Implementing Critical Cybersecurity Controls in a DevOps Environment

Steven Sim , Vice President (ISACA Singapore Chapter)

15 Jul 2020

ISACA Singapore Chapter

Backdrop – New Cybersecurity Normal

- All organisations that have a cyber footprint can be breached
- Not a matter of IF but **WHEN** incidents would happen?
- Either you **KNOW** you are breached or you don’t?
- How can we better prepare ourselves against the **INEVITABLE**?

ISACA Singapore Chapter

Backyard - DevOps and Cloud

- **Benefits**

  - Deliver applications and services at high velocity
  - Evolve and Improve products at a faster pace
  - Improve trust between development and operations teams

- **Cloud Adoption**

  - For ability and flexibility, cloud integration allows resources to be de-focused
  - Rely on Infrastructure as Service (IaaS) or Platform as a Service (PaaS)
  - More common for public or virtual private cloud to be used.

“Infrastructure as Code”

- Configuration of servers can be run as code
- Can be versioned and tested
- Assure repeated configurations
- Eliminates issue of code that works fine in staging failing in production
- Continuous Integration / Continuous Delivery or Deployment: Jenkin, Dockers
- Configuration Management: Chef, Puppet, Saltstack, Ansible, Terraform, etc
- Containerisation and Microservices: Kubernetes, etc

Key Security Concerns

Docker Hub Distributing Cryptomining Malware?

June 26, 2020 container images, container security, cryptomining, docker hub, malware

by Mike Vizard

A pair of cybersecurity reports published this week suggests the level of cryptomining malware lurking in the Docker Hub repository is potentially greater than most IT teams realize.

- Automation is means to repeat human errors with rigor in a consistent manner.
- Cloud reduces control and visibility at hardware and network
- Faulty spin-ups may leave a virtual machine in unstable state
- Lack segregation of duties between DEVeloper and OPerator
- How do we know developers adhered to secure development standards?
- Multiple images of varying security may be running?
- How quickly will patches be released when a security flaw is found?

What is your Cyber Security and Risk Culture?

DevSecOps & Security Responsibility

*"The simple premise of DevSecOps is that **everyone in the software development life cycle is responsible for security**, in essence bringing operations and development together with security functions. DevSecOps aims to embed security in every part of the development process. It is about trying to automate core security tasks by embedding security controls and processes early in the DevOps workflow (rather than being bolted on at the end). For example, this could be the case when migrating to microservices, building out a CI/CD pipeline, compliance automation or simply testing cloud infrastructure."*

– CSO Online

DevSecOps & Security Responsibility

*“DevOps is accomplished through automation and technology, but culturally it depends on creating the **three Cs—collaboration, communication and cohesiveness**—between development and operations. ”*

– ISACA

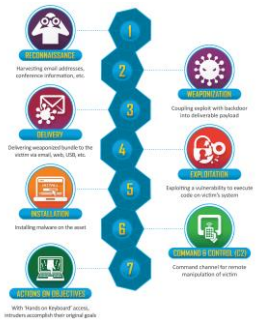
ISACA Singapore Chapter

Governance underscores the Ability to Future-proof against Threats

❶

Adopt IT Risk Management Framework

❷

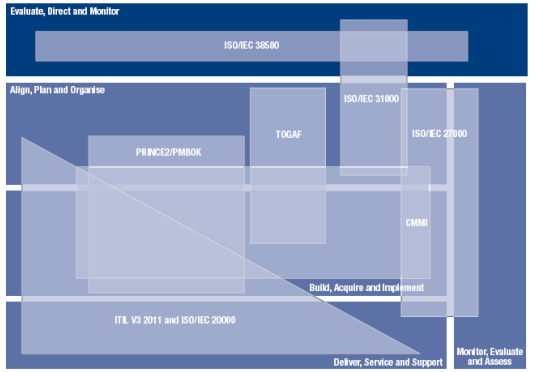


Perform Threat Modelling

❸

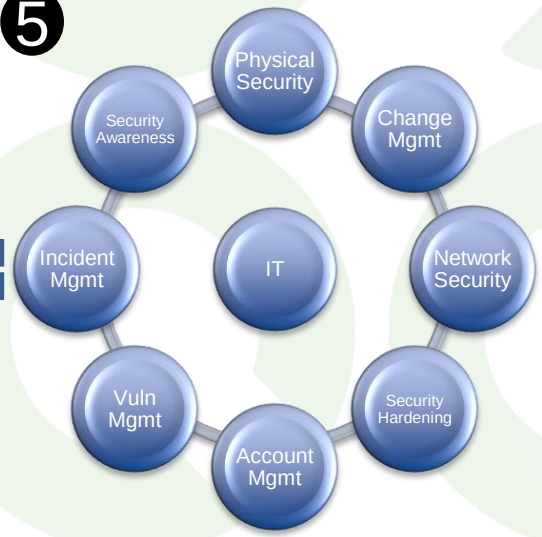
Adopt Key Principles

❹



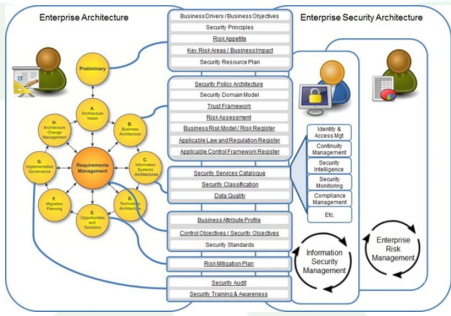
Adopt Cybersecurity Framework

❺



Determine Key Security Controls

❻



Determine Architecture

Doing the right things

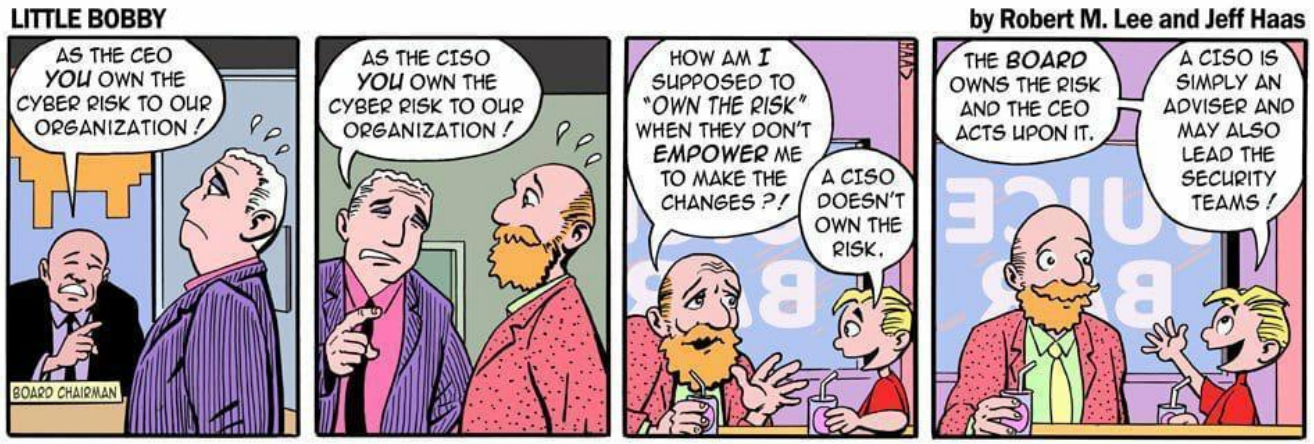
Doing the things right

Adopt IT Risk Management Framework

ISACA Risk IT Framework

Key points

- Business-operation-IT risk **alignment**
- Risk **optimization** is key to risk management
- Risk owner is **accountable**



Risk of Adoption vs Risk of Non-adoption

Risk of non-adoption

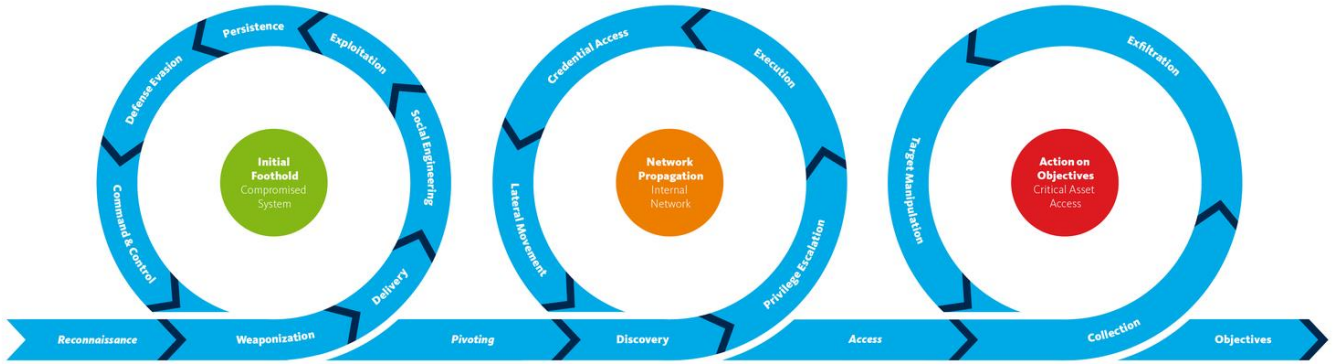
- Risk of decreased competitive advantage
- Practitioner opportunity cost
- Shadow adoption

http://www.isaca.org/Knowledge-Center/Research/Documents/DevOps-Practitioner-Considerations_whp_Eng_0815.pdf

ISACA Singapore Chapter

❷

Perform Threat Modelling



MITRE Enterprise ATT&CK™ Framework

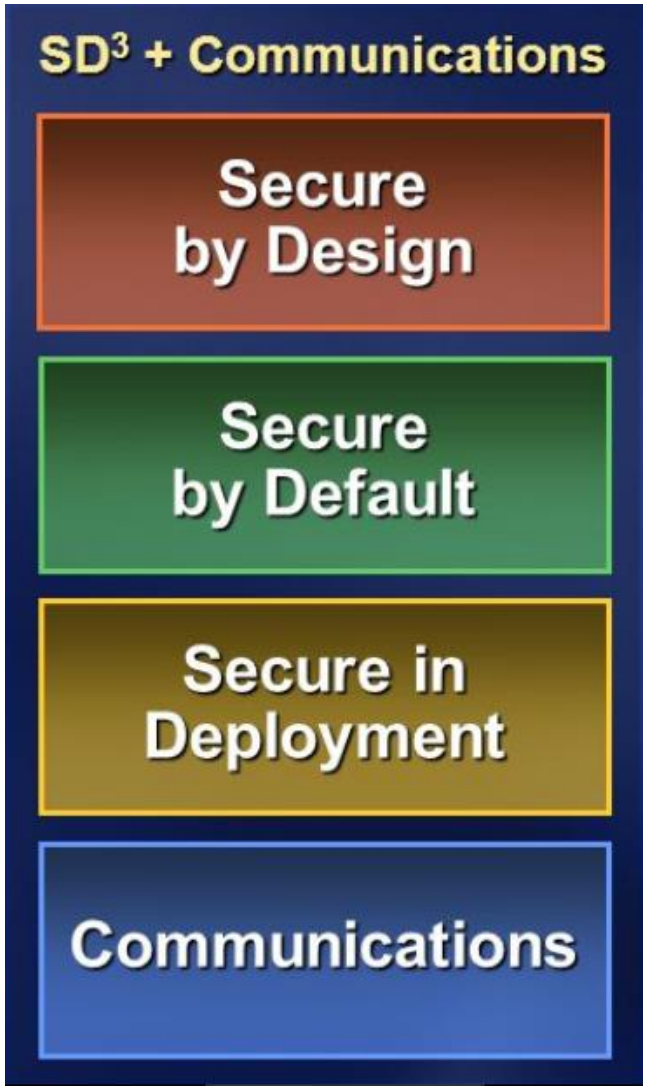
Persistence	Privilege Escalation	Defense Evasion	Credential Access	Discovery	Lateral Movement	Execution	Collection	Exfiltration	Command and Control
Image File Execution Options Injection			Forced Authentication	Network Share Discovery	AppleScript		Man in the Browser	Exfiltration Over Physical Medium	Multi-hop Proxy
Plist Modification			Hooking	System Time Discovery	Third-party Software		Browser Extensions		Domain Fronting
Valid Accounts			Password Filter DLL	Peripheral Device Discovery	Windows Remote Management		Video Capture	Exfiltration Over Command and Control Channel	Data Encoding
DLL Search Order Hijacking			LLMNR/NBT-NS Poisoning	Account Discovery	SSH Hijacking	LSASS Driver	Audio Capture		Remote File Copy
AppCert DLLs		Process Doppelgänging	Securityd Memory	File and Directory Discovery	Distributed Component Object Model	Dynamic Data Exchange	Automated Collection	Scheduled Transfer	Multi-Stage Channels
Hooking		Mshta	Private Keys	System Information Discovery		Mshta	Clipboard Data	Data Encrypted	Web Service
Startup Items		Hidden Files and Directories	Keychain		Pass the Ticket	Local Job Scheduling	Email Collection	Automated Exfiltration	Standard Non-Application Layer Protocol
Launch Daemon		Launchctl	Input Prompt	Security Software Discovery	Replication Through Removable Media	Trap	Screen Capture	Exfiltration Over Other Network Medium	
Dylib Hijacking		Space after Filename	Bash History			Source	Data Staged		Communication Through Removable Media
Application Shimming		LC_MAIN Hijacking	Two-Factor Authentication Interception	System Network Connections Discovery	Windows Admin Shares	Launchctl	Input Capture	Exfiltration Over Alternative Protocol	
AppInit DLLs		HISTCONTROL			Remote Desktop Protocol	Space after Filename	Data from Network Shared Drive		Multilayer Encryption
Web Shell		Hidden Users	Account Manipulation	System Owner/User Discovery	Pass the Hash	Execution through Module Load		Data Transfer Size Limits	Standard Application Layer Protocol
Service Registry Permissions Weakness		Clear Command History	Replication Through Removable Media		Exploitation of Vulnerability		Data from Local System	Data Compressed	
Scheduled Task		Gatekeeper Bypass		System Network Configuration Discovery	Shared Webroot	Regsvcs/Regasm	Data from Removable Media		Commonly Used Port
New Service		Hidden Window	Input Capture		Logon Scripts	InstallUtil			Standard Cryptographic Protocol
File System Permissions Weakness		Deobfuscate/Decode Files or Information	Network Sniffing	Application Window Discovery	Remote Services	Regsvr32			
Path Interception			Credential Dumping		Application Deployment Software	Execution through API			Custom Cryptographic Protocol
Accessibility Features		Trusted Developer Utilities	Brute Force	Network Service Scanning		PowerShell			
Port Monitors		Regsvcs/Regasm	Credentials in Files	Query Registry	Remote File Copy	Rundll32			Data Obfuscation
Screensaver		Exploitation of Vulnerability		Remote System Discovery	Taint Shared Content	Scripting			Custom Command and Control Protocol
LSASS Driver	Extra Window Memory Injection			Permission Groups Discovery		Graphical User Interface			Connection Proxy
Browser Extensions	Access Token Manipulation			Process Discovery		Command-Line Interface			Uncommonly Used Port
Local Job Scheduling	Bypass User Account Control			System Service Discovery		Scheduled Task			Multiband Communication
Re-opened Applications	Process Injection					Windows Management Instrumentation			Fallback Channels
Rc.common	SID-History Injection	Component Object Model Hijacking				Trusted Developer Utilities			
Login Item	Sudo	InstallUtil				Service Execution			
LC_LOAD_DYLIB Addition	Setuid and Setgid	Regsvr32							
Launch Agent		Code Signing							
Hidden Files and Directories		Modify Registry							
.bash_profile and .bashrc		Component Firmware							
Trap		Redundant Access							
Launchctl		File Deletion							
Office Application Startup		Timestomp							
Create Account		NTFS Extended Attributes							
External Remote Services		Process Hollowing							
Authentication Package		Disabling Security Tools							
Netsh Helper DLL		Rundll32							
Component Object Model Hijacking		DLL Side-Loading							
Redundant Access		Indicator Removal on Host							
Security Support Provider		Indicator Removal from Tools							
Windows Management Instrumentation Event Subscription		Indicator Blocking							
Registry Run Keys / Start Folder		Software Packing							
Change Default File Association		Masquerading							
Component Firmware		Obfuscated Files or Information							
Bootkit		Binary Padding							
Hypervisor		Install Root Certificate							
Logon Scripts		Network Share Connection Removal							
Modify Existing Service		Rootkit							
		Scripting							

attack.mitre.org

ISACA Singapore Chapter

❸

Adopt Key Principles – “Security as Code”



Microsoft

1. Tender Specs (Firewall, VPN, Common Criteria, etc)
2. Product allows Vulnerability to be Managed
3. Layered Defense Architecture
4. Architecture Security Review

1. Security Standards
2. Server Hardening i.e. Disable Unnecessary Services
3. Network-based Firewall
4. Pre-deployment Vulnerability Assessment & Penetration Testing

1. Regular Vulnerability Scan
2. Regular Vulnerability alert Monitoring
3. Timely Vulnerability Remediation/Patching
4. **Continuous Audit and Monitoring**

1. Security Training and Awareness
2. Security Advisories to Custodians
3. Phishing Simulation Exercise
4. **Extension to Supply Chain**

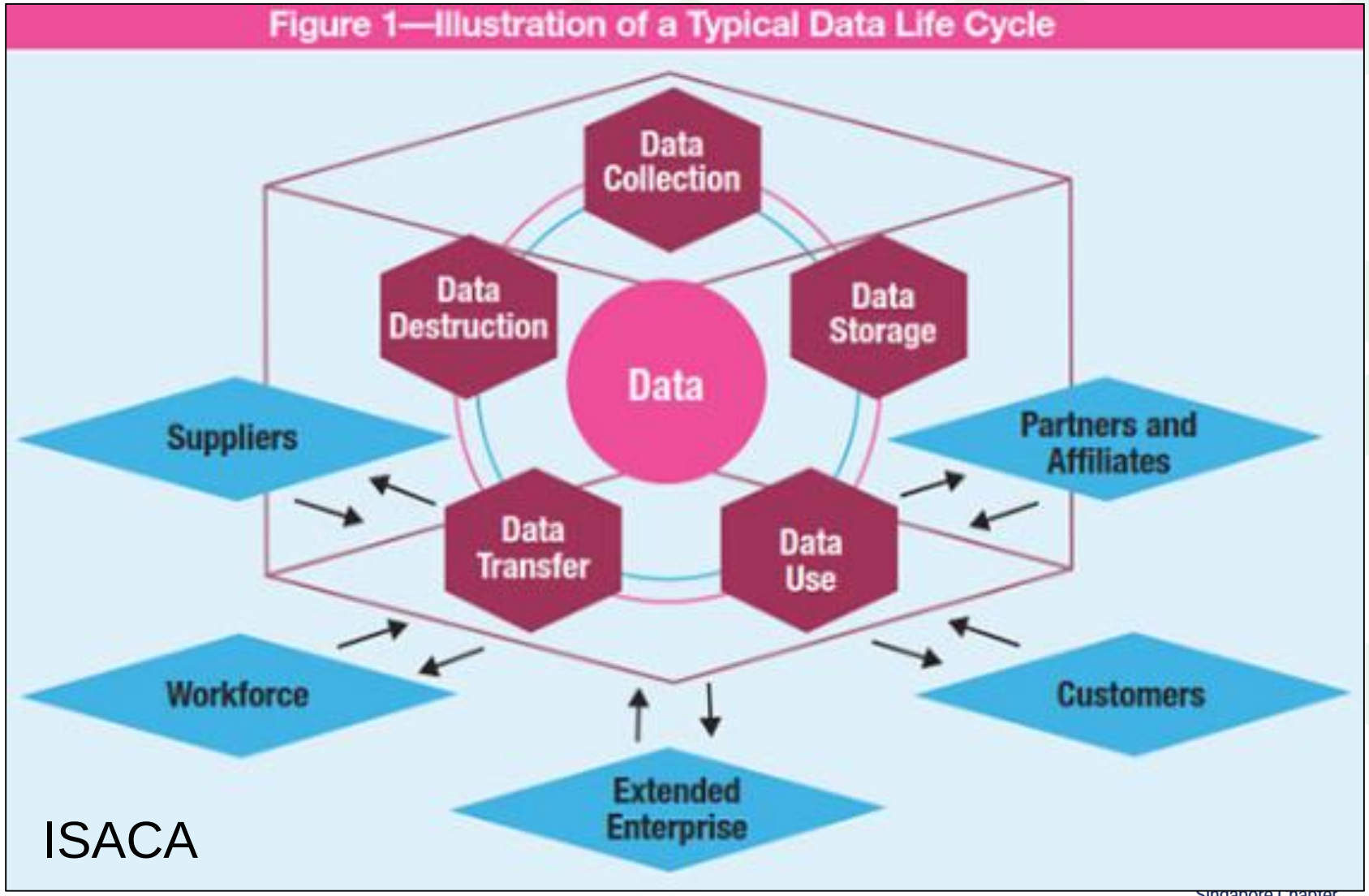
Figure 4—Supply Chain Security Risk Management by Phase

Phase	Activities
Requirements and design	• Perform a risk assessment. • Establish security requirements. • Develop auditing plans.
Manufacture (development)	• Monitor processes and product flows. • Inspect, test, verify and validate final products.
Distribution	• Monitor processes and product flows.
Warehousing	• Monitor processes and product flows. • Check that the product has not been removed, substituted or added.
Deployment	• Monitor processes and product flows. • Check that delivered products and systems are correct and authentic. • Provide user guidance to ensure that products and systems are not adulterated or otherwise compromised.
Operation	• Monitor operation for unusual behavior and damaging events. • Review operational readiness on a continuing basis. • Develop and implement a plan for responding to security incidents.
Maintenance and support	• Monitor suppliers of products and components for any adverse reports relating to the viability of supplier companies or any security or safety issues with products. • Develop contingency plans for potential disruptions in supply of parts or patches, for example, and support.
Disposal	• Monitor disposal of intellectual property and sensitive data, such as personal information and health data, and destruction of media containing such information.

ISACA Singapore Chapter

Privacy-by-Design (integrated with Security-by-Design)

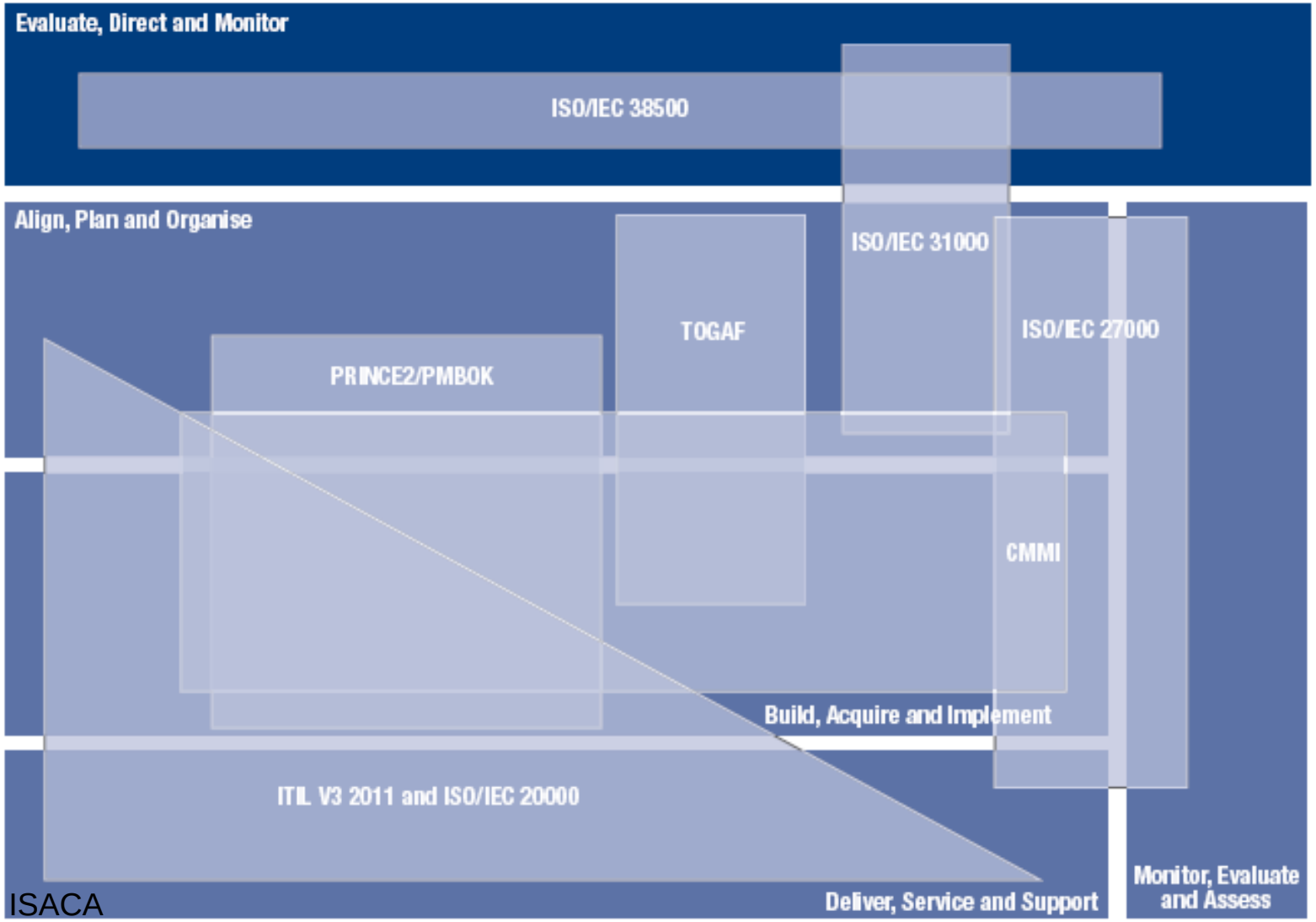
- Data as the new oil
- Adopt a data-centric approach



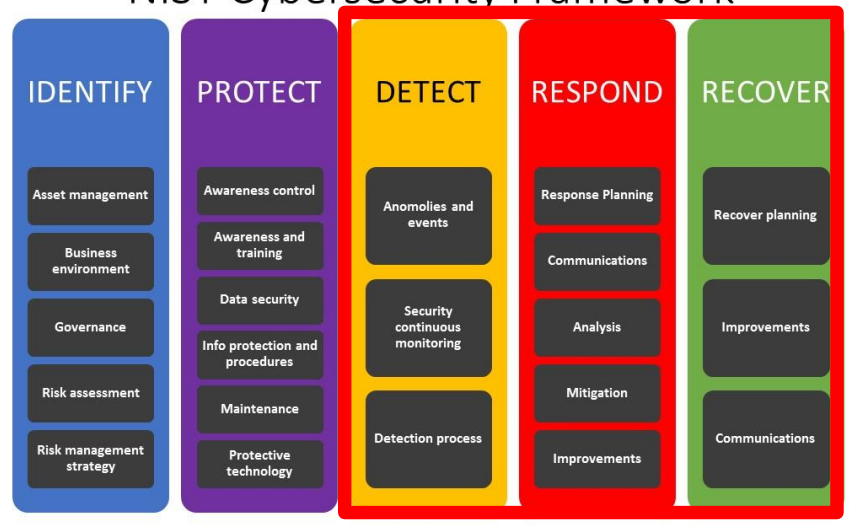
❹

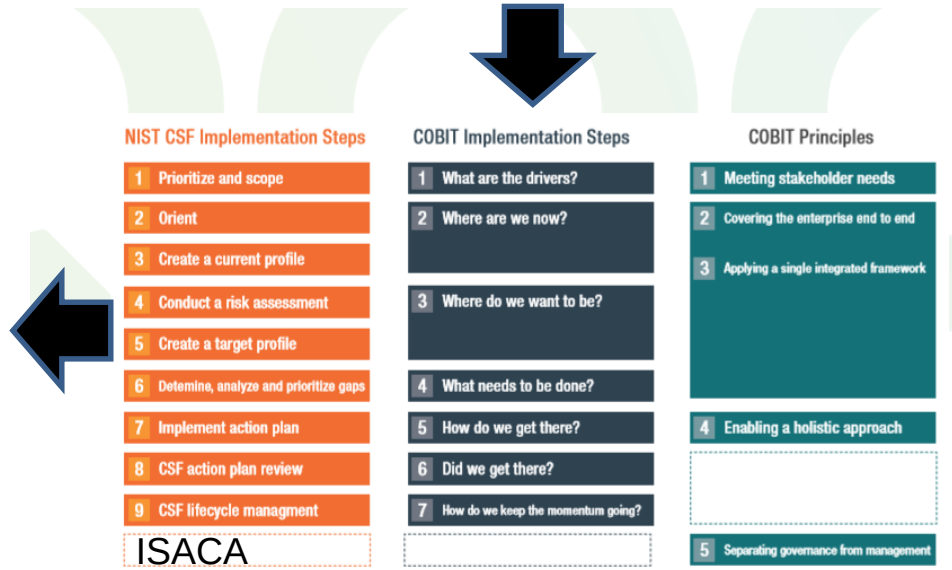
Adopt Cyber Security Framework (1)

COBIT



NIST Cybersecurity Framework





Adopt Cyber Security Framework (2)

DevOps Maturity Model

*“Enterprises that use CMMI or COBIT 5 can align their DevOps approach to gain value and apply adaptive approaches to address challenges. By **adapting robust governance and maturity practices from frameworks like CMMI and COBIT** while maintaining a flexible approach to interpreting requirements from those frameworks, enterprises can realize the benefits of DevOps and still maintain a robust and mature approach.”*

-- ISACA

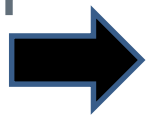
ISACA Singapore Chapter

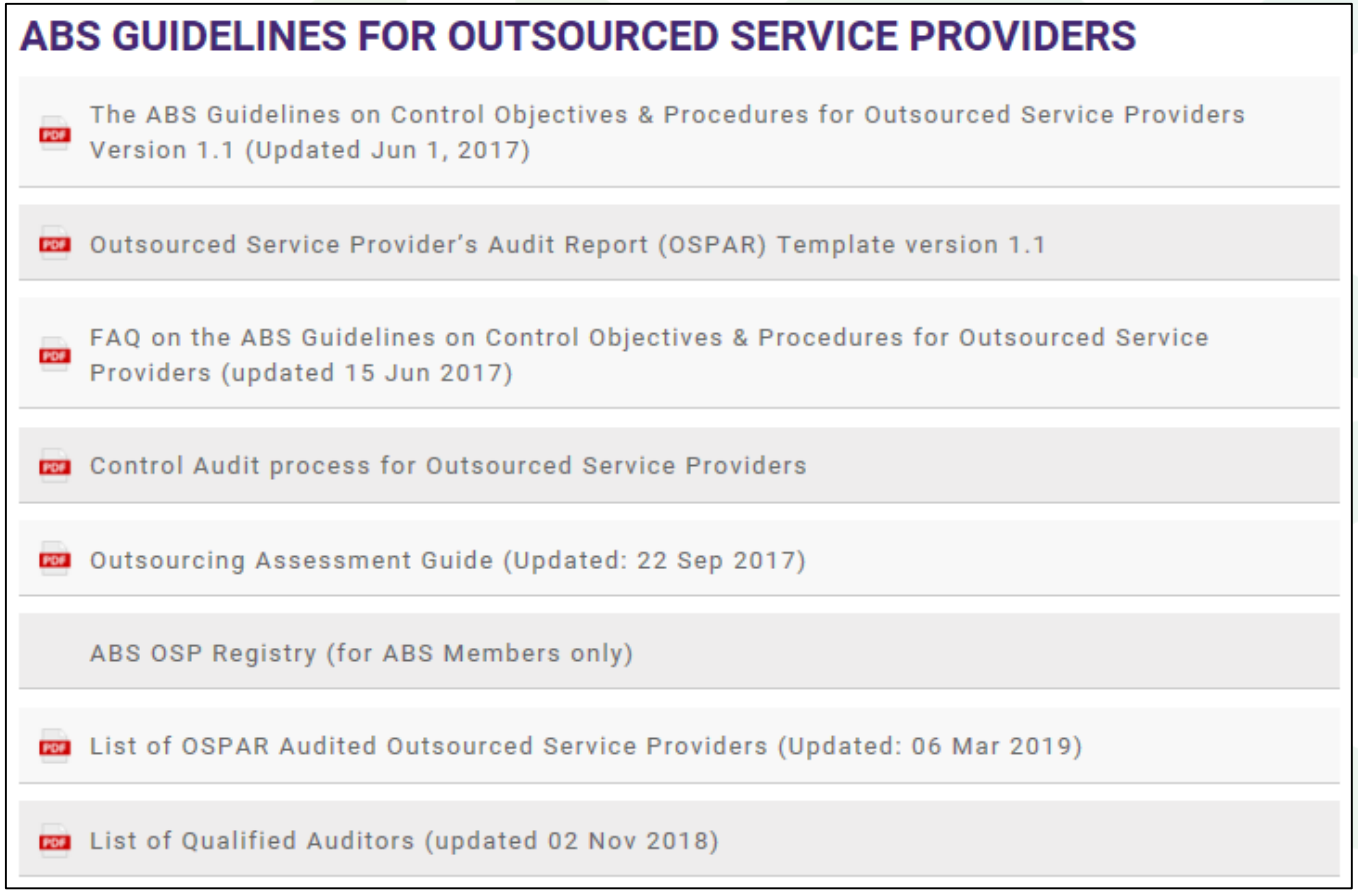
Adopt Cyber Security Framework (3)

Third-party Attestations

1. Multi-Tiered Cloud Services
2. Cyber Security Alliance Cloud
3. Control Matrix – CSA STAR
4. Common Criteria
5. CREST
6. MITRE Pre-ATT&CK Framework
7. ABS Guidelines

- **OSPA (Outsource Service Provider Assessment)**
- PTG (Penetration Testing Guideline)
- RTAASEG (Red Team Adversarial Attack Simulation Exercises Guidelines)





ISACA Singapore Chapter

Key Cloud Security Considerations

1. Asset Criticality and Sensitivity Identification.
2. Roles and Responsibilities for each Key Control.
3. Architecture Security Review and Approval Process.

Off-premise should NOT be worse off than on-premise unless the increased risk is deemed acceptable

Pre-deployment Key Controls: Some Examples

Threat	Controls
Lack of adoption of complying standards	IT security standards compliance
External (Internet) Threats	Vulnerability remediation process
	2-layer Firewall
	Network-based Intrusion Detection System
	24x7 Monitoring
	System hardening
	Vulnerability scanning
	Penetration testing
	Vulnerability advisory tracking
	Component management
	Intranet and Secure remote access
Insider Threats	Host-based Intrusion Detection System
	Security review portal
	Account management
Lack of independent audit assessment	Audit management
Account Breach	2FA deployment
	Admin portal access
Distributed Denial-of-Service (unavailability)	Anti-DDoS protection
Web Defacement (reputation loss)	Web defacement monitoring/recovery
Data Leakage (reputation loss, customer loss)	Data encryption
Delayed Incident Containment and Remediation	**Incident management process and drills**

Cloud Security Key Considerations

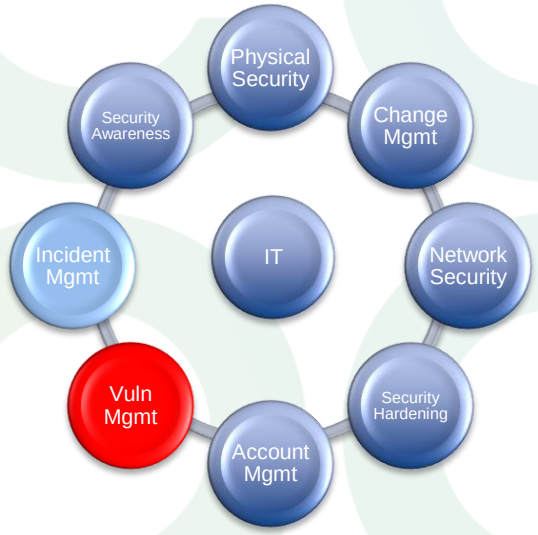
Maintenance phase key controls: Some Examples

Threat	Controls
Lapse in controls and oversight	**Change management controls are put in place.**
	Regular checkpoint meetings to obtain evidence of monthly reviews.
	Obtaining regular independent audit and penetration testing reports.
	Obtaining evidence of regular review of accesses.
	Obtaining evidence of regular review of security checklists and setups.

❺

Determine Key Security Controls

Vulnerability Management



PATCHING is NOT the only means to FIX a VULNERABILITY

Different ways of fixing a vulnerability

- Disable unnecessary services
- Network-based firewall
- Host-based firewall
- Hardening the configuration
- Virtual Patching
- Patching

Vuln Remediation Timeline

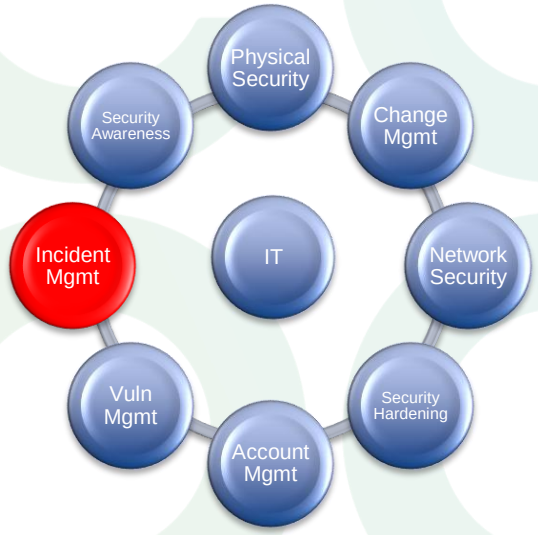
- Risk-based
  Exploit Public Availability
- Attack Surface Exposure
  Peace Time vs Heightened

Systems / Services	Vulnerability Severity	Exploitable remotely from Internet / Building	Exploitable remotely from Gateway / Clients	Exploitable only locally on host
Internet / Extranet-facing	Critical / High			
	Medium			
	Low			
Intranet-facing	Critical / High			
	Medium			
	Low			

Determine Key Security Controls (5)

Incident Management

Optiv IR Org Model

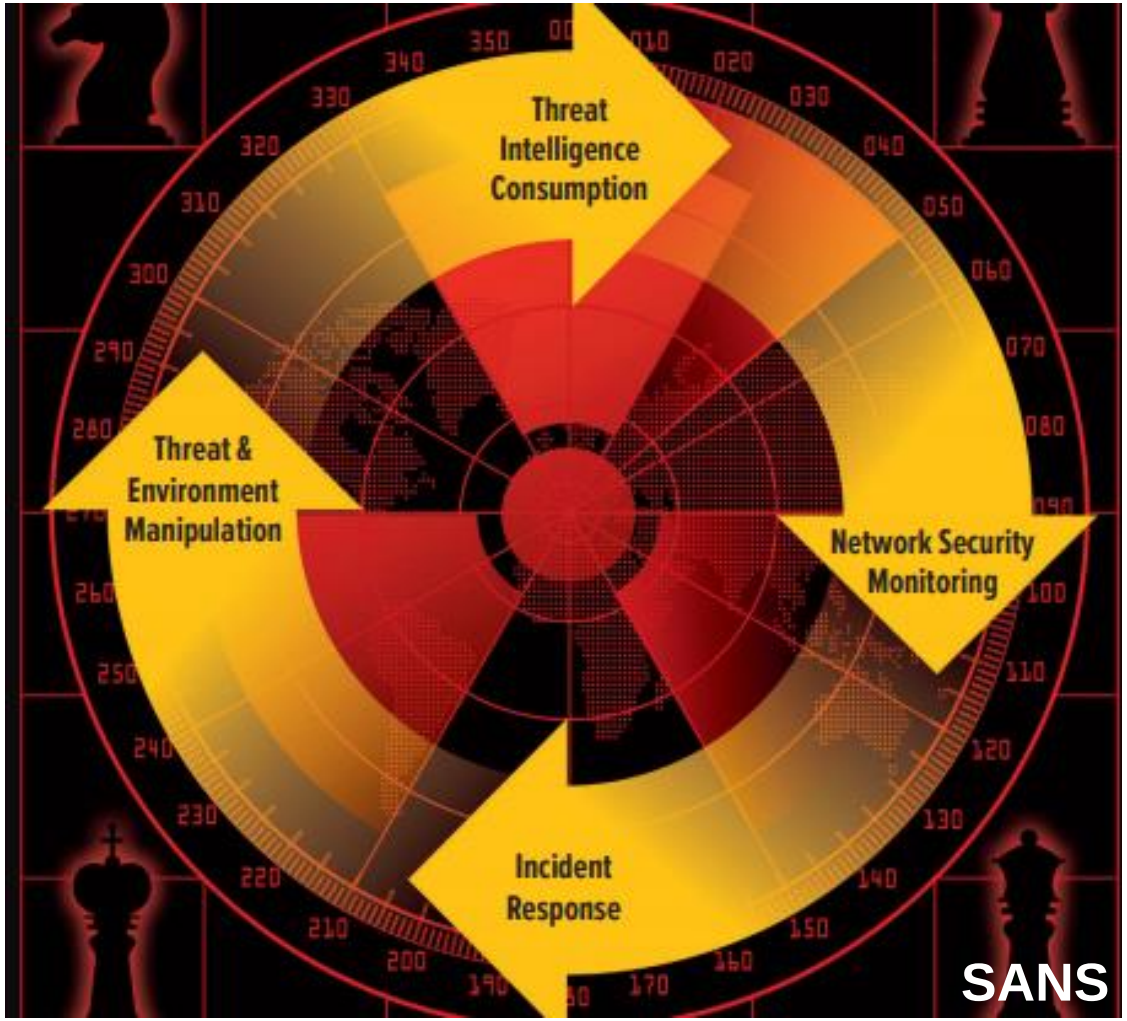


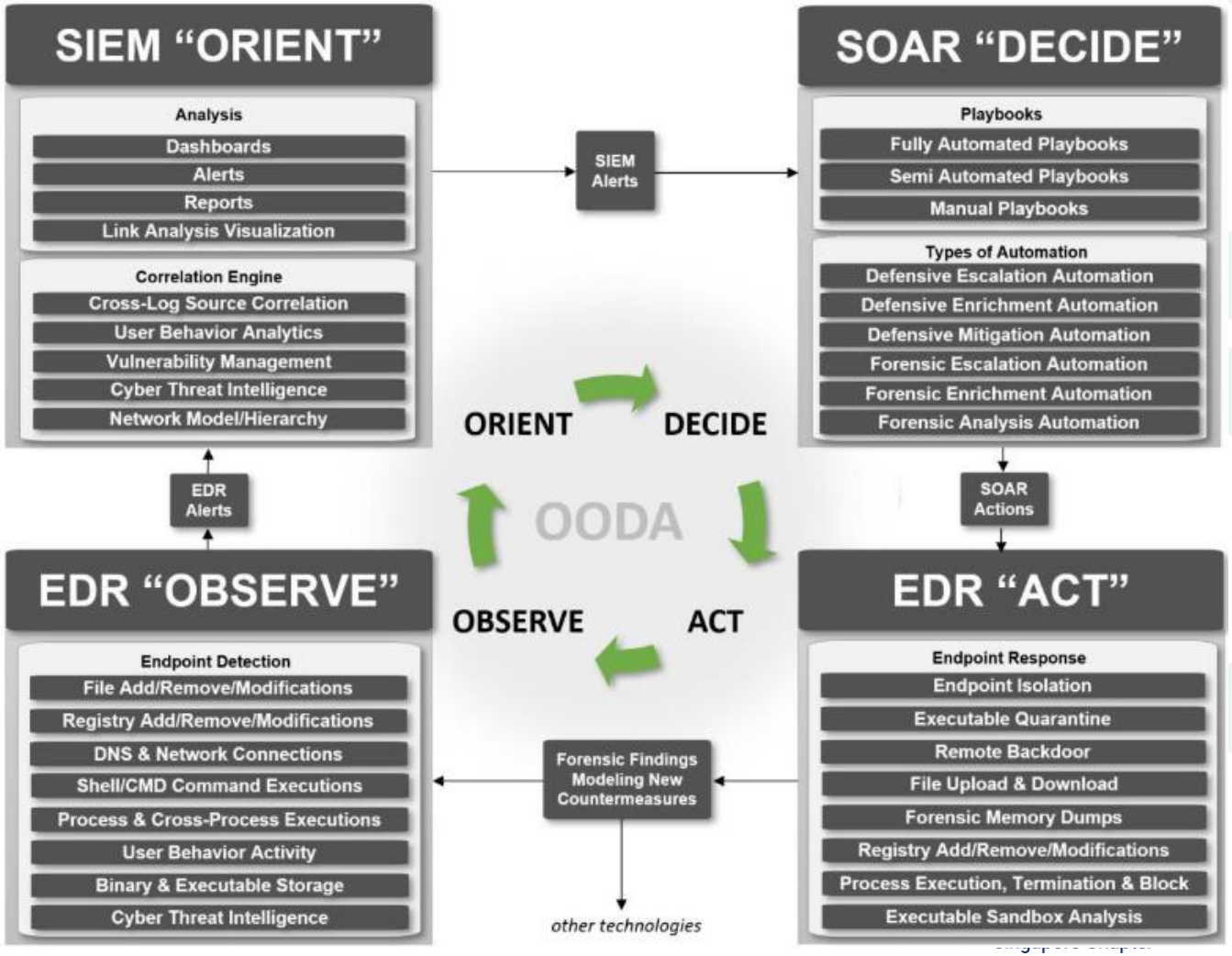
Key Areas of Consideration

- Baselining
- Black Swans
- Business continuity
- Recovery Order
- Alternate Comms

ISACA Singapore Chapter

Active Cyber Defense Strategy



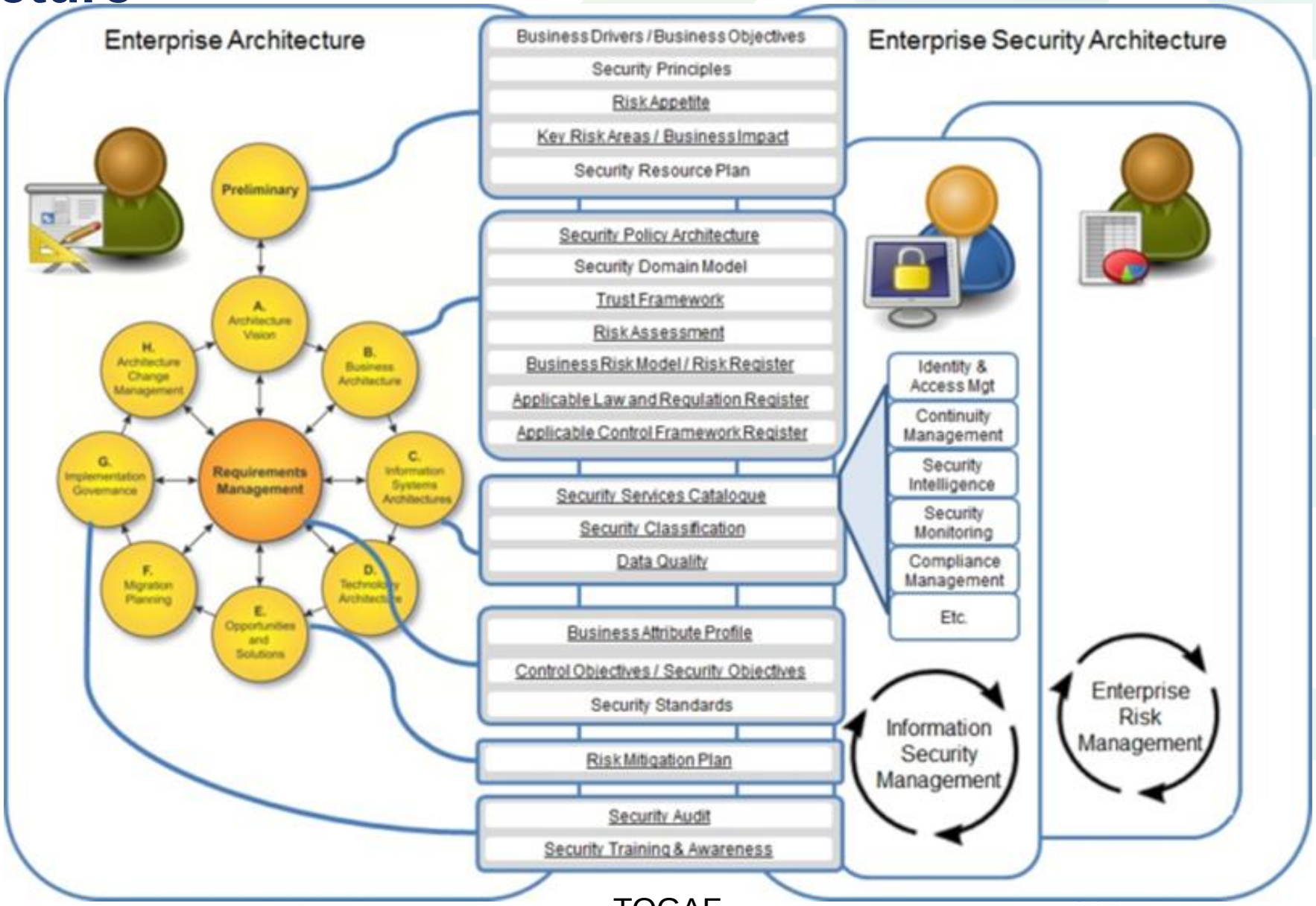


❻

Determine Architecture

An architect needs to **optimize the solution architecture** based upon business needs, operational risk, security and regulatory requirements.

Residual risks (operational, regulatory or security) needs to be **approved by risk owner**.

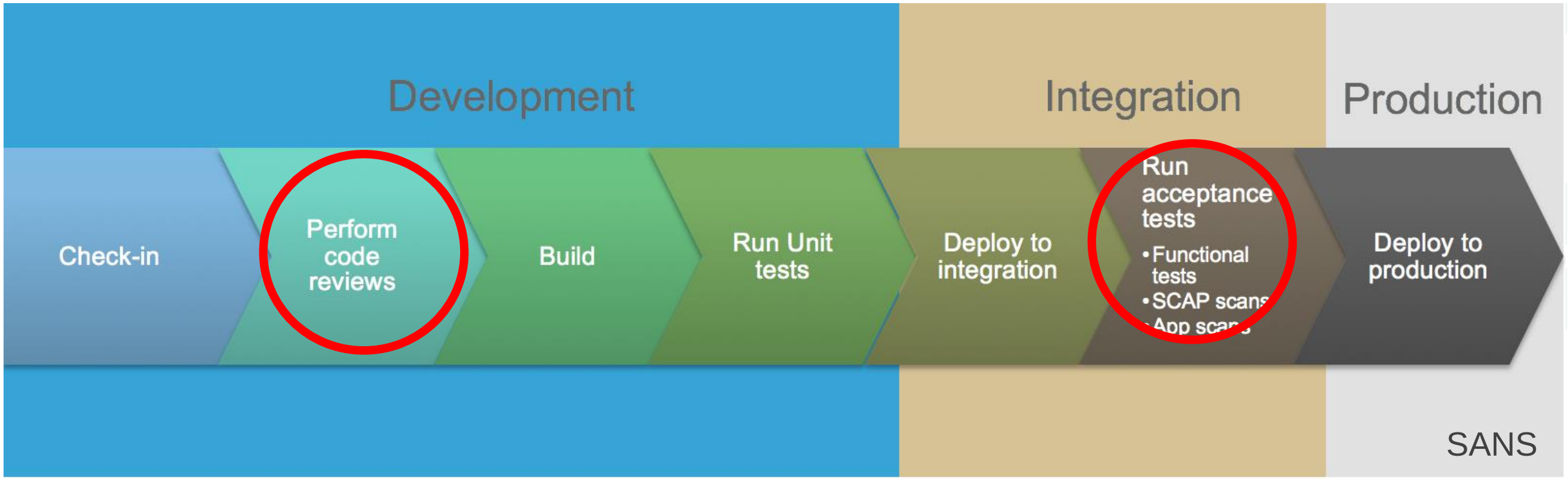


TOGAF

Baking Security into DevOps

- Continuous integration with automation allows better integration with security tools such as secure code review tools
- Configuration management allow secure configuration (e.g. via SCAP Security Control Automation Protocol) to be enforced, including standards on logging, alerting and security metrics.
- Containers allow isolation of applications, particularly in multi-tenant environments. Tools available to scan Docker images.
- CIS Benchmarks available for deploying pre-hardened cloud images such as Docker security benchmark https://github.com/docker/docker-bench-security
- Cloud provider portals and APIs provide independent verification of automated inventory
- Asset tracking and scanning via security providers e.g. Qualys
- Updates to “infrastructure as code” security configuration should trigger automated application scans or SCAP checks.

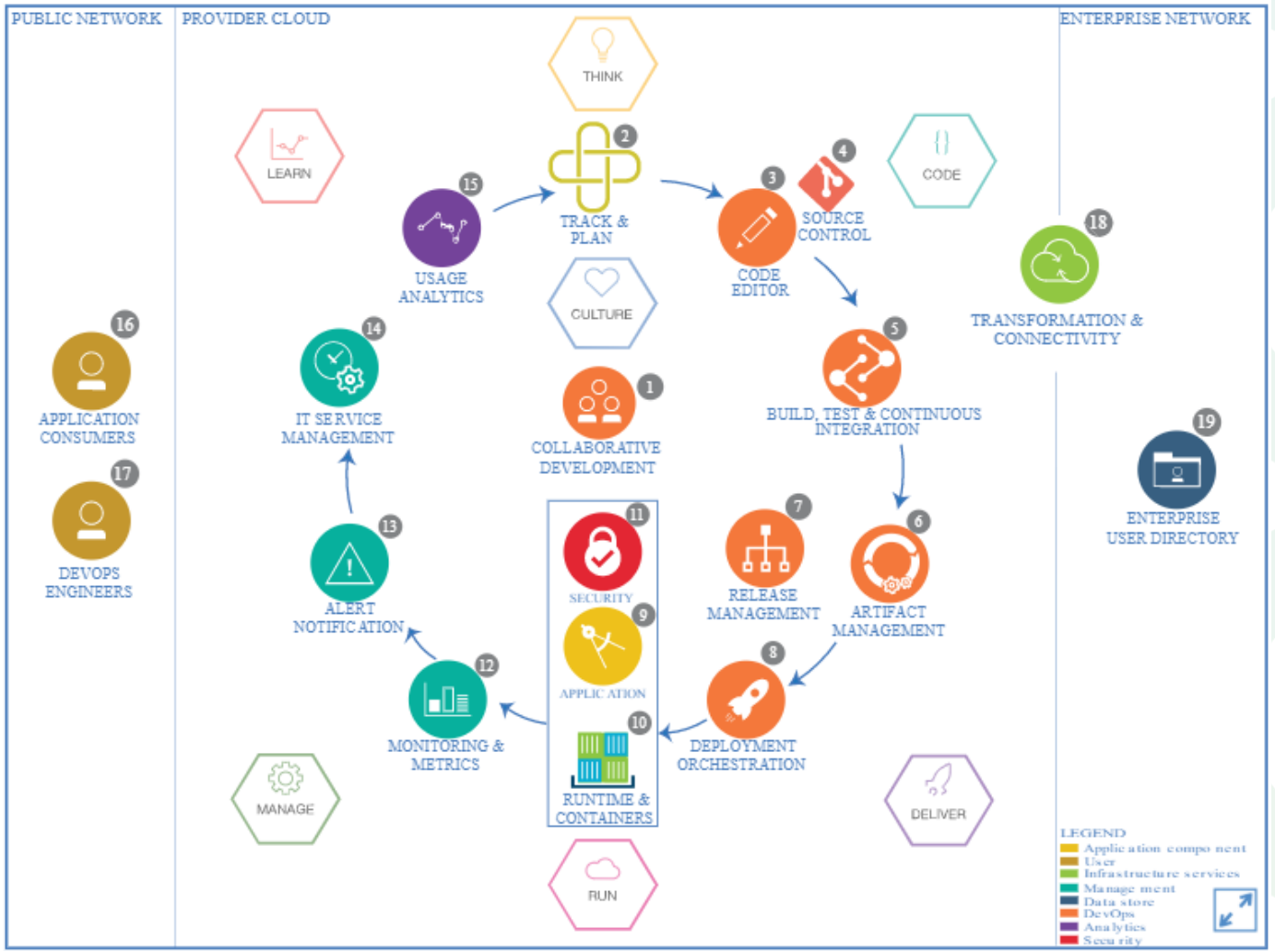
Baking Security into DevOps



Baking Security into DevOps

IBM Reference Architecture for DevOps

- **Deployment strategies**
  - **Blue-Green deployments** or **A-B testing** allows gradual rollout and immediate feedback e.g. scans are part of deployment provide verification.
  - **Variant of this deployment** is to roll out newly patched image files in new VMs by scaling the system up with them and then removing the older, un-patched systems when scaling down.



ISACA Singapore Chapter

What it really means to the DevOps Practitioner

- Not always guaranteed that development, operations or QA personnel will be focused on ensuring compliance with these requirements.
- SAST / DAST require application code to be extant to operate so deployment need to be modified to fit DevOps approach.
- DevOps can mean a fully automated runway to production, results need to be properly are captured and fedback into development processes.
- Segregation of duties and change control can adopt a mostly “detection” form i.e. Developer’s access may be severely restricted and tightly controlled and perhaps change control logs are created and tied to that change so that every adjustment is auditable.

Conclusion – Internalise DevSecOps

Security—Security-relevant configuration changes can be made quicker with use of automated configuration management. the configuration change required to support closing that service could utilize automation features to remediate the issue in the same manner as those made to support new application code.

Assurance—Automated configuration systems often retain a record of when configuration changes are made, by whom and for what purpose. This information might be challenging to gather in an environment that is primarily driven by manual processes. Automated systems can be used to gather evidence about configuration to help streamline the audit process in a way that has reliability advantages over a manual approach. •

Governance—Collecting reliable metrics about processes is often facilitated by using automated approaches. These metrics can support the performance management aspects of governance activities. Likewise, policy enforcement goals can be advanced through the use of technical means to enforce those policies.

http://www.isaca.org/Knowledge-Center/Research/Documents/DevOps-Practitioner-Considerations_whp_Eng_0815.pdf

Where can I find more on DevOps Security and Governance?

- **DevOps Process Maturity By Example**
  http://www.isaca.org/Knowledge-Center/Research/Documents/Devops-Process-Maturity-By-Example_res_eng_1117.pdf

- **DevOps Practitioner Considerations**
  http://www.isaca.org/Knowledge-Center/Research/Documents/DevOps-Practitioner-Considerations_whp_Eng_0815.pdf

- **Continuous Security – Implementing the Critical Controls in a Dev Ops Environment**
  https://www.sans.org/reading-room/whitepapers/critical/paper/36552

ISACA

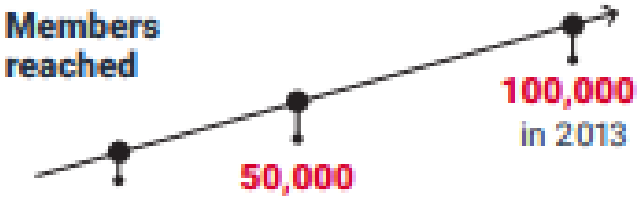
Global Presence

Certifications

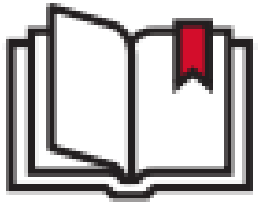
GLOBAL PRESENCE:

2 offices / **220+** chapters worldwide

Members reached



140,000+
members in 188 countries in 2019



97 student groups

CERTIFICATIONS:

ISACA has certified:

146,000+
CISA Professionals

43,000+
CISM Professionals

25,000+
CRISC Professionals

8,000+
CGEIT Professionals

ISACA's core certifications consistently maintain a retention rate of 94–96%.

ISACA SINGAPORE

Local Context

Certifications

~2,500 Members

1,400+ CISA Professionals

~650 CISM Professionals

~400 CRISC Professionals

100+ CGEIT Professionals

ISACA COMMUNITY DAY PEOPLE | SERVICE | PURPOSE **5 Oct**

GTACS 2020

GOVERNANCE · TECHNOLOGY AUDIT · CONTROL · SECURITY

Cyber Resilience to Confidence

Transition to Fully Virtual
28 August 2020

SCAN HERE TO REGISTER

https://www.gtacs.sg

Guest of Honour
Gaurav Keerthi
Assistant Chief Executive
Cyber Security Agency of Singapore

ISACA Member / Supporting Organisations/ Group pricing	$28
Non-Member	$48

Morning Keynotes (0900hr - 1250hr)

0900hr - 0905hr
Opening Address
Phoram Mehta, President, ISACA Singapore Chapter

0905hr - 0915hr
GOH Address
Gaurav Keerthi, Assistant Chief Executive, Cyber Security Agency of Singapore

0915hr - 0930hr
ISACA HQ Address

0935hr - 1000hr
The Route to Data Protection by Design
Koh Suat Hong, Personal Data Protection Commission

1005hr - 1030hr
Keynote 2
TBC

1045hr - 1120hr
Panel: From Cyber Resilience to Confidence
Moderator: Phoram Mehta
Panelists: Koh Suat Hong (PDPC), Lim Thian Chin (CSA), Joe Weiss (ISA99), John Yong (SATA)

1125hr - 1150hr
What can we look for to secure our cyber Future?
Joe Weiss, ISA99

1155hr - 1220hr
Topic Title: TBC
Lim Thian Chin, Cyber Security Agency of Singapore

1225hr - 1250hr
The Singapore Cyber Security Landscape: Learnings from ISACA-Frost & Sullivan Survey 2020
Kenny Yeo, Frost & Sullivan

Afternoon Tracks (1400hr - 1730hr)

Governance & Risk
Track Manager: Gaurav Thorat, OVO

1400hr - 1430hr
Security Governance in Healthcare
John Yong, SATA Commhealth

1435hr - 1505hr
Key Cybersecurity and Risk Trends post-COVID19
Tobias Gondrom, United Overseas Bank

1510hr - 1540hr
Governance & Risk Case Study

1545hr - 1615hr
BCM in Post-COVID19 New Normal
Goh Moh Heng, BCM Institute

1620hr - 1650hr
The Scourge of Data Loss and an Whole-of-Organisation Approach needed
Thomas Kok, OCBC Bank

1655hr - 1730hr
Panel: Governing for Cyber Resilience
Moderator: Gaurav Thorat
Panelists: Goh Moh Heng, Thomas Kok, Tobias Gondrom

Compliance & Audit
Track Manager: Jenny Tan, CapitaLand

1400hr - 1430hr
How to effectively audit your Active Directory against APTs
Paige Sundquist, FedEx, Memphis Chapter

1435hr - 1505hr
Digitalisation vs Transformation: Why you need to take your time for it
Jenny Tan, CapitaLand

1510hr - 1540hr
Compliance & Audit Case Study

1545hr - 1615hr
Effective Auditing for ICS/SCADA Systems
Daniel Ehrenreich, 5th ICS Cybersec 2020, Israel

1620hr - 1650hr
Ensuring Compliance for Automation Security
Ulrich Seldeslachts, EU LSEC Leaders in Security

1655hr - 1730hr
Panel: Auditing for Cyber Resilience
Moderator: Jenny Tan
Panelists: TBC

Design & Architecture
Track Manager: Steven Sim, Singapore Chapter

1400hr - 1430hr
Securing Critical Infrastructure in the New Normal
Lim Shih Hsien, SP Group

1435hr - 1505hr
Understanding Cybersecurity Risk in the age of serverless
Ian Loe, NTUC Enterprise

1510hr - 1540hr
Design & Architecture Case Study

1545hr - 1615hr
Effectively applying MITRE ATT&CK Framework on ICS
Freddy Dezeure, EU MITRE ATT&CK User Group

1620hr - 1650hr
Designing an effective OT Cyber Incident Plan
Oren Elimelech, Cyber 360, Israel Chapter

1655hr - 1730hr
Panel: Architecting for Cyber Resilience
Moderator: Steven Sim
Panelists: Freddy Dezeure, Ian Loe, Lim Shih Hsien, Oren Elimelech

Security Planning & Program
Track Manager: Yap Lip Keong, Avaloq

1400hr - 1430hr
Debunking myth about red teaming - A tale spoken by a red-teamer
Chong Rong Hwa, Government Technology Agency

1435hr - 1505hr
Planning a successful Bug Bounty Program
Ang Leong Boon, National University of Singapore

1510hr - 1540hr
Security Planning & Program Case Study

1545hr - 1615hr
Planning a secure migration to Cloud
Zhuang Hao Jie, Cloud Security Alliance

1620hr - 1650hr
Planning for GDPR in Cloud Security
Egide Nzabonimana, SOCRAI, Belgium Chapter

1655hr - 1730hr
Panel: Planning for Cyber Resilience
Moderator: Yap Lip Keong
Panelists: Ang Leong Boon, Chong Rong Hwa, Egide Nzabonimana, Zhuang Hao Jie

ISACA
Singapore Chapter

Only way to keep up with rising threats is

to keep finding weaknesses in our own ideas

ISACA Singapore Chapter

ISACA®

Singapore Chapter