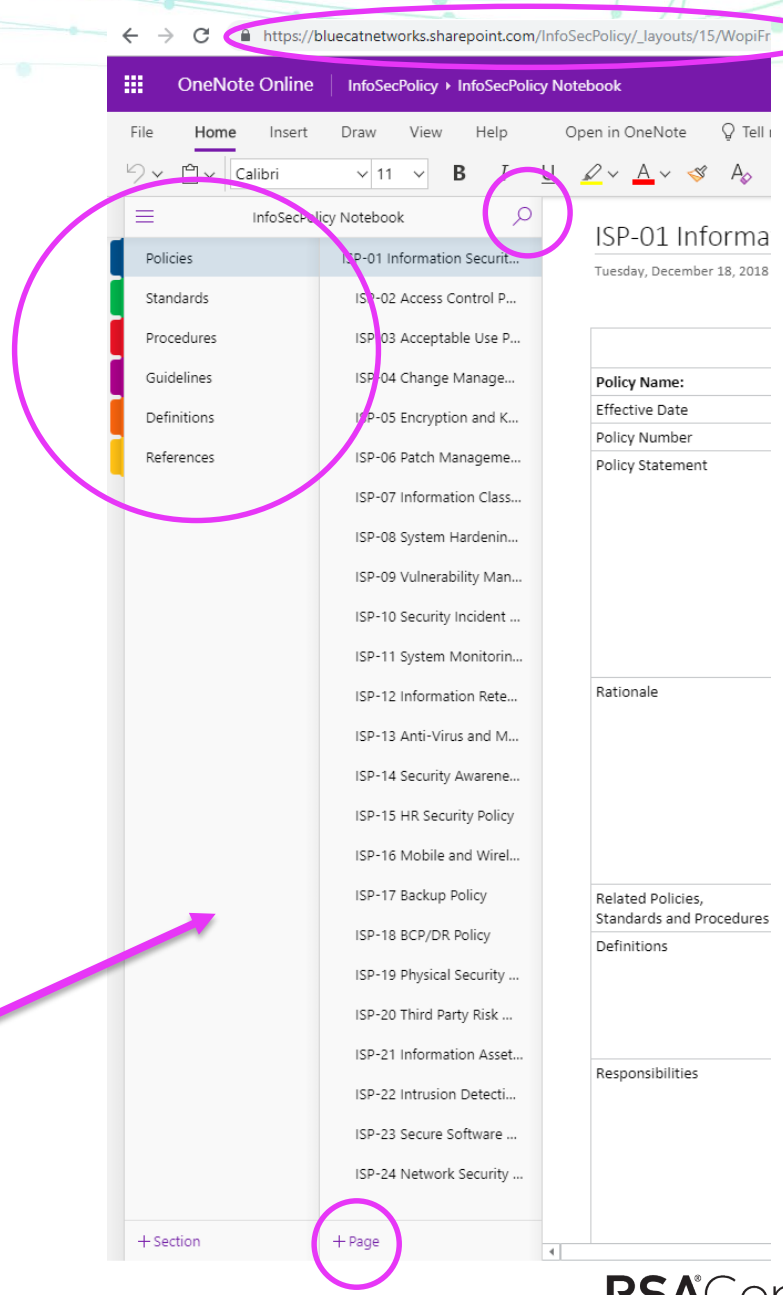
- An Intranet Portal
- Role Based Access Control
- Link documents internally
- Easy to manage
- Version control

Nice to Have

- Different views (HTML, PDF, etc.)
- Object Level Access Control and Logging
- Link documents externally
- Easy to manage, edit, and publish
- Built-in approval/acknowledgement process
- Searchable

Some Options Evaluated

- Jostle
- Wiki.js
- Jira
- Confluence
- Fluid Topics
- Write from scratch!
- Office 365 OneNote Online



Summary

- Policies are essential tools, use them effectively
- Policies are complex, make them easier to manage and consume
- Object-Oriented Approach can help
- Clearly define the structure of your policies, standards, procedures & guidelines
- Link documents to a single source of truth, don’t repeat
- Choose the optimal medium to implement your framework

Recommendations

- Understand your needs. One size does not fit all!
- Less is more. Avoid redundancy, be concise
- Leverage the tools you have
- Realize that policy framework is more than a document repository
- Make it easy to manage and consume
- Policy framework management is a process, not a project

RSAConference2019
Asia Pacific & Japan

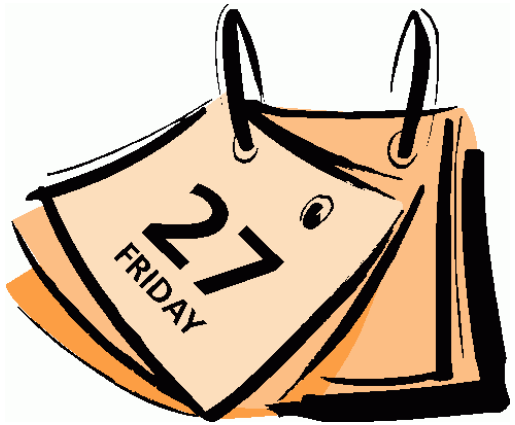
Apply What You've Learned

When you return to your office ...

When you return to your office

Next week you should

- Take an inventory of your security policies, standards, procedures, and guidelines
- Determine if you have all you need or if you have gaps to fill



Within 3 months you should

- Make a list of all the policies you think your organization needs
- Determine what information you need in a policy and convert your existing policies to this format
- Choose a medium to manage your policy framework
- Start building your policy framework

Thank you!

Please contact me for further information or discussion

Cuneyt Karul

ckarul@bluecatnetworks.com

LinkedIn: https://www.linkedin.com/in/cuneytkarul/