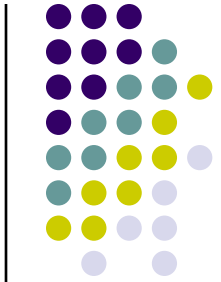
Microsoft© Information Security - Cloud & Mobile

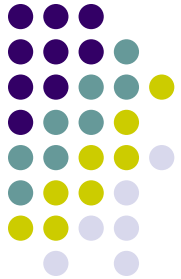
Presented by

Vijay Mohire



Introduction

Information Security and Risk Management (IS&RM)

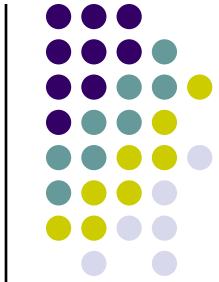


- Microsoft's Information Security (**InfoSec**) organization
- Responsible for information security risk management
- Information protection, enterprise **business continuity** planning
- Accelerate **secure and reliable business** for Microsoft, partners and customers
- Publisher of **The Security Risk Management Guide**

ACE team

- The ACE (Assessment, Consulting & Engineering) team is the **assessment arm** of Microsoft's Information Security & Risk Mgmt. (IS&RM) organization
- Provides **security assessment** services to both Microsoft and Microsoft's enterprise + public sector customers
- Shares and **showcases** with external customers how Microsoft manages risks
- **Learns** and brings back **best practices** from Microsoft's customers

My planned contributions to ACE



Assessments

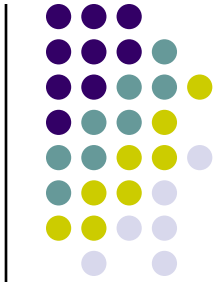
- **Risk assessments** – Threat modeling, business impact analysis, threat to vulnerability pairing, qualitative/ quantitative analysis, STREAD, DREAD

- **Compliance checks-** ISO, HIPAA, PCI

- **Due diligence** – Security gap analysis, Future state model design, constraints assessments

- **Strategy** - Assess the capability, maturity and roadmaps for investments in Info Sec, business continuity , migration to cloud

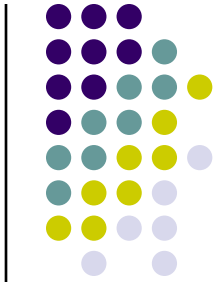
My planned contributions to ACE



Consultation

- Assist clients in **achieving their goals** in areas of cloud and mobile security
- Provide **advice** on use of **Microsoft's security tools**, SDL based development methodology
- Assist clients' in leveraging security **frameworks**
- **Educate** in effective use of security best practices
- Help companies in developing & establishing **security practice**, programs, RFP/ RFI

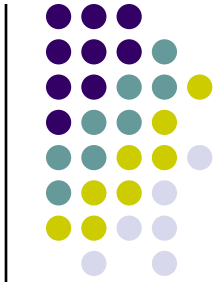
My planned contributions to ACE



Engineering

- Manage installation, instrumentation of data center **components** where security is in scope
-
- Manage security features in **electrical cabling**, power units, physical security devices, storage areas
- Triage and delegate **security issues**, related to engineering systems, motherboards

My planned contributions to ACE



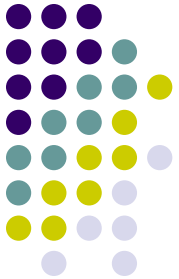
Program Management

- Plan, design, develop strategies for innovative security features for "**mobile-first, cloud-first**" environment

- Delegate, monitor project activities based on program needs and client feedbacks

- Manage **red / blue teams** related to penetration testing / ethical hackers

- Work on internal training programs and mentor juniors in achieving **capabilities** in Info Sec



Info-Sec basics

Risk

What is risk ?

- Risk is a function of the likelihood of a given **threat**-source's exercising a particular potential **vulnerability**, and the resulting **impact** of that adverse event on the organization/**asset**

Threat-sources

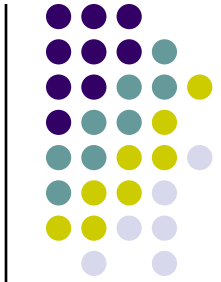
- Accidental / intentional disclosure
- Alteration of licensed IT components
- System Configuration errors
- Network errors
- Equipment malfunction
- Natural disaster
- War

Vulnerability

- A **flaw** or **weakness** in system security procedures, design, implementation, or internal controls

- This could be exercised (accidentally triggered or intentionally exploited) and result in a **security breach** or a violation of the system's security policy

Risk assessment

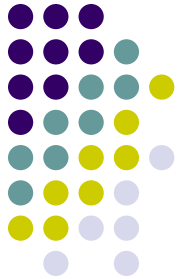


- Risk is assessed by **identifying** threats and vulnerabilities, then determining the **likelihood** and **impact** for each risk

- Broadly two types

  1. **Quantitative risk assessment**
  2. **Qualitative risk assessment**

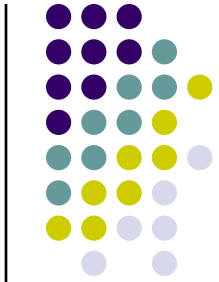
Quantitative risk assessment



- By assigning values to information, systems, business processes, recovery costs, etc., impact, and therefore risk, can be measured in terms of direct and indirect costs

- Mathematically, quantitative risk can be expressed as **Annualized Loss Expectancy** (ALE)

Quantitative risk assessment



ALE = SLE * ARO

Where:

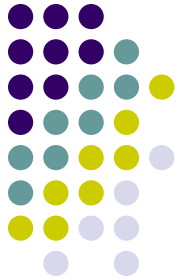
- ALE is the expected **monetary loss** that can be expected for an asset due to a risk being realized over a one-year period

- SLE (Single Loss Expectancy) is the value of a single loss of the asset. This is the **impact** of the loss

-

- ARO (Annualized Rate of Occurrence) is how often the loss occurs. This is the **likelihood**

Qualitative risk assessments



- **Qualitative risk assessments** typically give risk results of “High”, Moderate” and “Low”.

- By providing the **impact** and **likelihood** definition tables and the description of the impact, it is possible to adequately communicate the assessment to the organization’s management

Impact and likelihood table

Tabulating the variables to determine the criticality of the risk that need to be prioritized and addressed

Sample Risk Determination Matrix

		Impact		
		High	**Moderate**	**Low**
Likelihood	**High**	High	High	Moderate
	Moderate	High	Moderate	Low
	Low	Moderate	Low	Low

Relating threats to vulnerabilities

- Establishing the relationship is a **mandatory** activity, since risk is defined as the exercise of a threat against vulnerability
- This is often called threat-vulnerability (T-V) **pairing**
- For instance, a threat of “flood” obviously applies to a vulnerability of “lack of contingency planning”

How is risk managed?

- There are four basic strategies for managing risk: **mitigation, transference, acceptance and avoidance**

- For each risk management strategy, the cost associated with the strategy and the basic steps for achieving the strategy (known as the **Plan Of Action & Milestones** or POAM) must also be determined

Mitigation

- Mitigation is the most commonly considered risk management strategy

- Mitigation involves **fixing the flaw** or providing some type of compensatory control to reduce the likelihood or impact associated with the flaw

- A common mitigation for a technical security flaw is to install a patch provided by the vendor

Transference

- Transference is the process of allowing another party **to accept the risk on your behalf**

- This is not widely done for IT systems, however cloud models provide an opportunity

- Using SaaS, PaaS cloud models, some amount of risk is being transferred to CSP – cloud service provider

Acceptance

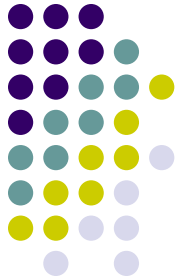
- Acceptance is the practice of simply allowing the system to **operate with a known risk**
- Many low risks are simply accepted
- Risks that have an extremely high cost to mitigate are also often accepted

Avoidance

- Avoidance is the practice of **removing the vulnerable** aspect of the system or even the system itself

- Example is removing a legacy admin system that is causing hi-impact errors in operations

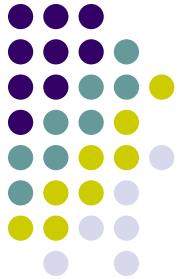
Communicating risks



Sample Risk Management Table

Risk	Risk Description	Impact	Likelihood	Risk Mgmt Strategy	Cost	Residual Risk After Implementing Risk Management Strategy
M[1]	Failure in environmental systems (e.g. air conditioning) leaves systems unavailable.	Failure in environmental controls could cause system to become unavailable for more than 48 hours.	Past data indicates this happens 1-2 times annually	Implement a hot spare at the alternate site	$250,000	L

Communicating risks



- A **Plan Of Action & Milestones** (POAM) should be part of the risk assessment report presented to management

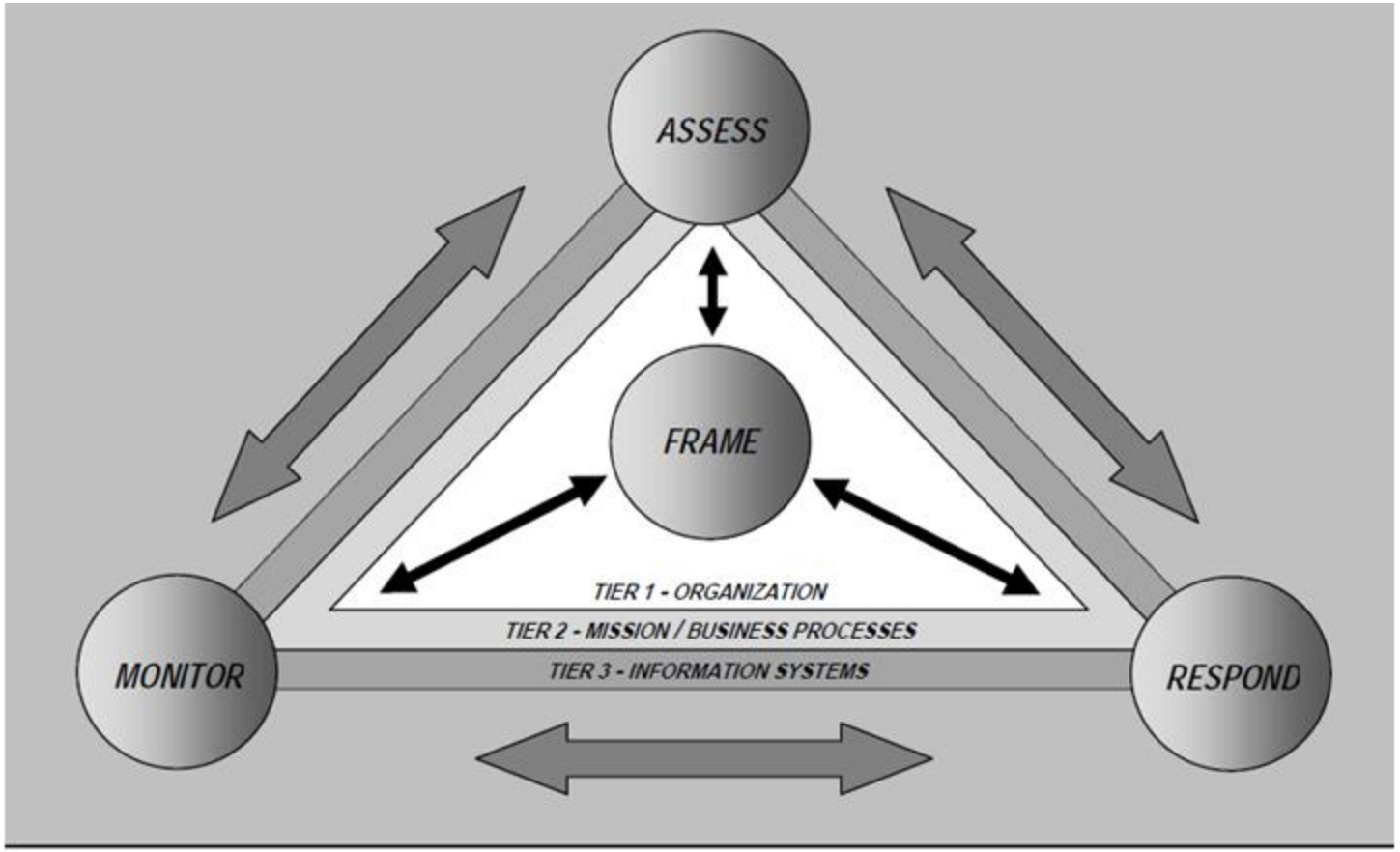
- The POAM is a tool to communicate to management on the proposed and actual completion of the implementation of the risk management strategies

Communicating risks

Sample POAM

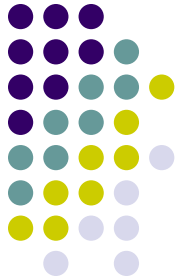
Risk	Risk Mgmt Strategy	POC	Resources Required	Milestones	Target Completion Date	Actual Completion Date
Failure in environmental systems (e.g. air conditioning) leaves systems unavailable.	Implement a hot spare at the alternate site	Joe Smith	$100,000 hardware, $50,000 software, $100,000 labor	Procure hardware & software Install hardware Install software Configure system Test system	9/1 9/15 10/1 10/15 11/1	

Risk management process



RISK MANAGEMENT PROCESS APPLIED ACROSS THE TIERS

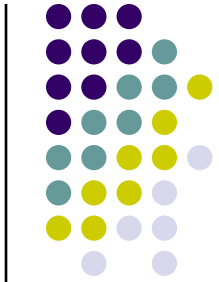
Framing risk



- **Risk framing** establishes the context and provides a common perspective on how organizations manage risk
-
- Risk framing, as its principal output, produces a **risk management strategy** that addresses how organizations intend to assess risk, respond to risk, and monitor risk

- Mainly senior leaders, program manager at Tier 1 & 2 are responsible

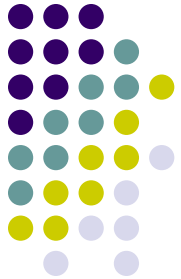
Risk assessment



- Risk assessment **identifies**, **prioritizes**, and **estimates** risk to organizational operations (i.e., mission, functions, image, and reputation), organizational assets, individuals, other organizations, and the Nation

- All tiers provide their reports to the security officer for further action plan

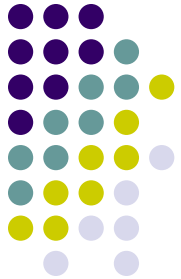
Risk response



- Risk response identifies, evaluates, decides on, and **implements** appropriate **courses of action** to accept, avoid, mitigate, share, or transfer risk to organizational operations and assets, individuals, other organizations, and the Nation

- Typically occurs at Tier 1 or Tier 2, with feedbacks from Tier 3

Risk monitoring



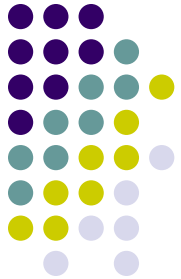
Risk monitoring provides organizations with the means to:

(i) **verify** compliance

(ii) determine the **ongoing effectiveness** of risk response measures; and

(iii) identify **risk-impacting changes** to organizational information systems and environments of operation

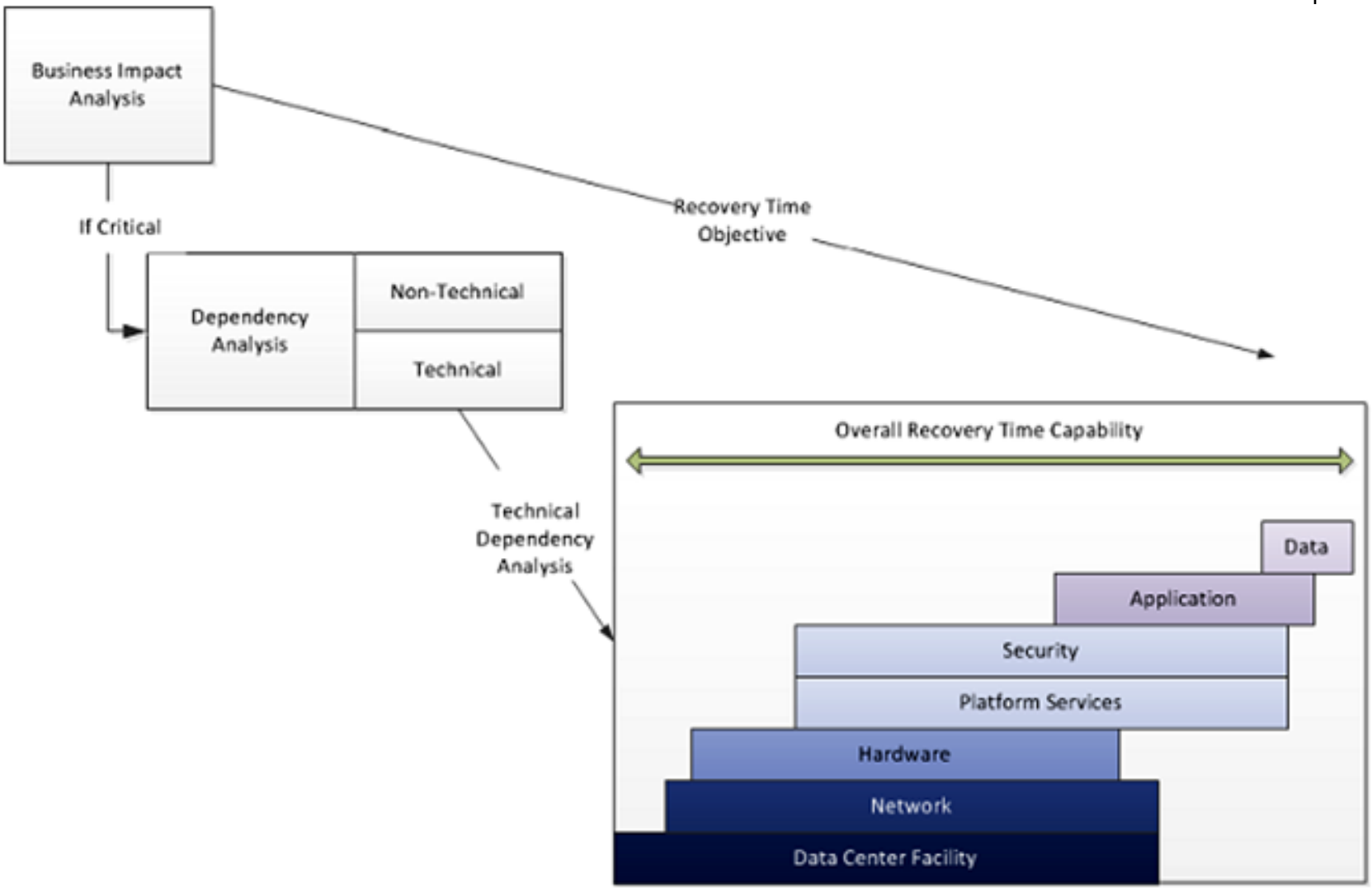
Information technology continuity plan



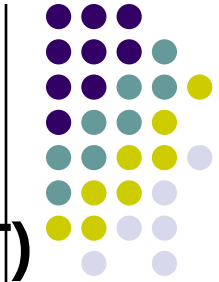
Conduct a business impact analysis to identify:

1. Critical IT resources
2. Outage impacts and allowable outage times
3. Protocols to provide uninterrupted power by using UPS devices, power
4. Store backup data in a secure and protected offsite location
5. Develop recovery strategies that allow critical IT resources to be recovered within 24 hours.
6. Document the recovery strategy

Microsoft's impact analysis



General risk assessment tools

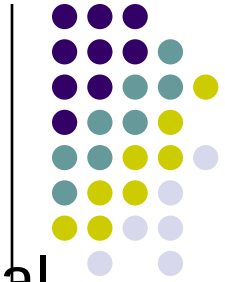


- **National Institute of Standards & Technology (NIST) Methodology** – US Federal based

- **OCTAVE®** - The Software Engineering Institute (SEI) at Carnegie Mellon University developed the Operationally Critical, Threat, Asset and Vulnerability Evaluation (OCTAVE) process

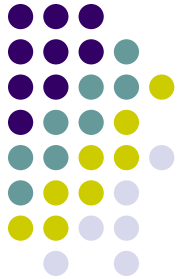
- **FRAP** - The Facilitated Risk Assessment Process (FRAP) is the creation of Thomas Peltier. FRAP uses formal qualitative risk analysis methodologies using Vulnerability Analysis, Hazard Impact Analysis, Threat Analysis and Questionnaires

General risk assessment tools



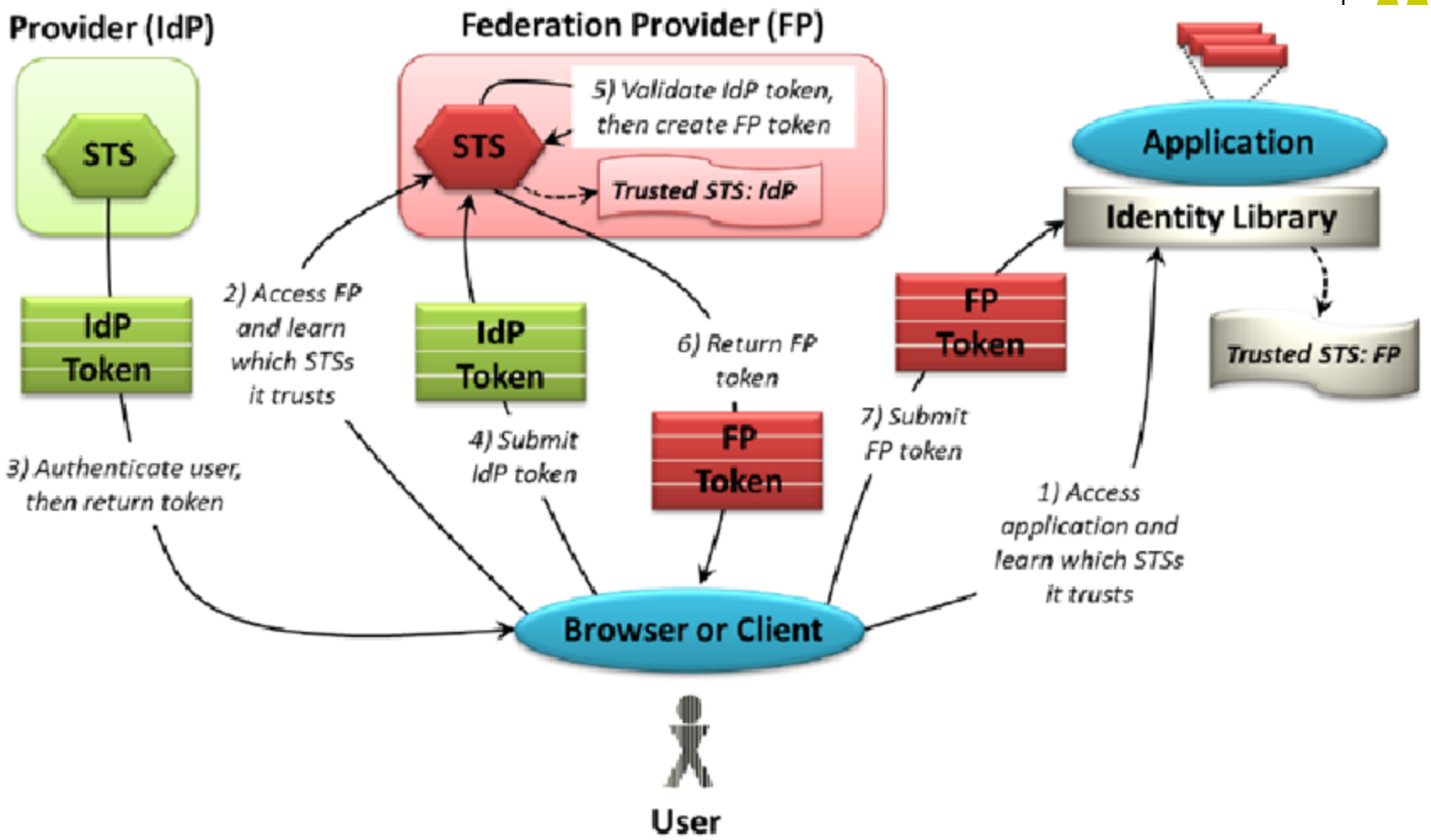
- **COBRA** - The Consultative, Objective and Bi-functional Risk Analysis (COBRA) process was created by C & A Systems Security Ltd.. Risk assessment is a business issue rather than a technical issue, tools that can be purchased and utilized to perform self-assessments of risk

- **Risk Watch**- Uses an expert knowledge database to walk the user through a risk assessment and provide reports on compliance as well as advice on managing the risks



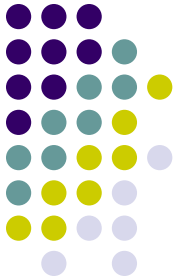
Microsoft security stack / tools

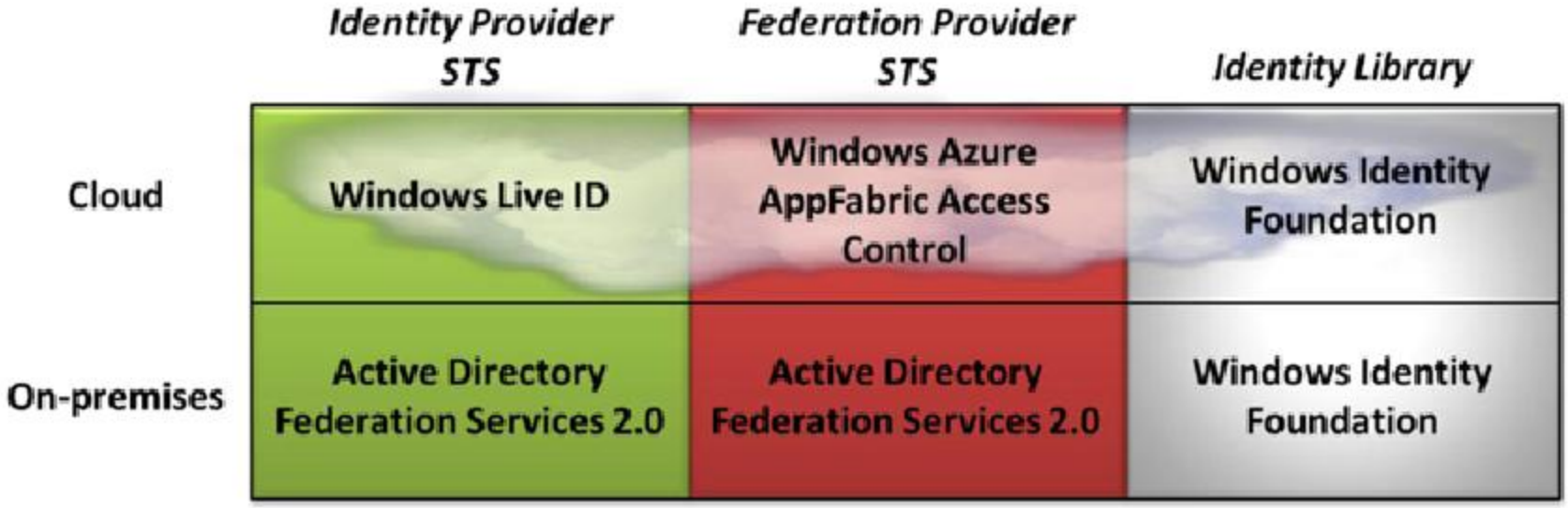
Claims based identity for Azure



An STS can act as a federation provider, accepting one token and producing another.

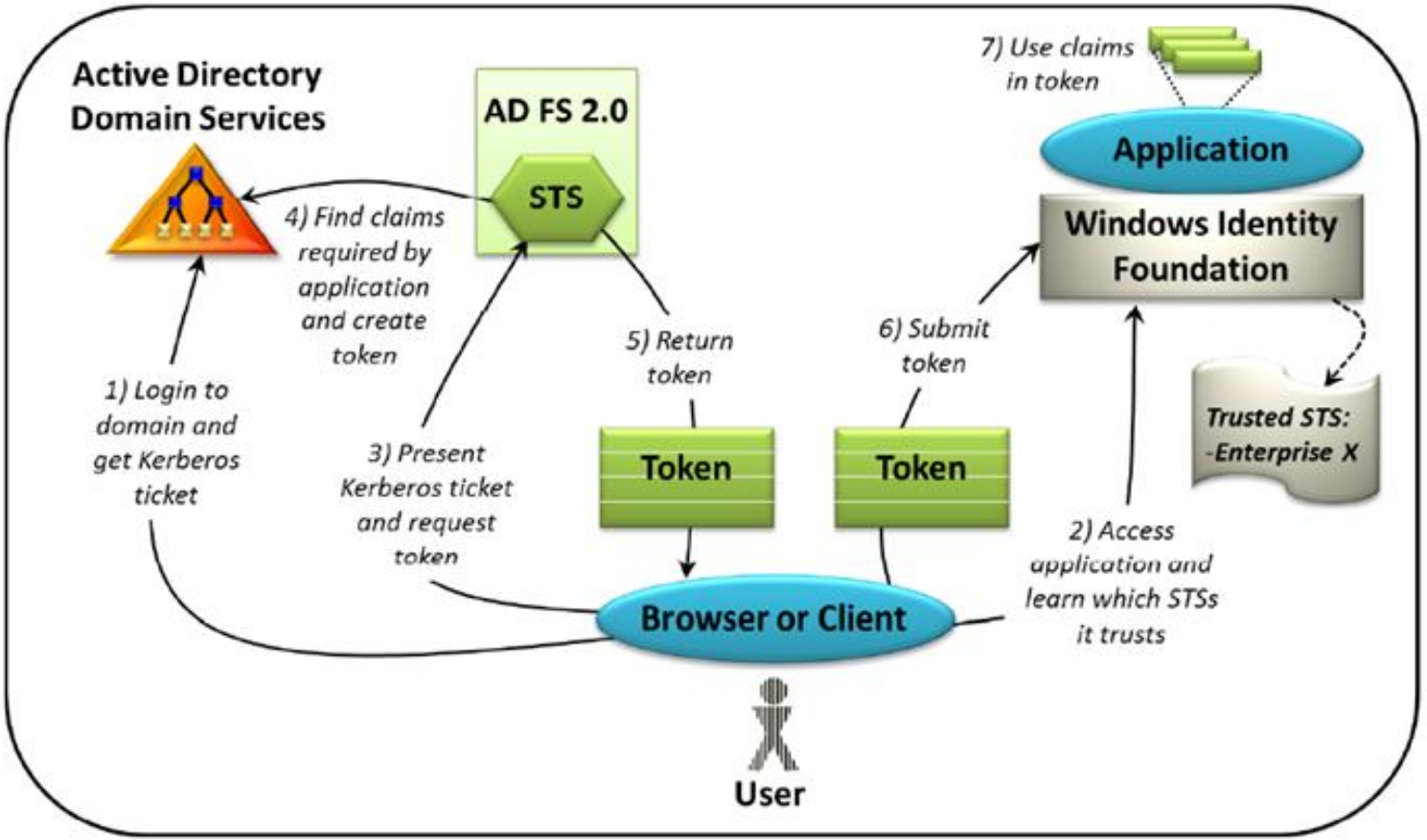
Microsoft offerings





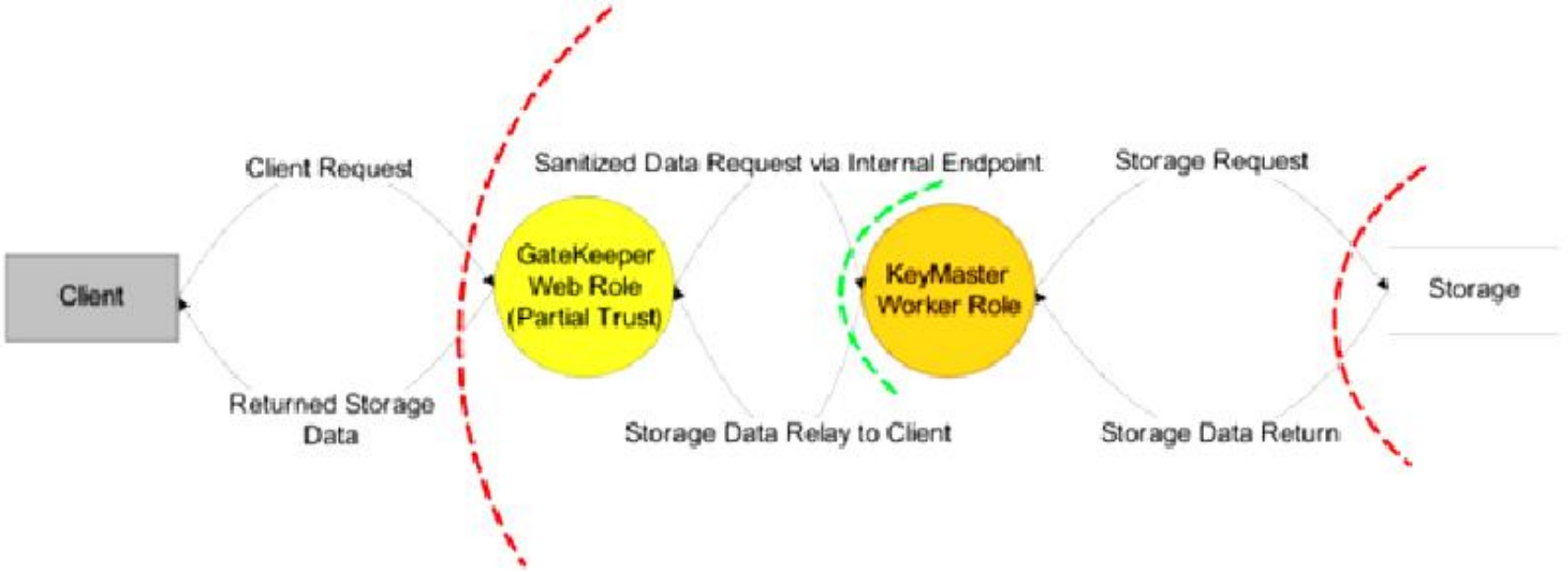
Microsoft provides cloud and on-premises technologies for an identity provider STS, a federation provider STS, and an identity library.

AD-DS, WIF, AD-FS



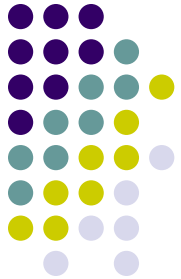
An enterprise can use AD FS 2.0 and WIF to support claims-based identity for its internal applications

Azure - gatekeeper design pattern



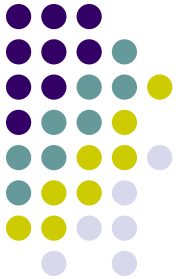
The Gatekeeper Design Pattern

Microsoft's STRIDE threat categories



- **S**poofing identity – pose as another user
- **T**ampering with data – malicious modification of data
- **R**epudiation – can the action (prohibited action) be traced?
- **I**nformation disclosure – disclose of information to individuals who aren't supposed to have it
- **D**enial of service – deny access to valid users (e.g. consume all the CPU time)
- **E**levation of privilege – unprivileged user gains privileged access (becomes part of the trusted system)

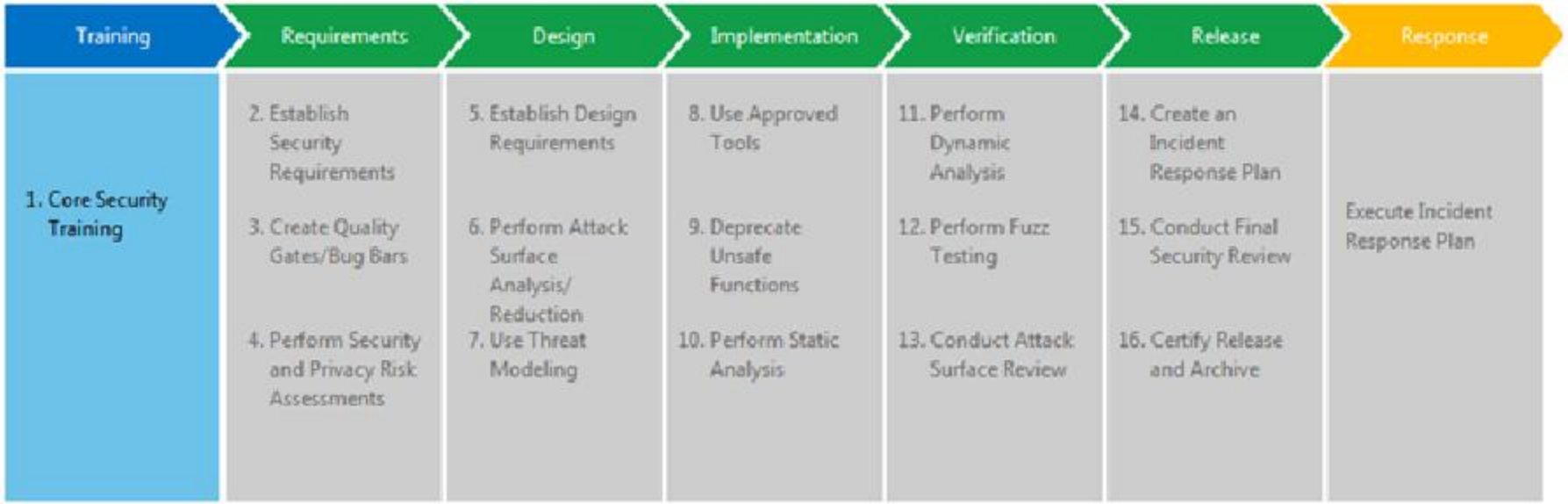
Microsoft's DREAD model to rank threat's severity



- **D**amage potential: The extent of the damage if vulnerability is exploited
- **R**eproducibility: How often an attempt at exploiting vulnerability works
- **E**xploitability: How much effort is required? Is authentication required?
- **A**ffected users: How widespread could the exploit become?
- **D**iscoverability: The likelihood that the researcher or hacker will find it

Security development lifecycle (SDL)

- SDL is a software development process that helps developers build secure code, address compliance



SDL tools

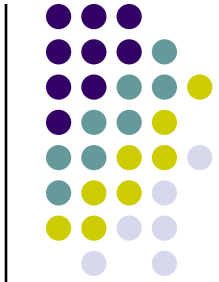
Requirements tools

- Microsoft Solutions Framework (MSF) for Capability Maturity Model Integration (CMMI) / Microsoft Solutions Framework (MSF) for Agile

Design tool

- Microsoft Threat Modeling Tool 2014 / 2016

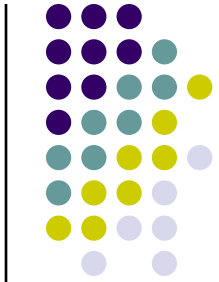
SDL tools



Implementation tools

- banned.h
- Code Analysis for C/C++
- SiteLock ATL Template
- Anti-Cross Site Scripting (Anti-XSS) Library
- FxCop (assemblies)
- Microsoft Code Analysis Tool .NET (CAT.NET) - binary code analysis for XSS, SQL Injection

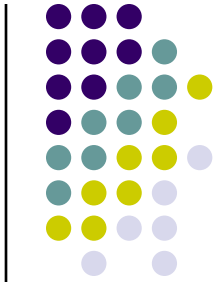
SDL tools



Verification tools

- **BinScope binary analyzer-** binary files
- **SDL Regex fuzzer** – tests reg. exp for DoS
- **SDL MiniFuzz file fuzzer**-detects file-handling flaws
- **Attack surface analyzer**-detect changes in OS, ACL, registry, Active-X control
- **Application verifier**-runtime verification tool for native code

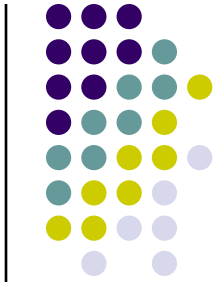
SDL tools



Release tools

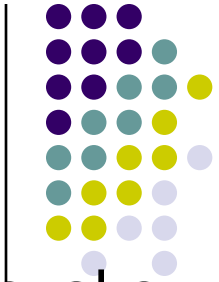
SDL process template- integrates the policy, process, and tools associated with Microsoft SDL Process Guidance version 4.1 directly into your VSTS

Azure network security



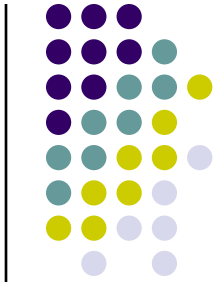
- **VNet** for isolation of VMs
- **ACL** and **NSG** – for access control at VM and subnet level
- **Azure Virtual Filtering** Platform (VFP) exposes an easy-to-program interface to network agents that act on behalf of network controllers and **packet processing** on each host running in the datacenter
- **Service endpoint** and azure **fabric level security** mechanism

Security for mobile-first, cloud-first world

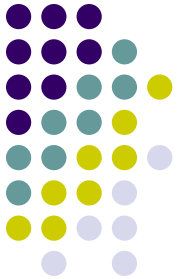


- **Office 365 app permissions -** ability to approve or revoke permissions
- **Azure AD Identity Protection -** prevents the use of compromised credentials
- **Microsoft Cloud App Security -** new advanced security capability
- **Customer Lockbox -** integrates the customer into the approval process
- **Azure Security Center-** Centralized security policy at the subscription level+ Resource Group level (tailored as per workloads)

Security for mobile-first, cloud-first world

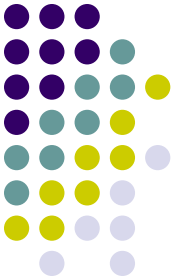


- **Azure Active Directory Identity Protection -** detects suspicious act, user risk severity is calculated and risk-based policies can be configured at user level
- **WindowsAzure.MobileServices.Backend.Security**-security extensions for your .NET mobile backend (controller code level permissions)hosted in Microsoft Azure
- **System Center 2012 and InTune-** mobile device management (MDM), BYOD policies, remote wipe out of data in case of theft



Industrial standards

Industry security management frameworks (ISO series)



27001 Specification for an information security management system (ISMS) against which thousands of organizations have been certified compliant.	**27002** Code of practice for information security describing a comprehensive set of information security control objectives and a set of generally accepted good practice security controls.
27003 Guidance for the implementation of 27001.	**27004** Information security system management measurement and metrics standard.
27005 Information security risk management standard.	**27006** Guidelines for accreditation of organizations offering ISMS certification.
27007 Guide to auditing Information Security Management Systems.	**27008** Guidelines for audit of technical security controls.

Industry security management frameworks

27010
Guidance on information security management for inter-sector and inter-organizational communications.

27011
Guidelines of information security management for telecommunications organizations.

27013
Guidance on the joint implementation of both ISO/IEC 20000-1 (derived from ITIL) and ISO/IEC 27001 (ISMS).

27014
Guidance about information security governance.

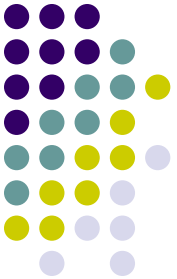
27015
Guidelines of information security management for organizations in the financial services industry.

27016
Paper covering the economics of information security management.

27017 (*)
Security techniques — Information security Management — Guidelines on Information security controls for the use of cloud computing services based on ISO/IEC 27002

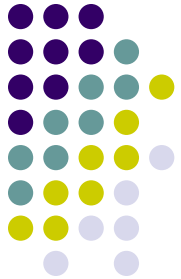
27018
Security techniques — Code of practice for PII protection in public clouds acting as PII processors.

Industry security management frameworks



27019 Security techniques — Information security Management — Guidelines on Information security controls for the use of cloud computing services based on ISO/IEC 27002	ISO/IEC 27031 Security techniques -- Code of practice for PII protection in public clouds acting as PII processors.
27032 Paper covering cybersecurity.	27033 Guidelines on IT network security.
27034 Guidelines for application security.	27035 Guidelines covering information security incident management.
27036 Guidelines for supplier relationships. Part 4: Guidelines for security of cloud services	27037 Guidelines for identification, collection, acquisition and preservation of digital evidence.
27038 Specification for digital redaction.	27039 Guidelines for selection, deployment and operations of intrusion detection systems.

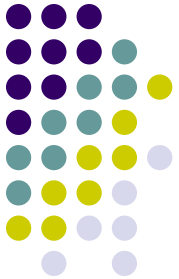
The Payment Card Industry Data Security Standard (PCI DSS)



- PCI DSS provides a baseline of technical and operational requirements designed to **protect cardholder data**

- PCI DSS applies to **all entities** involved in payment card processing—including merchants, processors, acquirers, issuers, and service providers

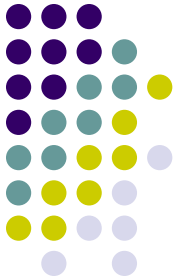
The Payment Card Industry Data Security Standard (PCI DSS)



PCI Data Security Standard – High Level Overview

Build and Maintain a Secure Network and Systems	1.	Install and maintain a firewall configuration to protect cardholder data
	2.	Do not use vendor-supplied defaults for system passwords and other security parameters
Protect Cardholder Data	3.	Protect stored cardholder data
	4.	Encrypt transmission of cardholder data across open, public networks
Maintain a Vulnerability Management Program	5.	Protect all systems against malware and regularly update anti-virus software or programs
	6.	Develop and maintain secure systems and applications
Implement Strong Access Control Measures	7.	Restrict access to cardholder data by business need to know
	8.	Identify and authenticate access to system components
	9.	Restrict physical access to cardholder data
Regularly Monitor and Test Networks	10.	Track and monitor all access to network resources and cardholder data
	11.	Regularly test security systems and processes
Maintain an Information Security Policy	12.	Maintain a policy that addresses information security for all personnel

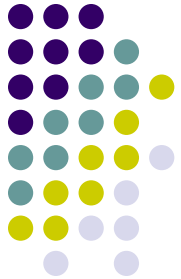
The Payment Card Industry Data Security Standard (PCI DSS)



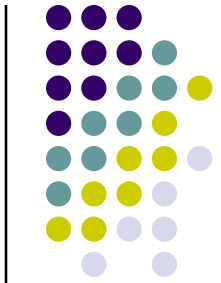
AUDIT TESTING

PCI DSS Requirements	Testing Procedures	Guidance
1.1 Establish and implement firewall and router configuration standards that include the following:	**1.1** Inspect the firewall and router configuration standards and other documentation specified below and verify that standards are complete and implemented as follows:	Firewalls and routers are key components of the architecture that controls entry to and exit from the network. These devices are software or hardware devices that block unwanted access and manage authorized access into and out of the network. Configuration standards and procedures will help to ensure that the organization's first line of defense in the protection of its data remains strong.
1.1.1 A formal process for approving and testing all network connections and changes to the firewall and router configurations	**1.1.1.a** Examine documented procedures to verify there is a formal process for testing and approval of all: • Network connections and • Changes to firewall and router configurations	A documented and implemented process for approving and testing all connections and changes to the firewalls and routers will help prevent security problems caused by misconfiguration of the network, router, or firewall. Without formal approval and testing of changes, records of the changes might not be updated, which could lead to inconsistencies between network documentation and the actual configuration.
	1.1.1.b For a sample of network connections, interview responsible personnel and examine records to verify that network connections were approved and tested.	

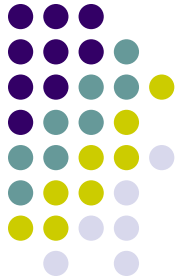
Disclaimer



- *Logos, images, text have been referenced from various sources like NIST, SANS, PCI journals, David Chappell, Microsoft websites, and internet data that is freely available. Full rights belong to the individual owners. References are made strictly for educational and illustration purposes only and for non-commercial use. Please take advice of original authors before using them. I am not responsible for any damages, monetary loss arising from the use of this document*



Q & A



Thank you