ISACA®
Trust in, and value from, information systems

Garry Barnes
Vice President, **ISACA**
Practice Lead, Governance Advisory, **Vital Interacts**

CYBERSECURITY ASSURANCE: CHALLENGES & OPPORTUNITIES

December 2014

BACKGROUND

ISACA:

International Vice President

Treasurer, Finance Committee

Strategic Advisory Council

Credentialing and Career Management Board

CISM Certification Committee (Chair) and TES

Oceania CACS Committees (2003, 2008, 2015)

Sydney Chapter 2003-2012 (President 2008-10)

Security, Governance, Risk and Audit:

Practice Lead, Governance Advisory, Vital Interacts

Managing Consultant, BAE Systems

Risk Manager & Information Security Consultant, Commonwealth Bank of Australia

Information Security Manager & IT Audit Manager, NSW Departments of Education & Commerce

CISA CISM CGEIT CRISC MAICD

ISACA

CISA | CISM
CGEIT | CRISC

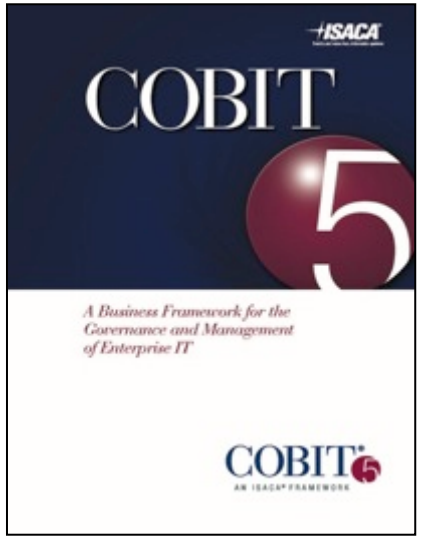
“Trust in, and value from, information systems”

Global association serving 115,000 IT security, assurance, governance and risk professionals

Established in 1969

200+ chapters in 80 countries

Members in 180 countries



CSX™
CYBERSECURITY NEXUS

ISACA®
Trust in, and value from, information systems

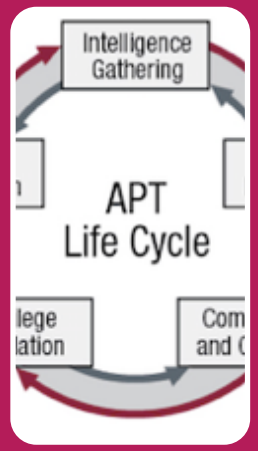
CHANGE IS CONSTANT

ISACA®
Trust in, and value from, information systems

KEY TRENDS AND DRIVERS OF CYBERSECURITY

IT-enabled transformation

- Cloud services
- Demand-based services
- Internet of Things
- Big Data

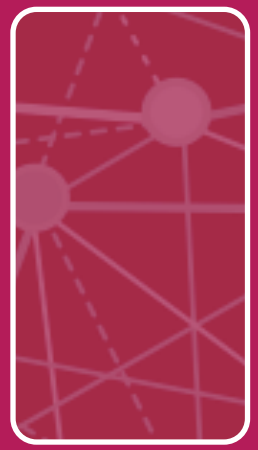


Emerging Threats

- Sophisticated cyber-attacks tools
- Targeted attacks
- Supply chain attacks
- Advanced persistent threats (APTs)

Consumerization

- Mobile devices
- Social media
- Home automation
- Wearables
- Intelligent devices



Regulatory and Compliance Pressures

- Industry-specific: PCI
- Regional: SOX, Privacy
- Standards-based Certification
- Supply chain assurance

TECHNOLOGY TRANSFORMING SERVICES AND BUSINESS

Education

- Connected classrooms
- Remote learning
- Online learning (MOOCs, …)

Health

- E-health records
- Telemedicine (remote medicine)
- Informatics
- mHealth
- Patient and inventory monitoring

Retail and Banking

- On-line & mobile banking
- Shopping & procurement
- Inventory management

Transportation

- Rolling stock management
- E-ticketing
- Service notification

Utilities

- Power generation
- Telecomms

Emergency Services

- Warning systems and sensors
- GIS & hazard mapping
- Response systems
- Disaster management

Farming

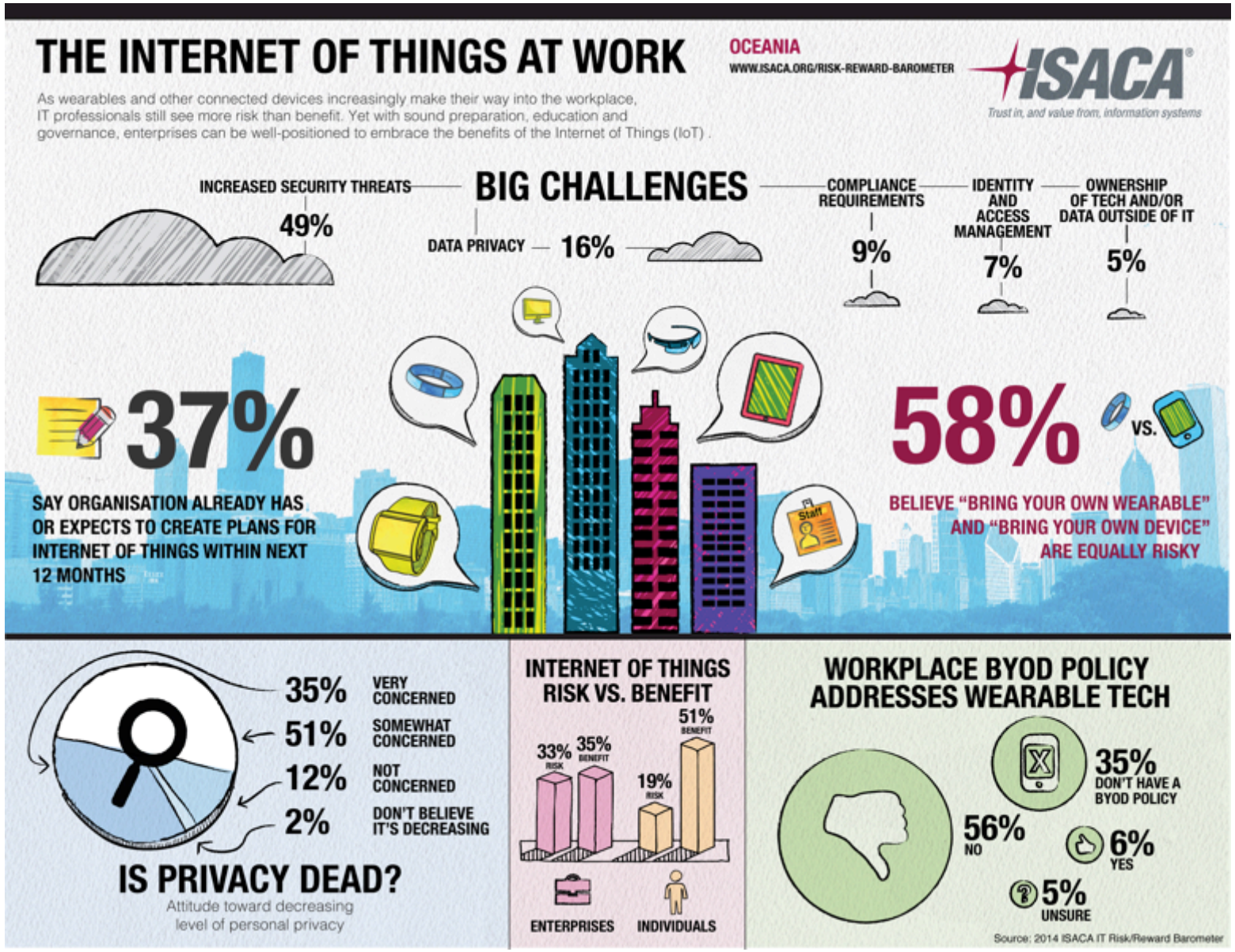
- Livestock tracking
- Equipment monitoring

Etc…….

TECHNOLOGY TRANSFORMING RETAIL IN NEW MARKETS

www.geek.com

EMERGING IMPACT OF THE INTERNET OF THINGS

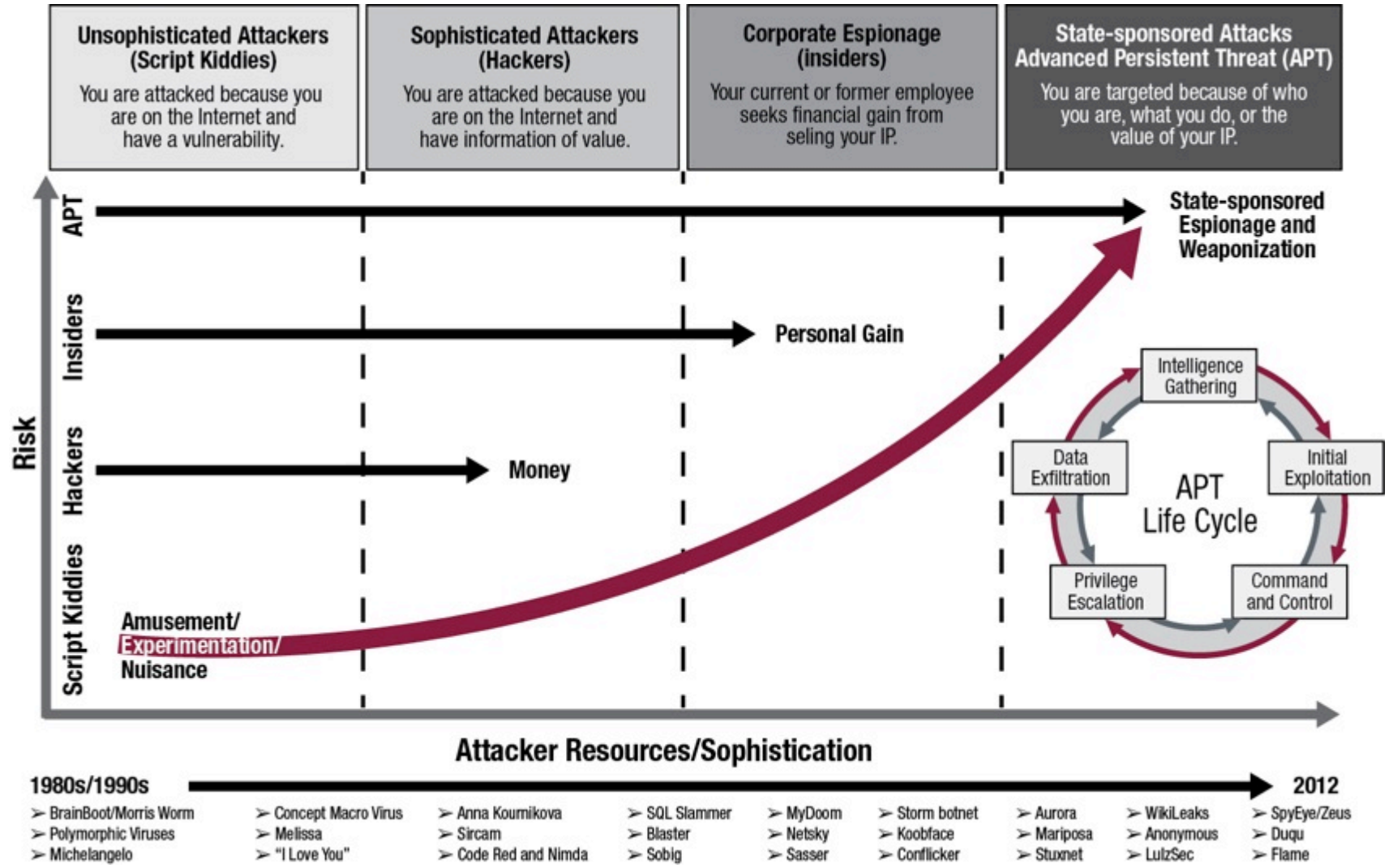


ISACA
Trust in, and value from, information systems

CYBER THREATS

ISACA®
Trust in, and value from, information systems

THE WORLD IS CHANGING



ISACA®
Trust in, and value from, information systems

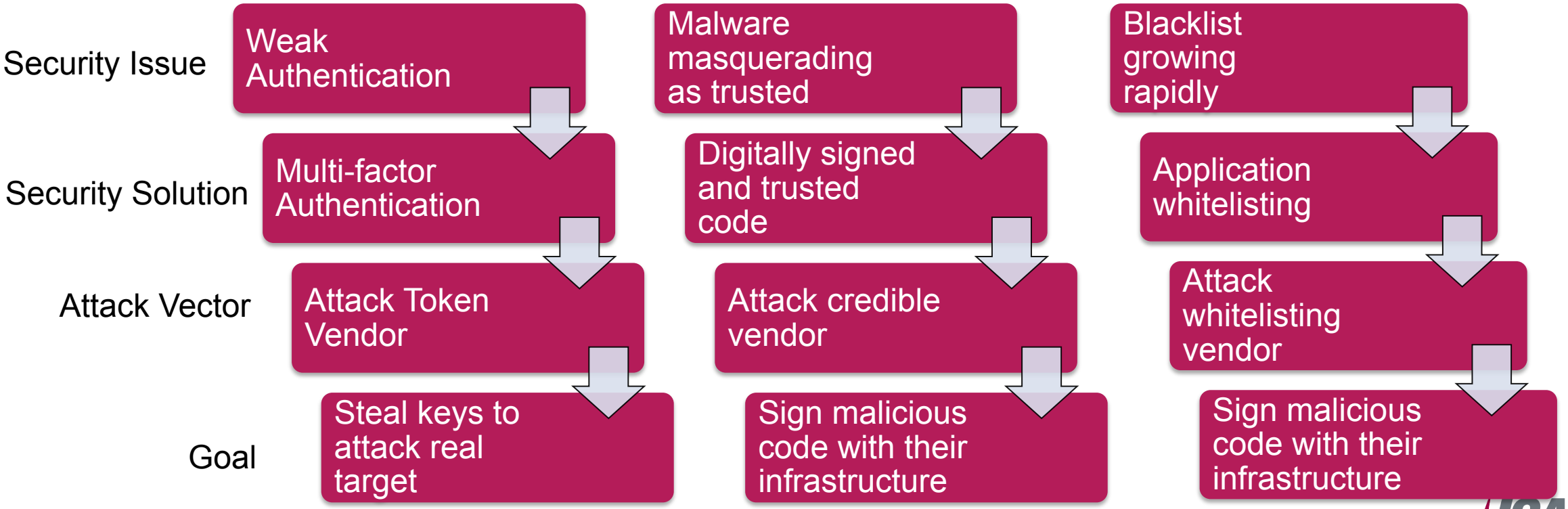
THE WORLD IS CHANGING

The 2010 Google Aurora attack forever changed the way we look at Internet security. This large-scale, sophisticated attack showed us that all sectors, from private to public, are vulnerable to a new class of security breach.

The Advanced Persistent Threat

ADAPTIVE ATTACK VECTORS

The threat landscape evolves as attackers adapt new and innovative attack methods while defenders deploy new defense strategies.



GLOBAL COST $USD3 TRILLION

Hacker claims passenger jets at risk of cyber attack

By Jim Finkle, Reuters

SHARELINES

AUGUST 4, 2014,

ECB hacked: Data stolen from central bank

Matt Clinch | @mattclinch81
Thursday, 24 Jul 2014 | 5:25 AM ET

CNBC

Email addresses and other contact information stored at the Europe**a**n **Central Bank (ECB)** have been stolen, the organization confirmed o**n** Thursday.

Security that protects a database serving its public website has been breached, it said in a statement published on its website, meaning users registering for information on conferences and visits at the ECB have been

Home / USA /

US utility's control systems hit by advanced cyber attack - DHS

Published time: May 21, 2014 03:12 Get short URL

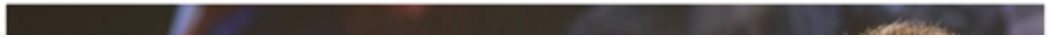
BBC News Sport Weather Earth Future Shop

NEWS TECHNOLOGY

Home World Asia Australia India China UK Business Health Science/Environment Technology

25 November 2014 Last updated at 08:34 Share

Sony Pictures computer system hacked in online attack



ISACA Trust in, and value from, information systems

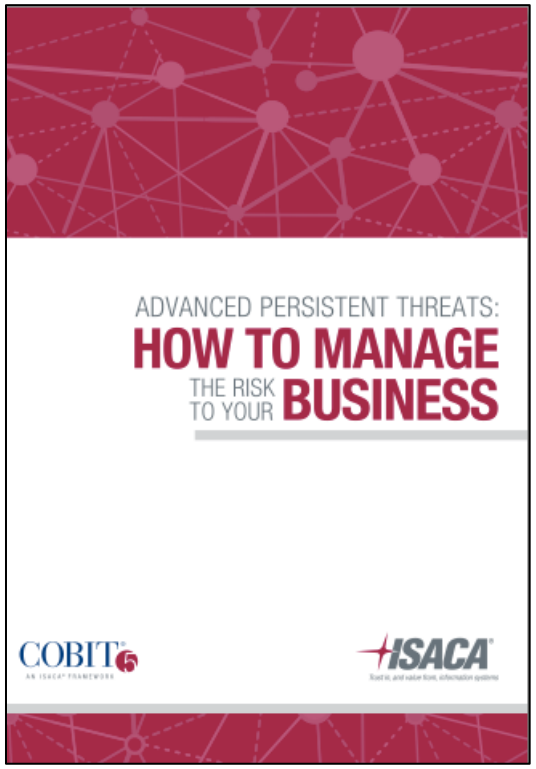
RESPONDING TO APT'S

ISACA guidance covering:

- Understanding the threat
- Managing the APT risk
- Responding to attacks

Understand

Manage

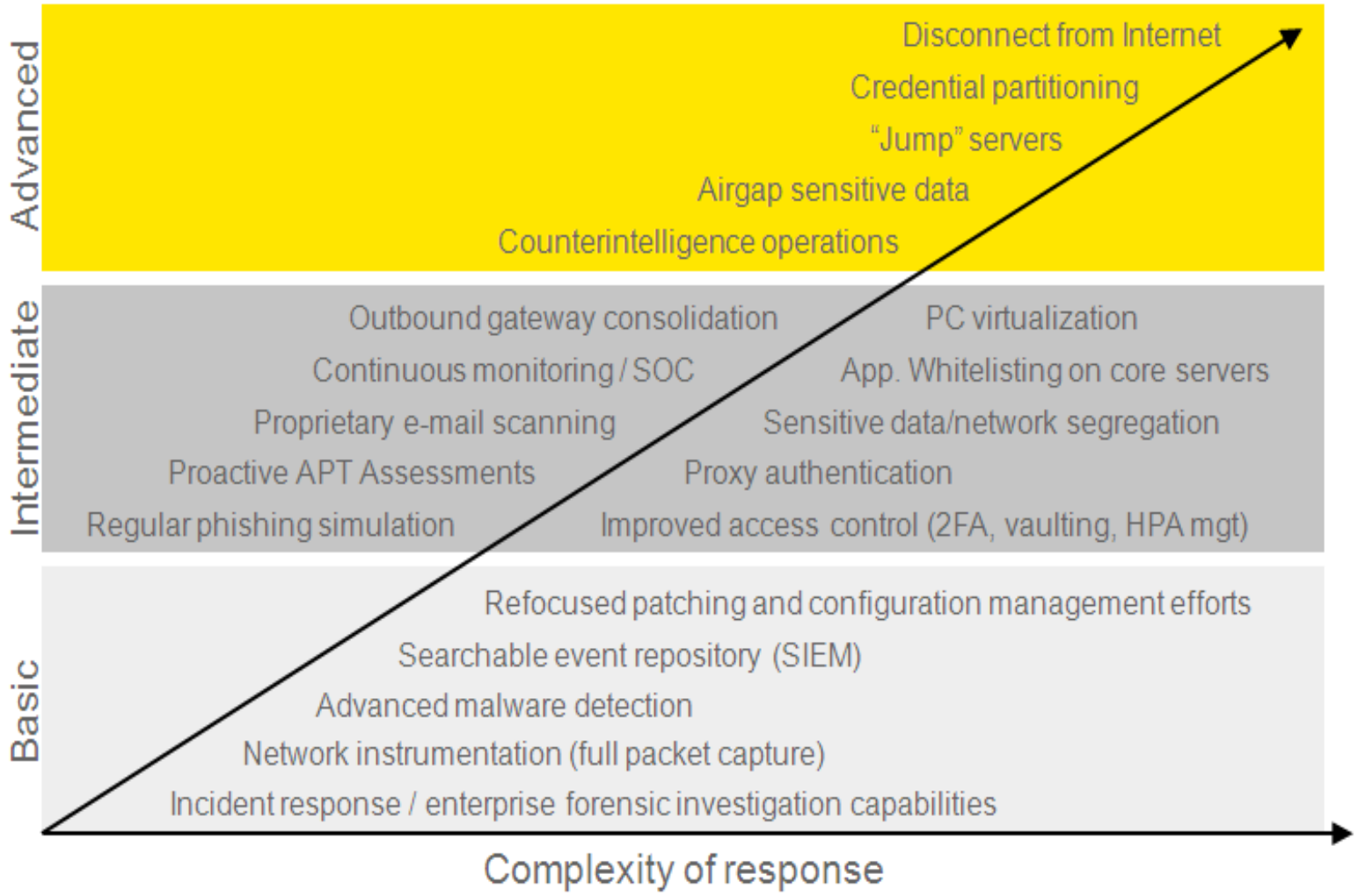


Respond

ISACA
Trust in, and value from, information systems

METHODS FOR DEFENDING AGAINST THE APT

Many enterprises implement some of the intermediate-level concepts. Because the APT and other advanced, sophisticated attackers have such a high success rate, it is recommended that every enterprise implement all of the basic concepts.



CYBER SECURITY ASSURANCE

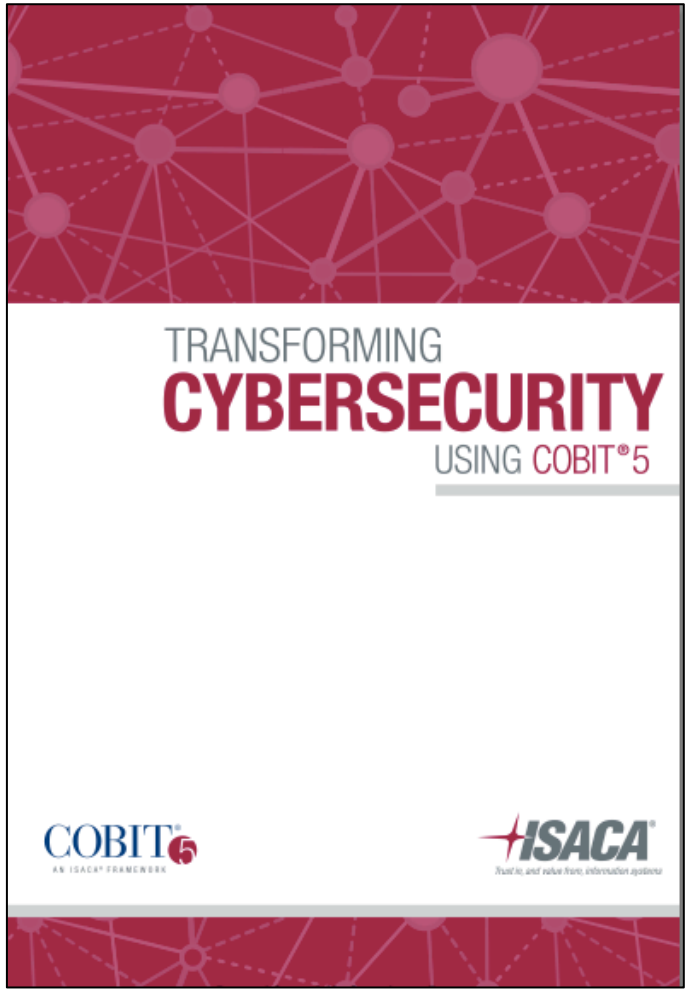
BE MORE

ISACA®
Trust in, and value from, information systems

CYBERSECURITY – EXAMPLE KEY RISKS

1. **Business dependency on technology** (resilience and recoverability)
2. **Proliferation of devices** (laptops, tablets, BYOD, smart devices)
3. **Cloud computing** (access, data sovereignty, service recovery)
4. **Supply chain** (entry points, people, vulnerable systems)
5. **Incident response** (detection and response capability including disaster recovery and business continuity)

TRADITIONAL RESPONSE STRATEGIES ARE NOT ENOUGH!



Transforming Cybersecurity using COBIT 5

Understand the impact of cybercrime and warfare on your enterprise.

Understand the business case and risk appetite of the enterprise.

Establish cybersecurity governance from top down.

Manage cybersecurity using COBIT5 principles and enablers.

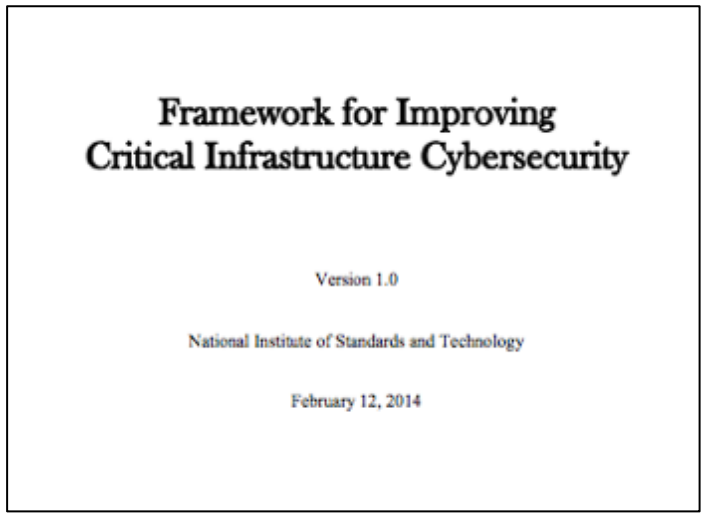
Establish cybersecurity assurance (monitoring, internal reviews, audits and, as needed, investigative and forensic analysis.)

Understand end users, their security skills and behaviors.

Establish and evolve systemic cybersecurity.

ISACA
Trust in, and value from, information systems

NIST CYBERSECURITY FRAMEWORK


Framework for Improving
Critical Infrastructure Cybersecurity

Version 1.0

National Institute of Standards and Technology

February 12, 2014

Implementing the NIST Cybersecurity Framework

Step 1: Prioritize and Scope

Step 2: Orient

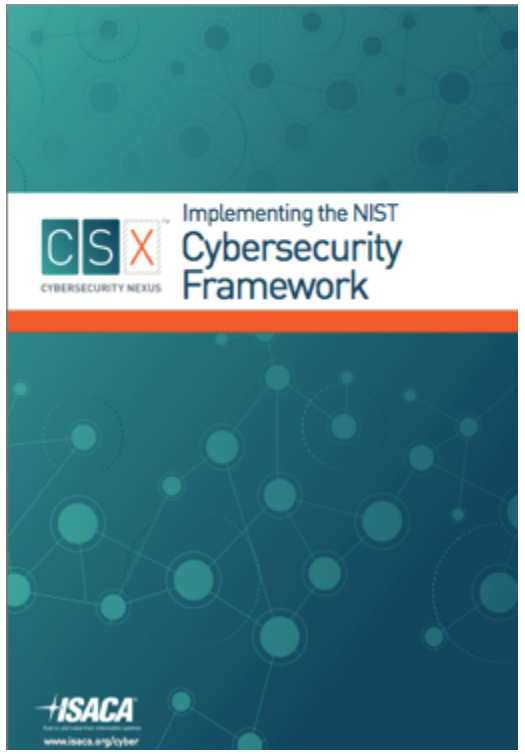
Step 3: Create a Current Profile

Step 4: Conduct a Risk Assessment

Step 5: Create a Target Profile

Step 6: Determine, Analyze, and Prioritize Gaps

Step 7: Implement Action Plan



ISACA
Trust in, and value from, information systems

CYBERSECURITY ASSURANCE PROGRAM COMPONENTS

1. Governance

- Board, Executive and/or Audit and Risk Committee discussions
  - Impact of cybersecurity and related attacks on your organisation and its supply chain
  - Appropriateness of current responses
  - Current state of monitoring and reporting
- Risk function, threat intelligence and risk reporting
  - Directing and monitoring the development of cybersecurity strategies
  - Oversight based of the risk function
  - Consideration of threat and risk information
- Supply chain relationship management
  - Engaging with the business cyber eco-system
  - Evaluating supply chain assurance reports

CYBERSECURITY AND THE BOARD

https://na.theiia.org

Board Oversight – www.nacdonline.org

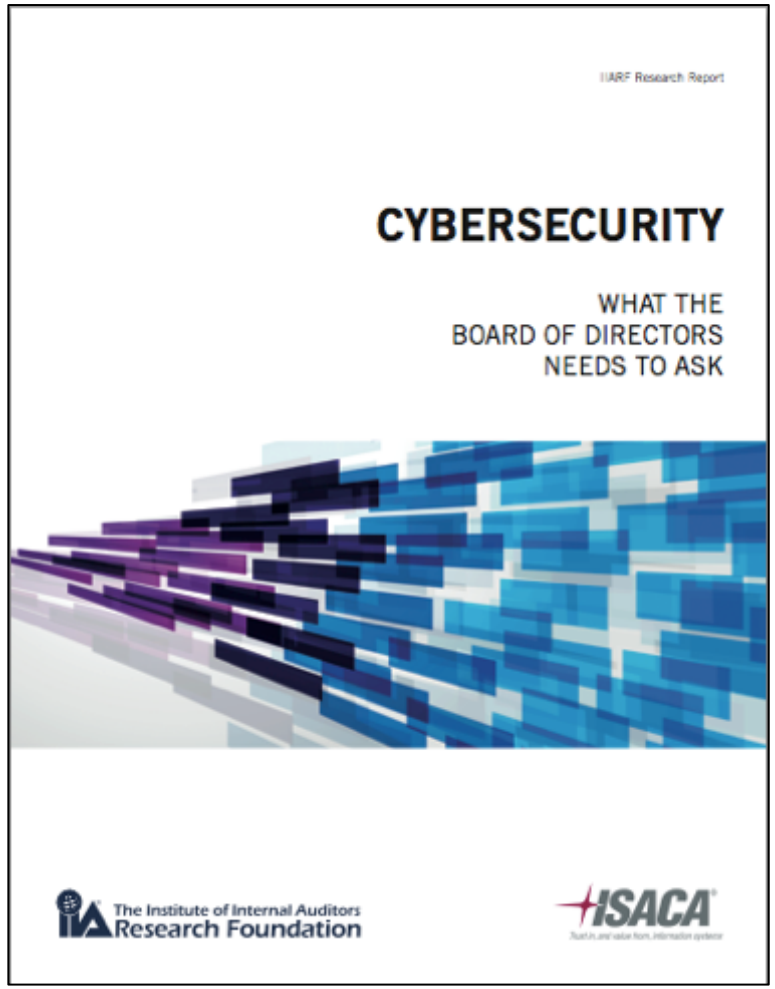
NACD Principle 1: Directors need to understand and approach cybersecurity as an enterprise-wide risk management issue, not just an IT issue.

NACD Principle 2: Directors should understand the legal implications of cyber risks as they relate to their company's specific circumstances.

NACD Principle 3: Boards should have adequate access to cybersecurity expertise, and discussions about cyber-risk management should be given regular and adequate time on the board meeting agenda.

NACD Principle 4: Directors should set the expectation that management will establish an enterprise-wide risk management framework with adequate staffing and budget.

NACD Principle 5: Board-management discussion of cyber risk should include identification of which risks to avoid, accept, mitigate, or transfer through insurance, as well as specific plans associated with each approach.

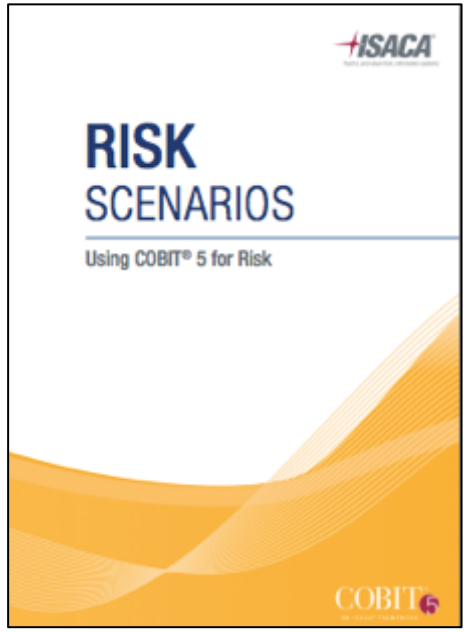


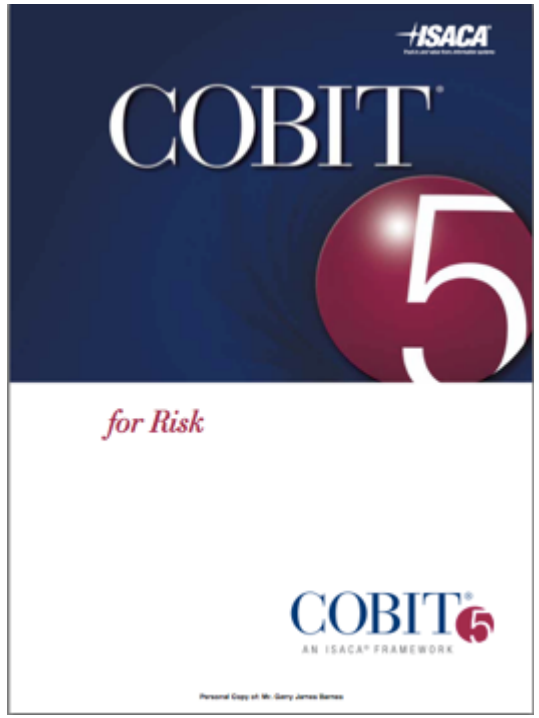
ISACA
Trust in, and value from, information systems

CYBERSECURITY ASSURANCE PROGRAM COMPONENTS

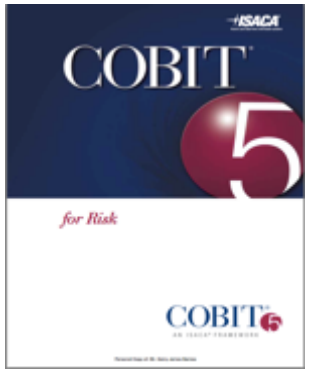
2. Risk Management

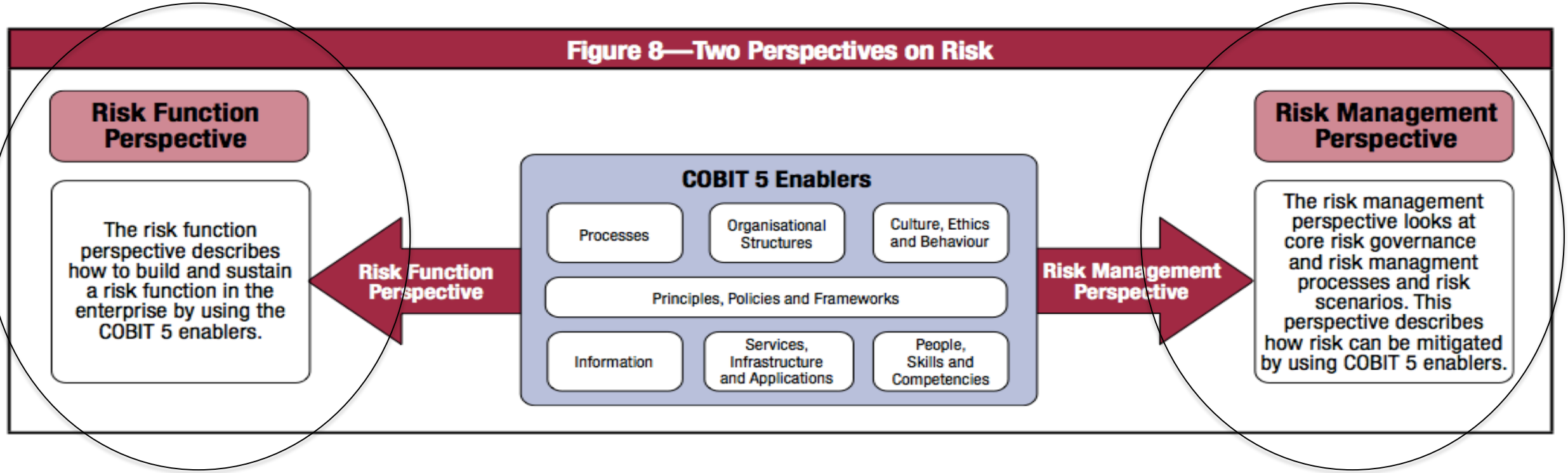
- Risk Function and Risk Management perspectives
- Risk profile, appetite, tolerance, metrics and reporting
- Risk assessment – scope, approach, scenarios, criteria, measurement
- Risk response – appropriateness, monitoring
- Risk reporting and analytics





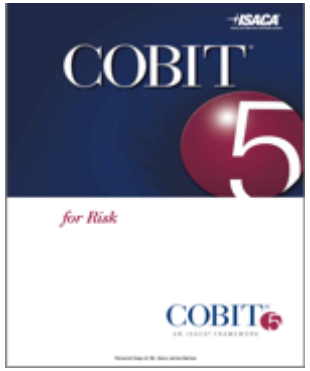
ADDRESSING TWO PERSPECTIVES ON RISK





ISACA
Trust in, and value from, information systems

RISK FUNCTION CAPABILITIES



Risk accountability

Risk methodology

Risk governance e.g. 3LoD

Risk Function Perspective

The risk function perspective describes how to build and sustain a risk function in the enterprise by using the COBIT 5 enablers.

Risk Function Perspective

COBIT 5 Enablers

- Processes
- Organisational Structures
- Culture, Ethics and Behaviour
- Principles, Policies and Frameworks
- Information
- Services, Infrastructure and Applications
- People, Skills and Competencies

Risk culture & behaviours

Risk principles, policy

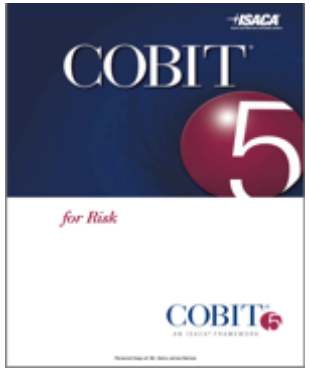
Risk criteria

Risk intelligence

Risk systems

Risk training

RISK MANAGEMENT CAPABILITIES



Risk methodology

Risk planning

Risk capacity

Risk governance

Risk indicators

COBIT 5 Enablers

- Processes
- Organisational Structures
- Culture, Ethics and Behaviour
- Principles, Policies and Frameworks
- Information
- Services, Infrastructure and Applications
- People, Skills and Competencies

Risk Management Perspective

Risk Management Perspective

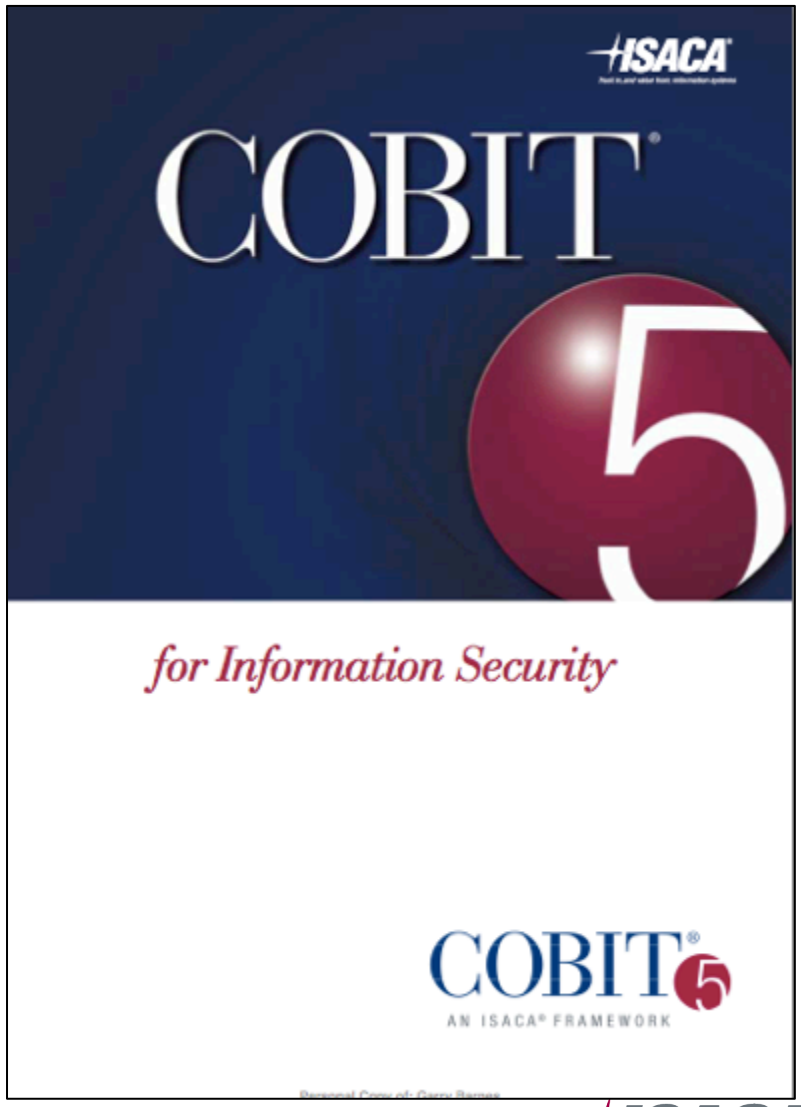
The risk management perspective looks at core risk governance and risk managment processes and risk scenarios. This perspective describes how risk can be mitigated by using COBIT 5 enablers.

Risk monitoring

CYBERSECURITY ASSURANCE PROGRAM COMPONENTS

3. Security Management

- Information Security Management System (ISO 27001)
- Security risk assessments
- Threat intelligence and analytics
- Policy framework, compliance and exception management
- Supply chain security assessments and reporting
- Awareness, culture and training
- Security metrics and reporting systems

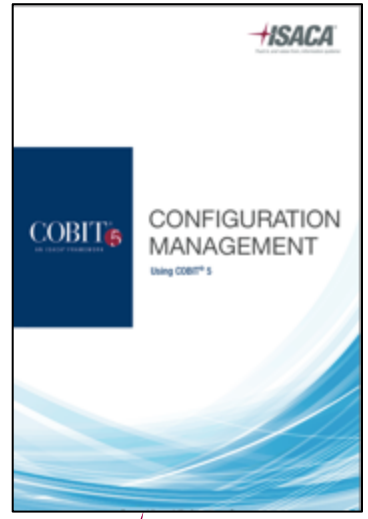


ISACA
Trust in, and value from, information systems

CYBERSECURITY ASSURANCE PROGRAM COMPONENTS

4. Security Operations

- Security service management
- Security architecture review
- Mobile device security
- Cloud management and compliance
- Configuration management
- Penetration testing and network security assessment
- Incident management, DR and BCP and communication to external bodies (PacCERT)



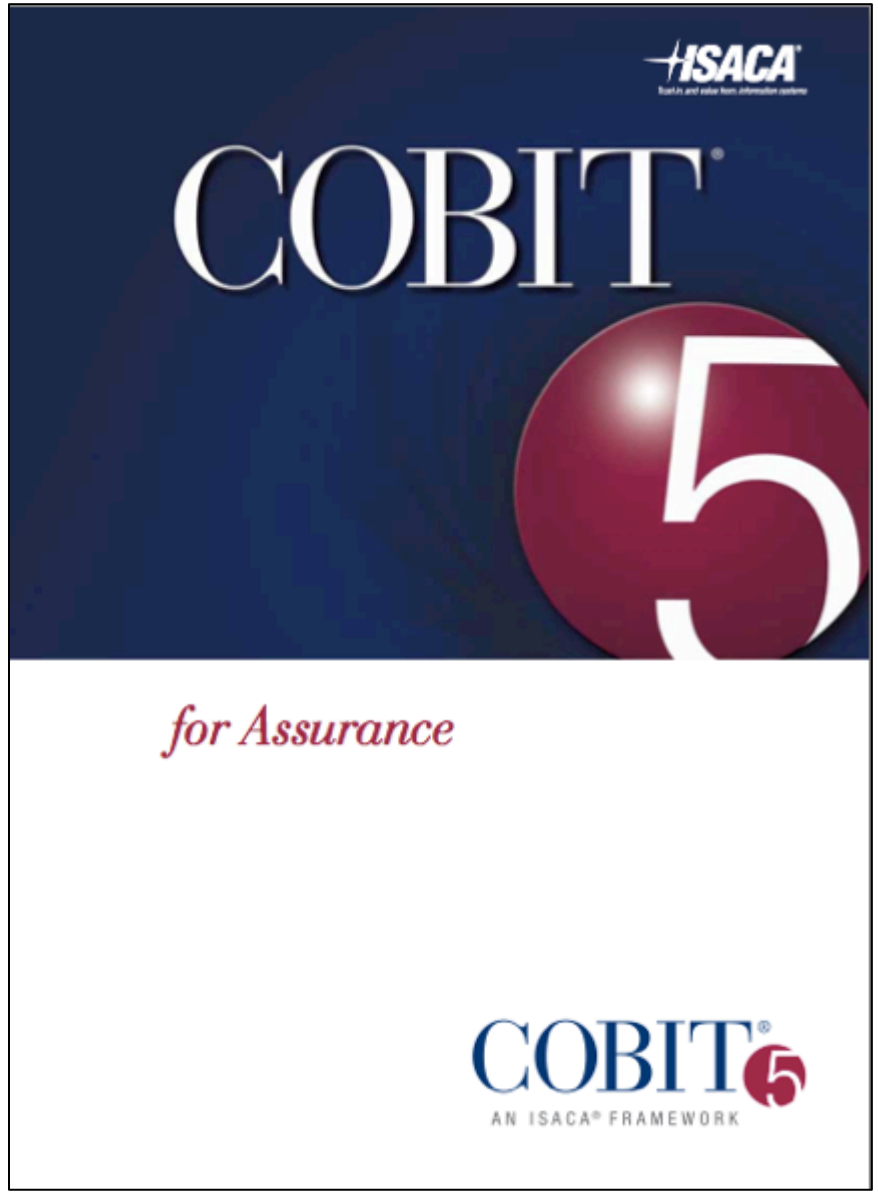
ISACA
Trust in, and value from, information systems

COBIT 5 FOR ASSURANCE

COBIT 5 for Assurance—much like COBIT 5 itself—is an umbrella approach for the provisioning of assurance.

The list of standards considered includes:

- ISACA ITAF, 2nd Edition, a professional practices framework for IS audit/assurance
- The Institute of Internal Auditors (IIA) International Professional Practices Framework (IPPF) Standards 2013
- American Institute of Certified Public Accountants (AICPA) Statement on Standards for Attestation Engagements (SSAE) 16



ISACA®
Trust in, and value from, information systems

COBIT 5-BASED ASSURANCE GUIDES

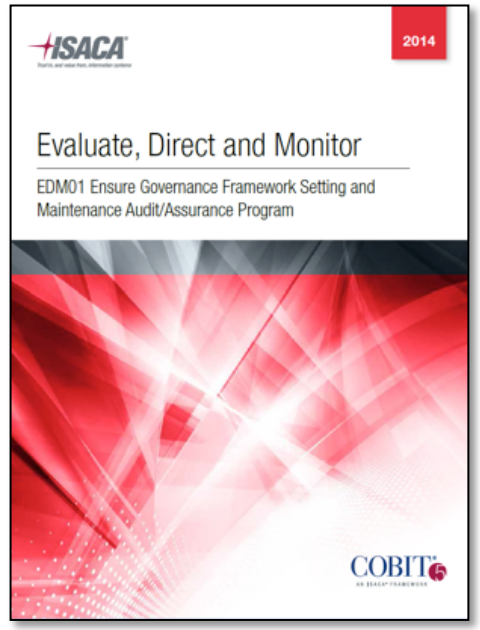
Aligned with generally accepted auditing standards and practices

Three phases:

- Phase A: Determine scope
- Phase B: Understand enablers, set assessment criteria and perform the assessment
- Phase C: Communicate and report the results

Audit / Assurance program guides cover:

- Evaluate, Direct and Monitor
- Align, Plan and Organise
- Build, Acquire and Implement
- Deliver, Service and Support (Available December 2014)



http://www.isaca.org/Knowledge-Center/Research/Pages/Audit-Assurance-Programs.aspx

ISACA
Trust in, and value from, information systems

COBIT 5 FOR ASSURANCE

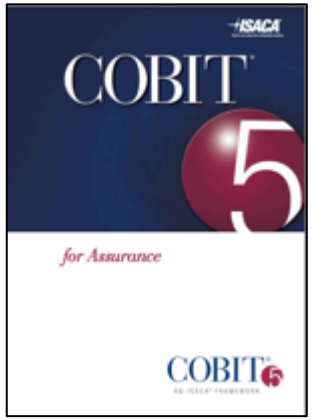


Figure 16—COBIT 5 Process Reference Model

Processes for Governance of Enterprise IT

Evaluate, Direct and Monitor

- **EDM01** Ensure Governance Framework Setting and Maintenance
- **EDM02** Ensure Benefits Delivery
- **EDM03** Ensure Risk Optimisation
- **EDM04** Ensure Resource Optimisation
- **EDM05** Ensure Stakeholder Transparency

Align, Plan and Organise

- **APO01** Manage the IT Management Framework
- **APO02** Manage Strategy
- **APO03** Manage Enterprise Architecture
- **APO04** Manage Innovation
- **APO05** Manage Portfolio
- **APO06** Manage Budget and Costs
- **APO07** Manage Human Resources
- **APO08** Manage Relationships
- **APO09** Manage Service Agreements
- **APO10** Manage Suppliers
- **APO11** Manage Quality
- **APO12** Manage Risk
- **APO13** Manage Security

Build, Acquire and Implement

- **BAI01** Manage Programmes and Projects
- **BAI02** Manage Requirements Definition
- **BAI03** Manage Solutions Identification and Build
- **BAI04** Manage Availability and Capacity
- **BAI05** Manage Organisational Change Enablement
- **BAI06** Manage Changes
- **BAI07** Manage Change Acceptance and Transitioning
- **BAI08** Manage Knowledge
- **BAI09** Manage Assets
- **BAI10** Manage Configuration

Deliver, Service and Support

- **DSS01** Manage Operations
- **DSS02** Manage Service Requests and Incidents
- **DSS03** Manage Problems
- **DSS04** Manage Continuity
- **DSS05** Manage Security Services
- **DSS06** Manage Business Process Controls

Monitor, Evaluate and Assess

- **MEA01** Monitor, Evaluate and Assess Performance and Conformance
- **MEA02** Monitor, Evaluate and Assess the System of Internal Control
- **MEA03** Monitor, Evaluate and Assess Compliance With External Requirements

Processes for Management of Enterprise IT

CYBERSECURITY SKILLS

ISACA®
Trust in, and value from, information systems

CSX ELEMENTS: CREDENTIALING

0-3 years:

- Cybersecurity Fundamentals Certificate

3-5 years:

- Cybersecurity practitioner-level certification
  - coming in mid- 2015

5+ years:

- Certified Information Security Manager certification
- 25,000+ professionals certified

CYBERSECURITY FUNDAMENTALS KNOWLEDGE CERTIFICATE

- Knowledge-based exam for those with 0 to 3 years experience

- Foundational level covers four domains:
  1) Cybersecurity architecture principles
  2) Security of networks, systems, applications and data
  3) Incident response
  4) Security implications related to adoption of emerging technologies

The exam is offered online and at select ISACA conferences and training events. The first was in September at EuroCACS.

ISACA
Trust in, and value from, information systems

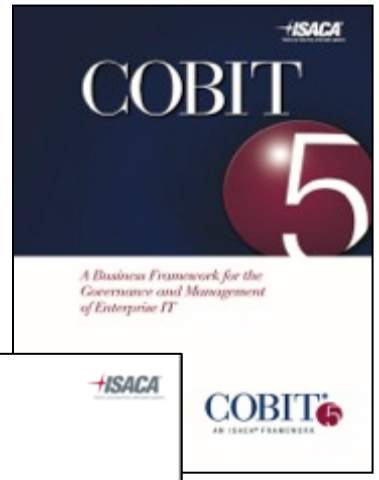
CSX ELEMENTS

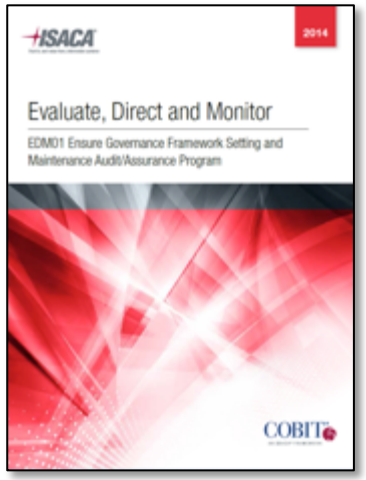
- Cybersecurity webinars:
  - Self-Defense Strategies to Thwart Cloud Intruders: Keep Your Data Safe in the Cloud
  - Why Implement the NICE Cybersecurity Workforce Framework?
  - Countering Cyber Insecurity with Strategic Planning
  - Cybersecurity Diagnosis in Industrial Environments
- Virtual and CACS/ISRM conferences
- Cybersecurity Knowledge Center community
- Implementing the NIST Cybersecurity Framework
  - Guidance and training (new)
- European Union Cybersecurity Strategy
- COBIT 5 Assessor for Security (new)

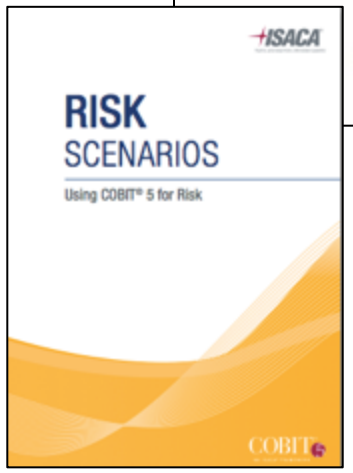
CSX™ CYBERSECURITY NEXUS

CYBERSECURITY ASSURANCE: CHALLENGES & OPPORTUNITIES

CSX™
CYBERSECURITY NEXUS







CISM® Certified Information Security Manager®
An ISACA® Certification

www.isaca.org/cyber

ISACA®
Trust in, and value from, information systems

QUESTIONS?

ISACA®
Trust in, and value from, information systems