MIS|TI™ PRESENTS

InfoSecWorld

Conference & Expo 2018

MEASURING THIRD-PARTY CLOUD SERVICE PROVIDERS: SERVICE LEVEL AGREEMENTS AS A PERFORMANCE BAROMETER

Summer Craze Fowler
Technical Director (Carnegie Mellon | CERT)
@sumfowler

Matthew J. Butkovic
Technical Manager(Carnegie Mellon | CERT)

INTRODUCTION

Summer Craze Fowler
Technical Director
CERT Division
Software Engineering Institute
sfowler@cert.org

Matthew J. Butkovic
Technical Manager
CERT Division
Software Engineering Institute
mjb101@cert.org

KEY TAKEAWAYS

- Organizations are increasingly reliant on third-party services
- The supply chain will continue to grow in complexity
- Unless cybersecurity requirements are identified and communicated, organizations have little reason to believe their needs will be met
- You can’t outsource risk to your organization
- Smart cybersecurity Service Level Agreements can help reduce risk to your organization
- Draft model based on resilience objectives is available for SLA development
- Van Halen can teach us something about SLAs

CERT MISSION

To anticipate and solve the nation's most challenging cybersecurity problems

We ***gather, analyze, and interpret data*** that others cannot access or handle

We ***engage in our constituents' target environments*** to solve critical software engineering and cybersecurity problems.

We ***attract and grow acknowledged domain experts*** focused on advancing the state of cybersecurity

We ***are the nexus*** of academia, government, industry, and the cybersecurity community

CYBERSECURITY RISK AND RESILIENCE

To protect and sustain assets that are important to the nation's cyber-dependent mission ensuring that they continue to operate during and recover from disruptive events.

Cybersecurity Assurance: Advance the state of the practice of cybersecurity evaluation (technical and process) and support the ability of critical infrastructure providers and government organizations to achieve missions dependent on cyber assets.

Cybersecurity Risk Management: Research, develop, and deploy processes, tools, and solutions to public and private customers that enable operational surety in times of distress.

Enterprise Threat & Vulnerability Management: Research and develop technical and behavioral policies, processes, and controls to discourage, detect, and contain malicious and non-malicious insider threats

THIRD-PARTY RISKS*

Ponemon Institute study indicates **a lack of trust in third-party vendors** to reliably notify your organization of a breach

- **37%** of respondents didn't believe vendors would notify them of a data breach
- when that vendor is further removed (a fourth-party vendor or greater), that number grows to **73%**.

Soha Systems study places the percentage of all data breaches linked directly or indirectly to third-party access at **63 percent**

Organizations spent **$10 million responding to third-party breaches** over the previous 12 months (May 2016 report)

*** www.ponemon.org and www.akamai.com**

EVOLVING ROLE OF MANAGING CYBERSECURITY

- ~15 years ago Information Security was about managing a co-located data warehouse or processing center with all functions performed in-house

- 2017 Ernst & Young survey of more than 1,700 company executives and IT managers from across the world:
  - 41% of companies have outsourced their security monitoring
  - 52% of companies outsource their vulnerability assessments
  - 21% outsource cybersecurity help center & self-phishing drills
  - 56% outsource business-specific cybersecurity activities
  - 33% subcontract the development of their cybersecurity management systems

- Forrester estimates that global cloud services revenues totaled $114 billion in 2016, up from $68 billion in 2014 — that's annual growth of 30%
- Public cloud services market expected to reach $236B USD by 2020

http://www.ey.com/gl/en/services/advisory/ey-global-information-security-survey-2016
https://go.forrester.com/blogs/17-06-08-cloud_security_spending_will_grow_to_35_billion_by_2021/

TOP SKILLS REQUIRED FOR A CISO…WHAT'S MISSING?

Listed as top skills for CISO/cybersecurity leadership (combination of sources):

- Communication and presentation skills
- Policy development and administration
- Political skills
- Collaboration and conflict management skills
- Planning and strategic management skills
- Supervisory skills
- Incident management
- Knowledge of regulation and standards compliance
- Risk assessment and management

External Dependencies Management skills – including contracts management - are critical for cybersecurity leadership of today and the future!

WHY OUTSOURCE?

REASONS FOR OUTSOURCING*

- Reducing and controlling operating costs
- Improving company focus
- Gaining access to world-class capabilities
- Freeing internal resources for other purposes
- Streamlining or increasing efficiency for time-consuming functions
- Maximizing use of external resources
- Sharing risks with a partner company

Cybersecurity risk is about much more than just confidentiality - Availability & Integrity are critical as well!

Commonly Noted Risks of Outsourcing

- Loss of control
- Vendor lock-in
- Hidden costs
- Geo-location (ease of doing business)
- Loss of confidentiality

*https://www.thebalance.com/why-do-companies-outsource-2553035

IMPROVING EXTERNAL DEPENDENCIES MANAGEMENT

EXTERNAL DEPENDENCIES MANAGEMENT

Establish and manage an appropriate level of controls to ensure the resilience of services and assets that are dependent on the actions of external entities

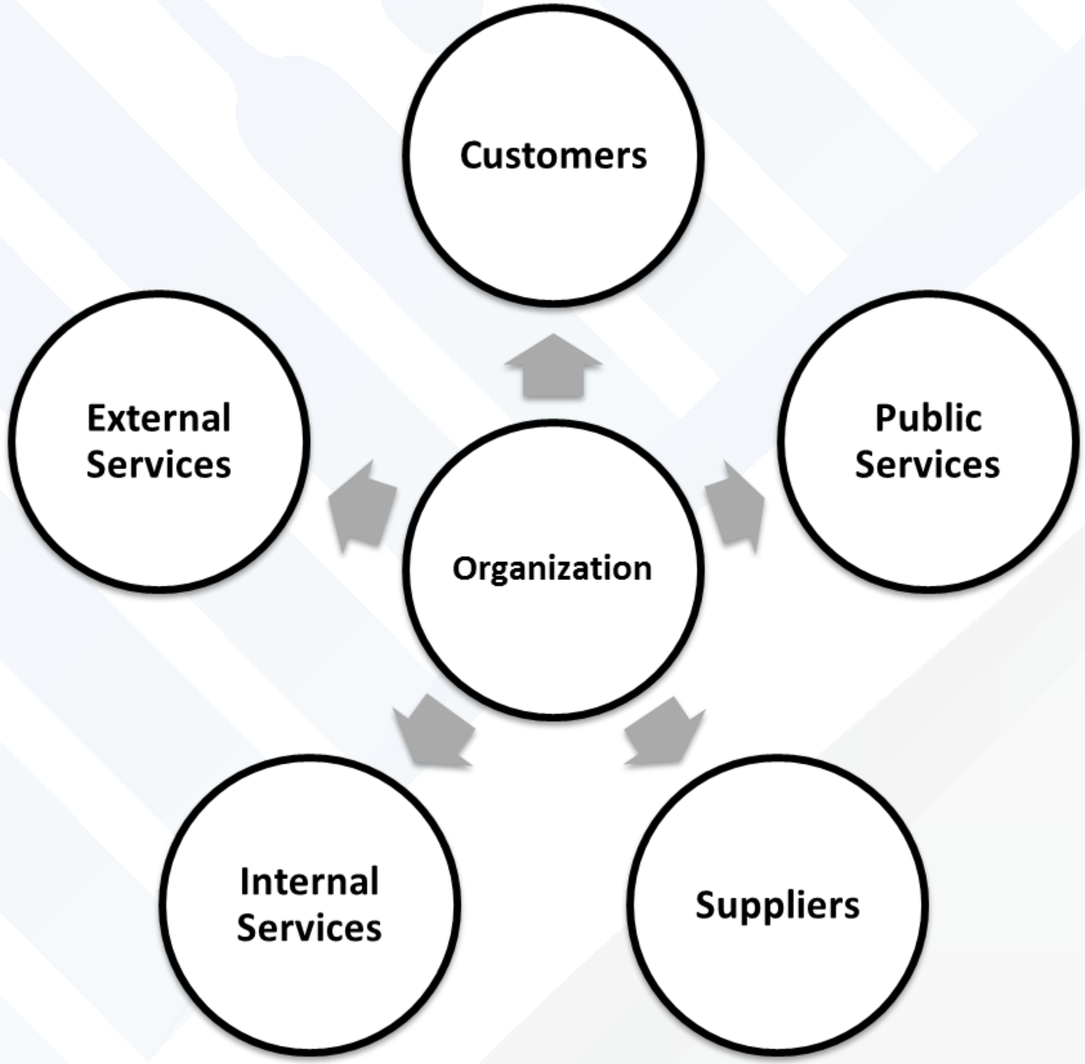
Goal is to maximize benefits of external relationships AND ensure resilience of organization to achieve its business objectives

RISK IN EXTERNAL DEPENDENCIES

"*One caveat of outsourcing is that you can outsource business functions, but you cannot outsource the risk and responsibility to a third party. These must be borne by the organization that asks the population to trust they will do the right thing with their data*."

-Verizon 2012 Data Breach Investigations Report

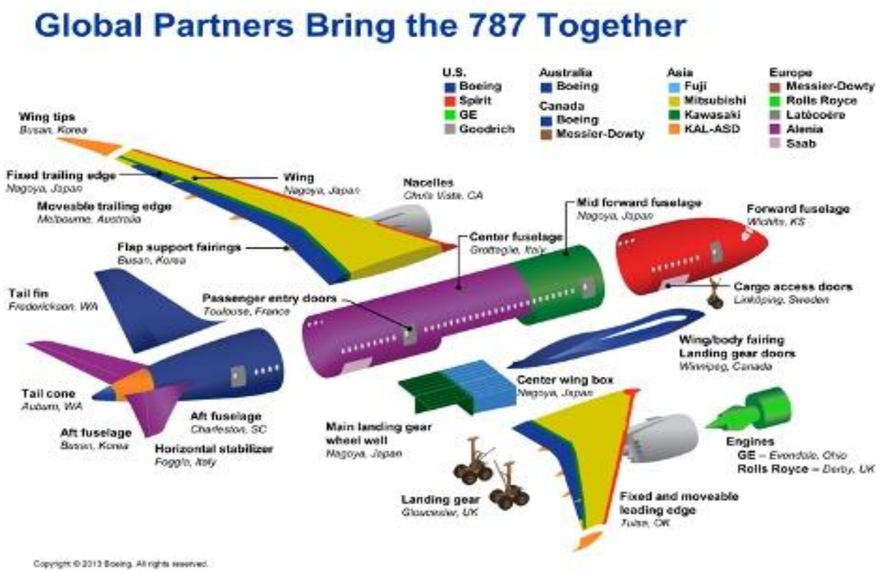
RANGE OF EXTERNAL DEPENDENCIES TO CONSIDER



YESTERDAY'S ENTERPRISE

Source: www.wikipedia.org

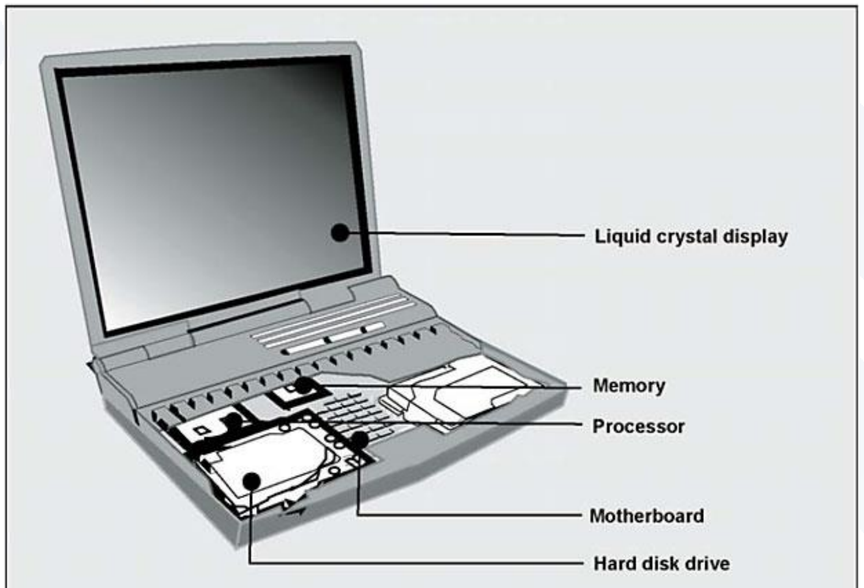
GROWING SUPPLY CHAIN COMPLEXITY



Source: www.boeing.com

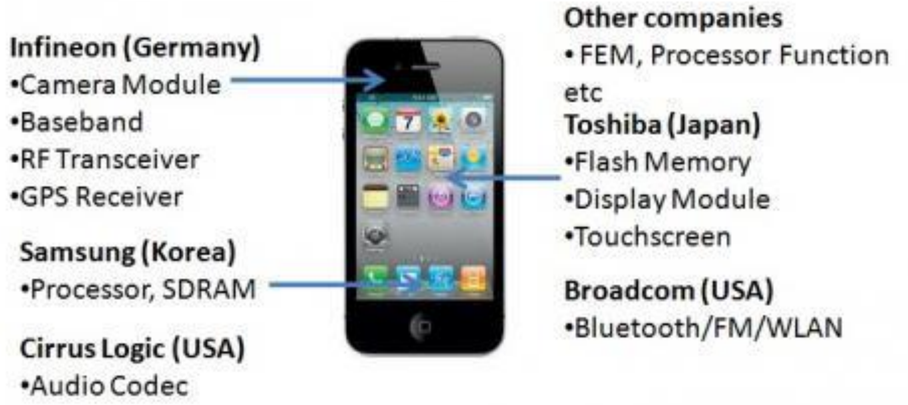
COMPONENT SOURCING

Potential Origins of Common Suppliers for Laptop Components



Component	Location of facilities potentially used by suppliers
Liquid crystal display	China, Czech Republic, Japan, Poland, Singapore, Slovak Republic, South Korea, Taiwan
Memory	China, Israel, Italy, Japan, Malaysia, Philippines, Puerto Rico, Singapore, South Korea, Taiwan, United States
Processor	Canada, China, Costa Rica, Ireland, Israel, Malaysia, Singapore, United States, Vietnam
Motherboard	Taiwan
Hard disk drive	China, Ireland, Japan, Malaysia, Philippines, Singapore, Thailand, United States

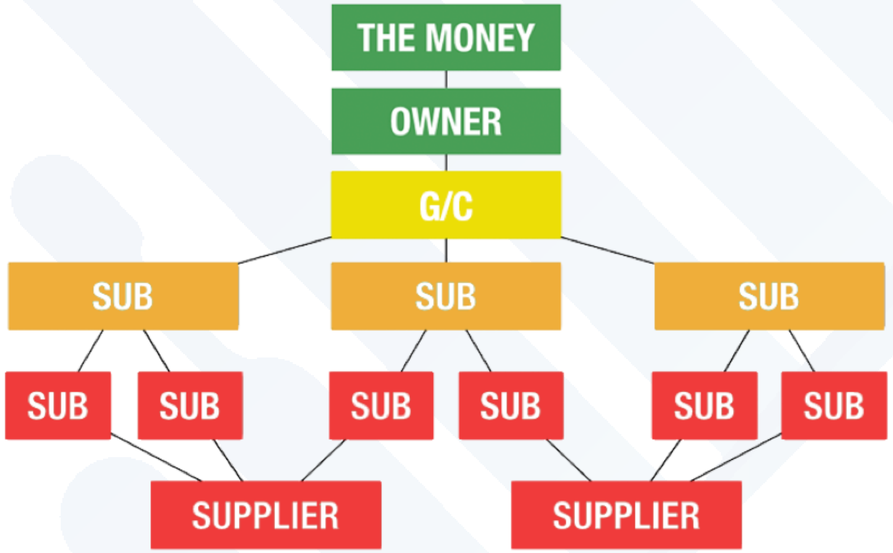
Source: US Government Accountability Office (GAO)



Source: www.iphonelife.com

Source: www.thehackernews.com

SUBCONTRACTOR RELATIONSHIPS



Source: www.fieldlen.com

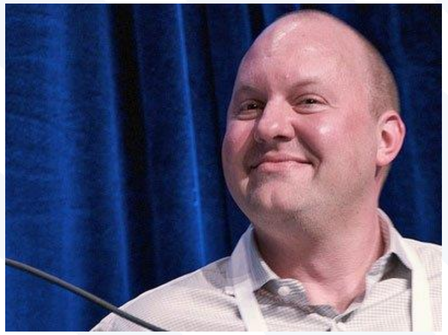
Source: www.theoutscoureblog.com

DFARS COMPLIANCE

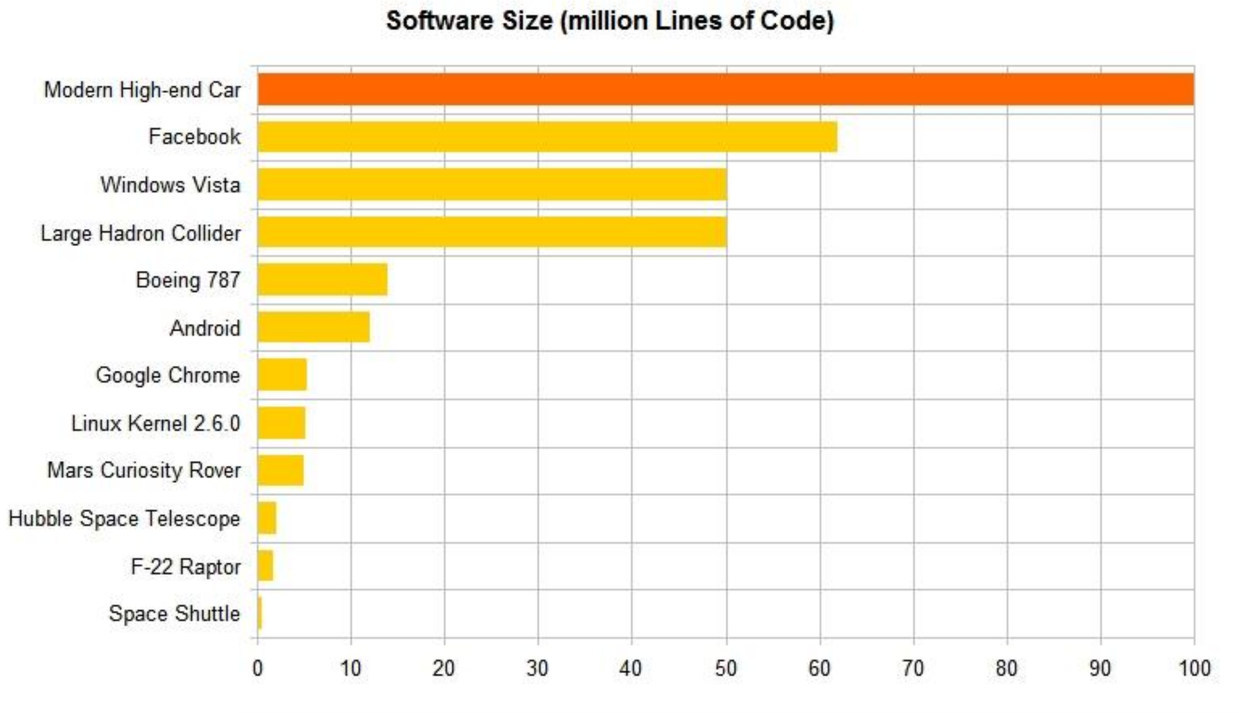
DEFENSE FEDERAL ACQUISITION REGULATION SUPPLEMENT

SOFTWARE IS EVERYWHERE

“In short, software is eating the world.”- Marc Andreesen



Source: www.wjs.com

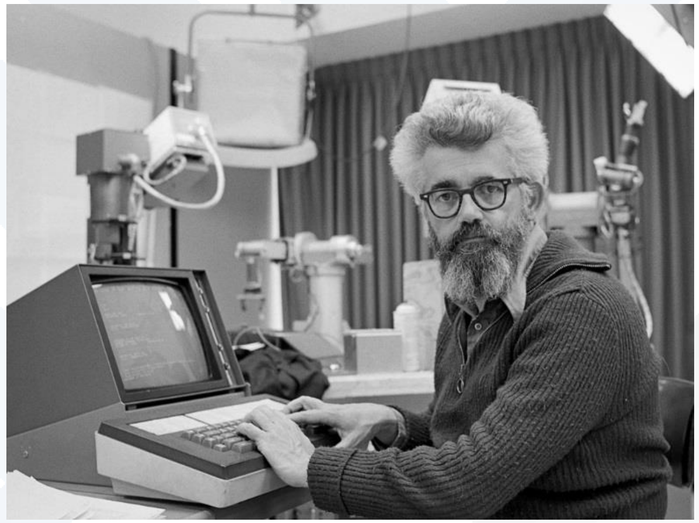


Source: Andrea Busnelli

CLOUD CONSIDERATIONS

HISTORY OF THE CLOUD

- Idea of cloud computing came from several people:
  - Professor John McCarthy of MIT
  - Dr. J.C.R. Licklider, director at the U.S. Department of Defense Advanced Research Projects Agency (ARPA)
- In 1999, Salesforce.com developed a Web service that applied digital marketing research to business subscribers
  - This service led the way to the cloud delivery model



CLOUD COMPUTING IS ONLY A METAPHOR AFTER ALL

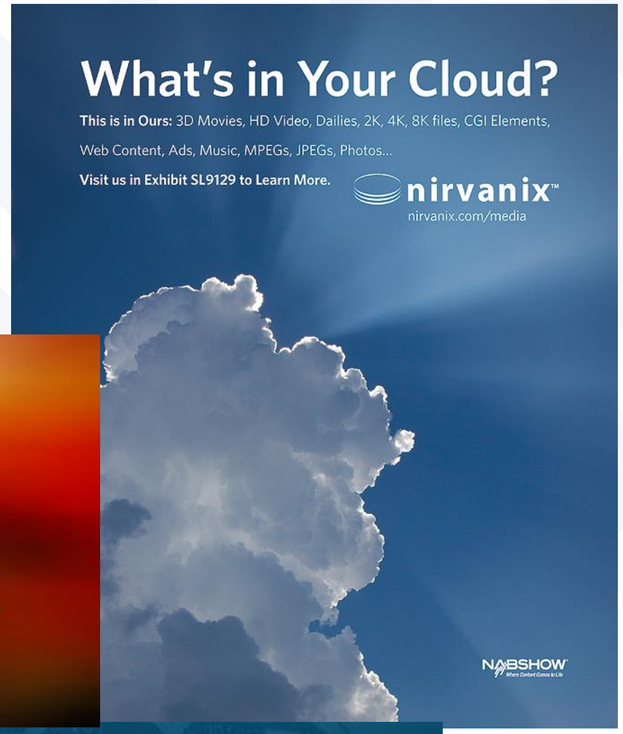
NOTABLE CLOUD PROVIDER OUTAGES

- IBM-Bluemix (January 26, 2017) =30 hrs.
- Github (January 31, 2017) = 18 hrs.
- Instapaper (February 9-12, 2017) = 96 hrs.
- Amazon AWS (February 28, 2017) = 4 hrs.
- Microsoft Azure (March 16, 2017) = 8hrs.
- Microsoft Office 365 (March 21, 2017) = 10hrs.
- Lululemon (IBM) (May 22, 2017) = 36hrs.
- Microsoft Skype (June 19, 2017) = 8hrs.
- Apple iCloud (June 28, 2017) = 36hrs.
- Microsoft Azure (September 29, 2017) = 7hrs.
- **Amazon AWS (March 2, 2018) = 6hrs**
  - **Atlassian and Twilio users affected resulting from wind storm!**

Source: http://www.infoworld.com

WHEN CLOUD PROVIDERS FAIL OR FADE

- Nirvanix (2013)
- Symantec (2013)
- Umano (2015)



Gartner analyst William Maurer expects about 1 in 4 IT-service providers to declare bankruptcy, be bought out or go out of business.

- Would you be able to get your data out?
- How would you be able to get your data out?
- If you're using the cloud-service provider as a backup to your main operation, should the service provider destroy all your data when the relationship ends?

- WHAT ELSE?!?!?!

CLOUD INCIDENTS AND THREAT TYPES

	Threat Category	Number of Incidents
1	Insecure interfaces and application programming interfaces (APIs)	51
2	Data loss or leakage	43
3	Hardware failure	18
4	Inadequate infrastructure design and planning	15
5	Abuse and nefarious use of cloud computing	12
6	Unknown risk profile	11
7	Cloud-related malware	6
8	Shared technology issues	5
9	Natural disasters	4
10	Closure of cloud service	4
11	Malicious insiders	3
12	Account or service hijacking	3

Source: http://www.isaca.org

SERVICE PROVIDER TRANSPARENCY

Source: www.reddit.com

Service Level Agreement

Service Level Agreement (SLA) (ITILv2)**:** A formal, negotiated document that defines (or attempts to define) in quantitative(and perhaps qualitative) terms the service being offered to a Customer. Confusion must be avoided over whether the quantitative definitions constitute thresholds for an acceptable service, targets to which the supplier should aspire or expectations that the supplier would strive to exceed. Any metrics included in a Service Level Agreement (SLA) should be capable of being measured on a regular basis and the SLA should record by whom. Typically it will cover: service hours, service availability. Customer support levels, throughputs and responsiveness, restrictions, functionality, and the service levels to be provided in a contingency. It may also include information on security, charges, and terminology.

Source: http://www.knowledgetransfer.net

Standard SLAs and Contracts . . .

- Basic reasons to have a contract (partial list):
  - Risk allocation
  - Recovering damages
  - Defining breach
  - Drive behavior

- However in practice cyber SLAs can be:

…unidirectional (they are written by the vendor, and smaller customers have trouble changing them)

…lacking specific measures, apart from availability metrics

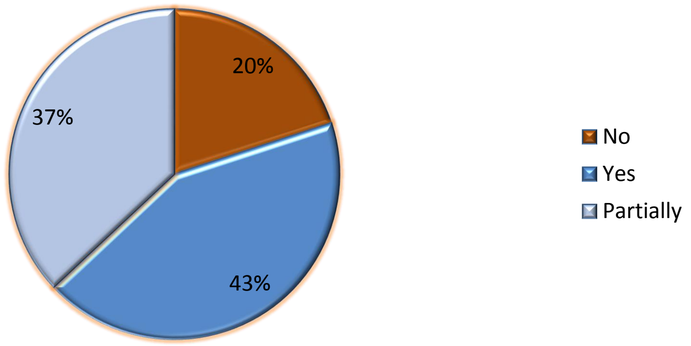
…frequently indemnify the provider to the greatest extent possible, limiting the provider's exposure.

AUDIENCE POLL

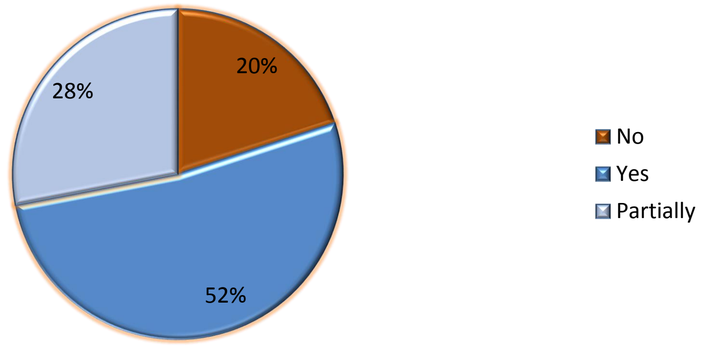
1. Does your organization document specific security objectives in agreements with third parties?
2. Does your organization include measures of cybersecurity performance in third-party agreements?
3. Does your organization monitor compliance with security objectives in agreements with third parties?
4. Is cybersecurity performance considered when selecting third parties?

STATE OF THE PRACTICE

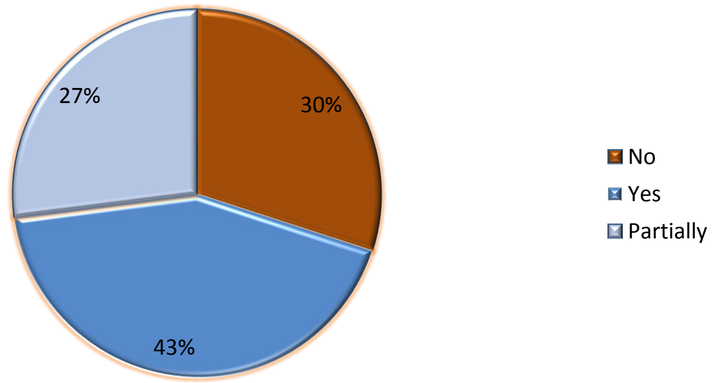
Does your organization document security objectives in agreements with third parties?



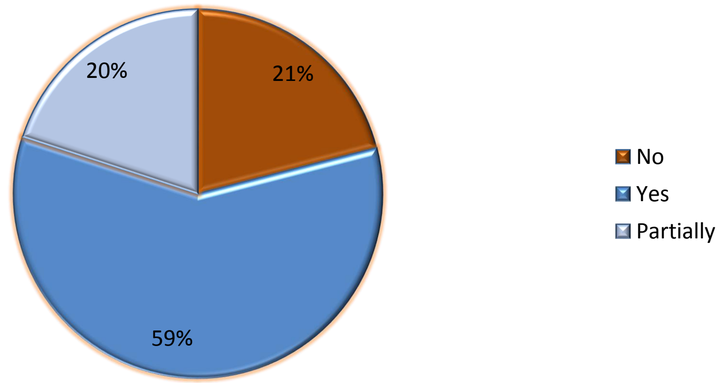
Does your organization include measures of security performance in agreements?



Does your organization monitor compliance to security objectives in agreements?



Is cybersecurity performance considered when selecting third parties?



THE ROLE AND LIMITATIONS OF FORMAL AGREEMENTS AND SLAS

Organizations should:

- Establish and maintain requirements for external entities
- Include requirements in SLAs and other agreements
- Monitor performance against these agreements

Key point: Managers should understand the role and limitations of contracts and formal agreements

EXAMPLE OF CLOUD SLA - GOOGLE

“Each party will protect the other party’s confidential information with the same standard of care it uses for its own information.”

6. **Confidential Information.**

6.1 **Obligations.** Each party will: (a) protect the other party's Confidential Information with the same standard of care it uses to protect its own Confidential Information; and (b) not disclose the Confidential Information, except to Affiliates, employees and agents who need to know it and who have agreed in writing to keep it confidential. Each party (and any Affiliates' employees and agents to whom it has disclosed Confidential Information) may use Confidential Information only to exercise rights and fulfill its obligations under this Agreement, while using reasonable care to protect it. Each party is responsible for any actions of its Affiliates' employees and agents in violation of this Section.

6.2 **Exceptions.** Confidential Information does not include information that: (a) the recipient of the Confidential Information already knew; (b) becomes public through no fault of the recipient; (c) was independently developed by the recipient; or (d) was rightfully given to the recipient by another party.

6.3 **Required Disclosure.** Each party may disclose the other party's Confidential Information when required by law but only after it, if legally permissible: (a) uses commercially reasonable efforts to notify the other party; and (b) gives the other party the chance to challenge the disclosure.

EXAMPLE OF CLOUD SLA - AMAZON

“Reasonable and appropriate measures”
“”You are responsible for properly configuring and using the Service Offerings and taking your own steps to maintain appropriate security…”
“Limitations of Liability”

- Amazon not responsible for damages

3. Security and Data Privacy.

3.1 AWS Security. Without limiting Section 10 or your obligations under Section 4.2, we will implement reasonable and appropriate measures designed to help you secure Your Content against accidental or unlawful loss, access or disclosure.

3.2 Data Privacy. We participate in the safe harbor programs described in the Privacy Policy. You may specify the AWS regions in which Your Content will be stored and accessible by End Users. We will not move Your Content from your selected AWS regions without notifying you, unless required to comply with the law or requests of governmental entities. You consent to our collection, use and disclosure of information associated with the Service Offerings in accordance with our Privacy Policy, and to the processing of Your Content in, and the transfer of Your Content into, the AWS regions you select.

4. Your Responsibilities

4.1 Your Content. You are solely responsible for the development, content, operation, maintenance, and use of Your Content. For example, you are solely responsible for:

(a) the technical operation of Your Content, including ensuring that calls you make to any Service are compatible with then-current APIs for that Service;

(b) compliance of Your Content with the Acceptable Use Policy, the other Policies, and the law;

(c) any claims relating to Your Content; and

(d) properly handling and processing notices sent to you (or any of your affiliates) by any person claiming that Your Content violate such person’s rights, including notices pursuant to the Digital Millennium Copyright Act.

4.2 Other Security and Backup. You are responsible for properly configuring and using the Service Offerings and taking your own steps to maintain appropriate security, protection and backup of Your Content, which may include the use of encryption technology to protect Your Content from unauthorized access and routine archiving Your Content. AWS log-in credentials and private keys generated by the Services are for your internal use only and you may not sell, transfer or sublicense them to any other entity or person, except that you may disclose your private key to your agents and subcontractors performing work on your behalf.

4.3 End User Violations. You will be deemed to have taken any action that you permit, assist or facilitate any person or entity to take related to this Agreement, Your Content or use of the Service Offerings. You are responsible for End Users’ use of Your Content and the Service Offerings. You will ensure that all End Users comply with your obligations under this Agreement and that the terms of your agreement with each End User are consistent with this Agreement. If you become aware of any violation of your obligations under this Agreement by an End User, you will immediately terminate such End User’s access to Your Content and the Service Offerings.

4.4 End User Support. You are responsible for providing customer service (if any) to End Users. We do not provide any support or services to End Users unless we have a separate agreement with you or an End User obligating us to provide support or services.

http://aws.amazon.com/s3-sla/

SLA RESTITUTION

	Amazon EC2	Azure Compute	Google Apps	Rackspace	Terremark/ Verizon
Credit	10% if <99.95	10% if <99.95 25% if <99	3 days if<99.9 7 days if <99 15 days if <95	5-100%	$1/15 min up to 50% of bill
Bill affected	Future	Current	Current	Current	Future
Credit filing window	30 days	1 month	30 days	30 days	30 days
Other comments		Must report within 5 days	$ instead of service permitted		

Lisa Spainhower,"Cloud Provider High Availability", January 18, 2013 IFIP WG10.4 Conference on Dependable Computing and Fault Tolerance, Tavira, Portugal

NEGOTIATING TERMS

PROCESS FOR EFFECTIVELY MANAGING SERVICE LEVEL AGREEMENTS

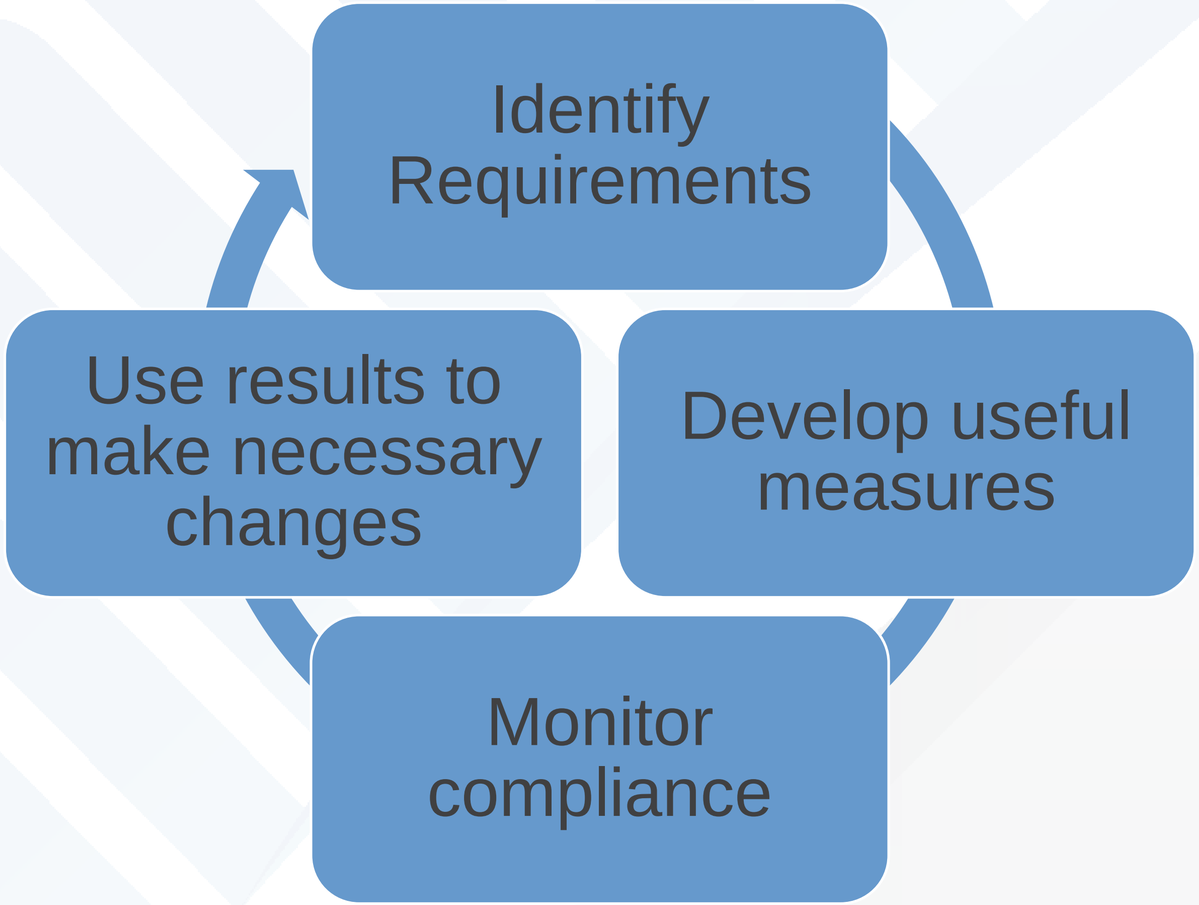
PLANNING FOR EXTERNAL DEPENDENCIES MANAGEMENT

Key goals:

- Identify program management objectives
- Identify services
- Prioritize services
- Identify service requirements
- Identify enterprise requirements
- Plan relationship formation
- Plan relationship management

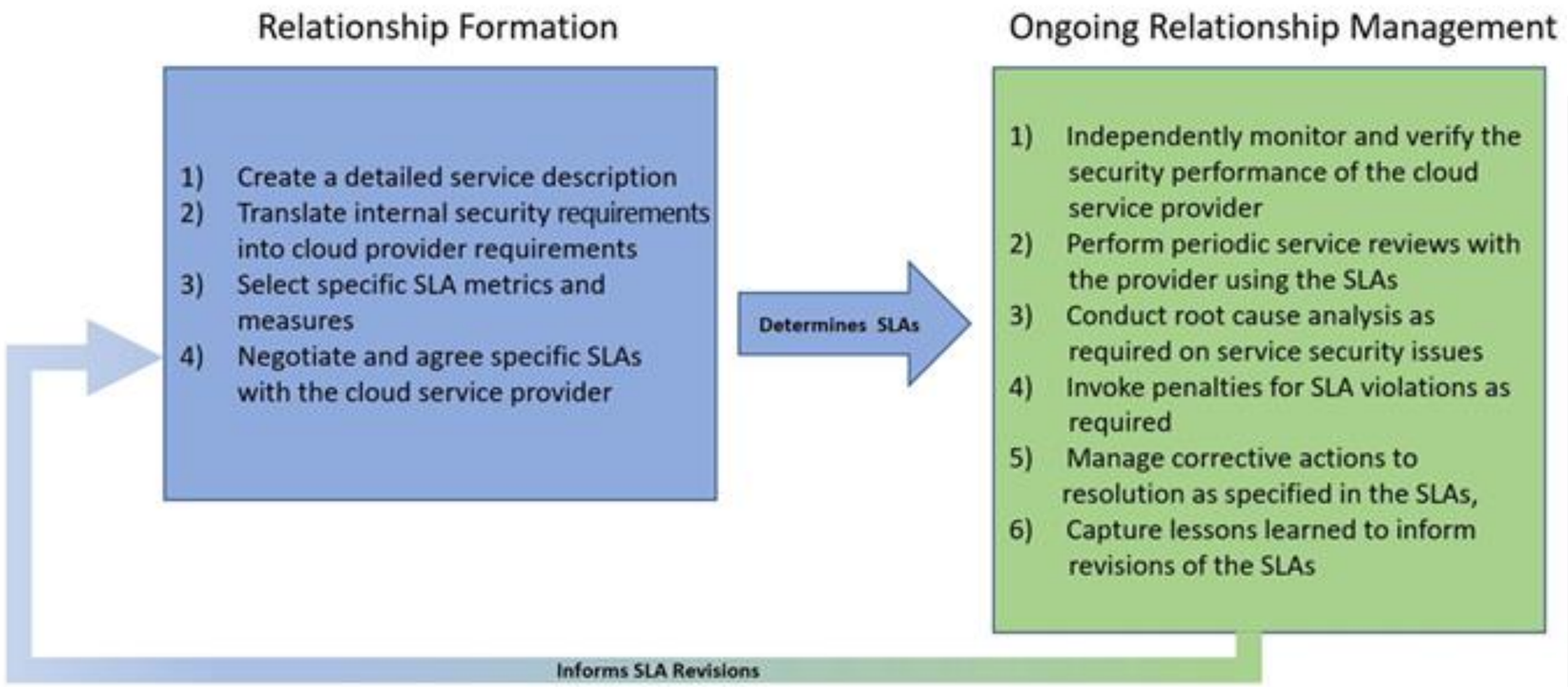
A BETTER MANAGEMENT PROCESS . . .

✓Plan, Do, Check, Act



EVOLUTION OF TRUST

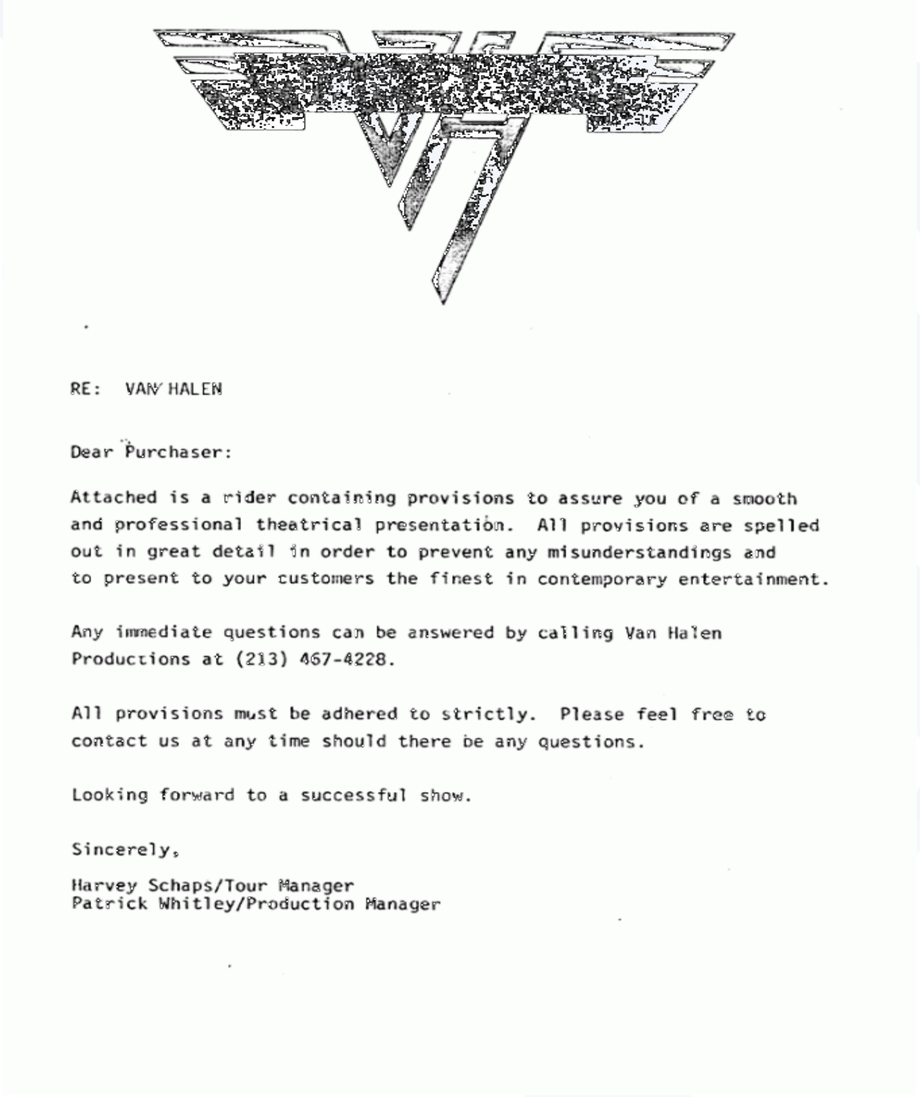
SLA CREATION AND MANAGEMENT



INTERDISCIPLINARY APPROACH

What can Van Halen teach us about Service Level Agreements?

ARTICLE 126 – VAN HALEN CONTRACT



RE: VAN HALEN

Dear Purchaser:

Attached is a rider containing provisions to assure you of a smooth and professional theatrical presentation. All provisions are spelled out in great detail in order to prevent any misunderstandings and to present to your customers the finest in contemporary entertainment.

Any immediate questions can be answered by calling Van Halen Productions at (213) 467-4228.

All provisions must be adhered to strictly. Please feel free to contact us at any time should there be any questions.

Looking forward to a successful show.

Sincerely,

Harvey Schaps/Tour Manager
Patrick Whitley/Production Manager

“So, when I would walk backstage, if I saw a brown M&M in that bowl . . . well, line-check the entire production. Guaranteed you're going to arrive at a technical error. They didn't read the contract. Guaranteed you'd run into a problem. Sometimes it would threaten to just destroy the whole show. Something like, literally, life-threatening” –David Lee Roth

Munchies

Potato chips with assorted dips
Nuts
Pretzels
M & M's (WARNING: ABSOLUTELY NO BROWN ONES)
Twelve (12) Reese's peanut butter cups
Twelve (12) assorted Dannon yogurt (on ice)

Source http://www.npr.org/blogs/therecord/2012/02/14/146880432/the-truth-about-van-halen-and-those-brown-m-ms

ARTICLE 126 – VAN HALEN CONTRACT

"There will be no brown M&M's in the backstage area, upon pain of forfeiture of the show, with full compensation."

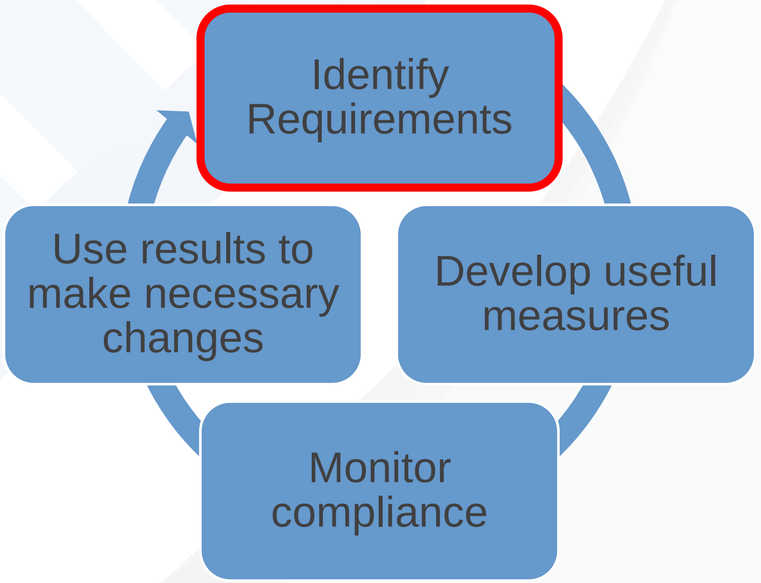
David Lee Roth…Auditor

Source http://www.npr.org/blogs/therecord/2012/02/14/146880432/the-truth-about-van-halen-and-those-brown-m-ms

HOW TO BE LIKE DAVID LEE ROTH!

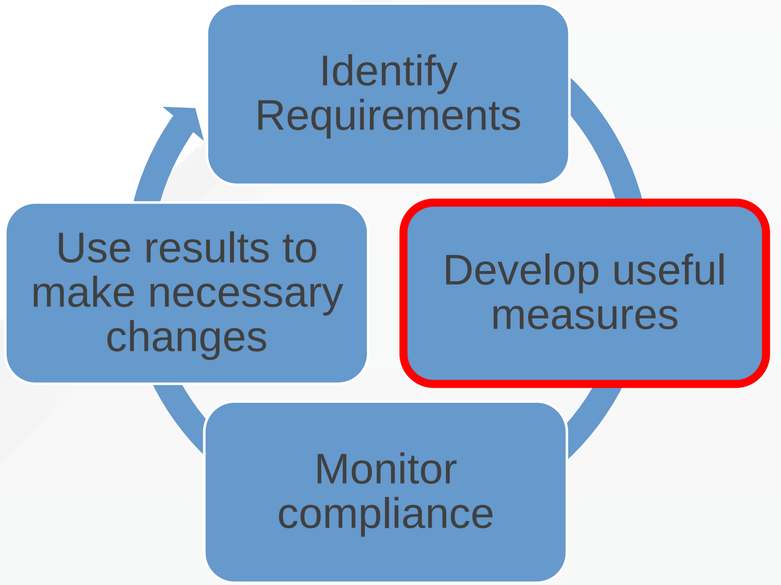
IDENTIFY CYBER REQUIREMENTS

- Confidentiality
  - Who has authorized access?
- Integrity
  - Who is authorized to make changes to the data?
- Availability
  - When does the data needed to be accessed?
- Use service (mission) requirements to develop requirements
  - Good:
    - Aligns with needs of the business
    - Can be a check against too much investment/expense
  - Bad:
    - Potentially expensive to develop



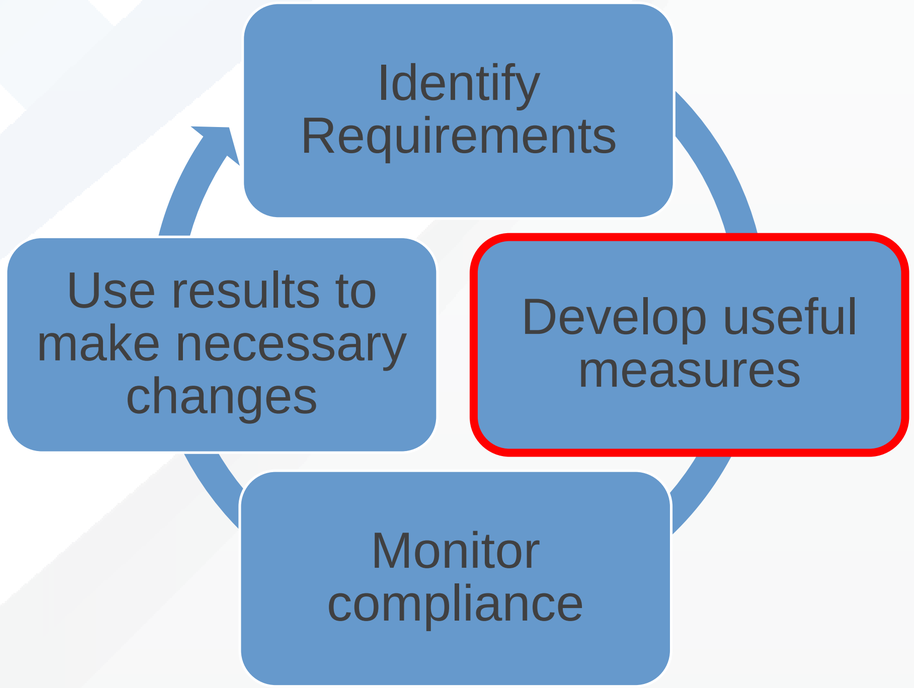
EXAMPLE BASIC MEASURES

- Percentage of (successful, failed) access attempts on confidential data by unauthorized (networks, users, processes)
- Number of incidents involving (successful, failed) unauthorized attempts to export data
- Percentage of inventoried confidential data accessed during cybersecurity incidents
- Number of incidents involving (successful, failed) unauthorized modifications to confidential data



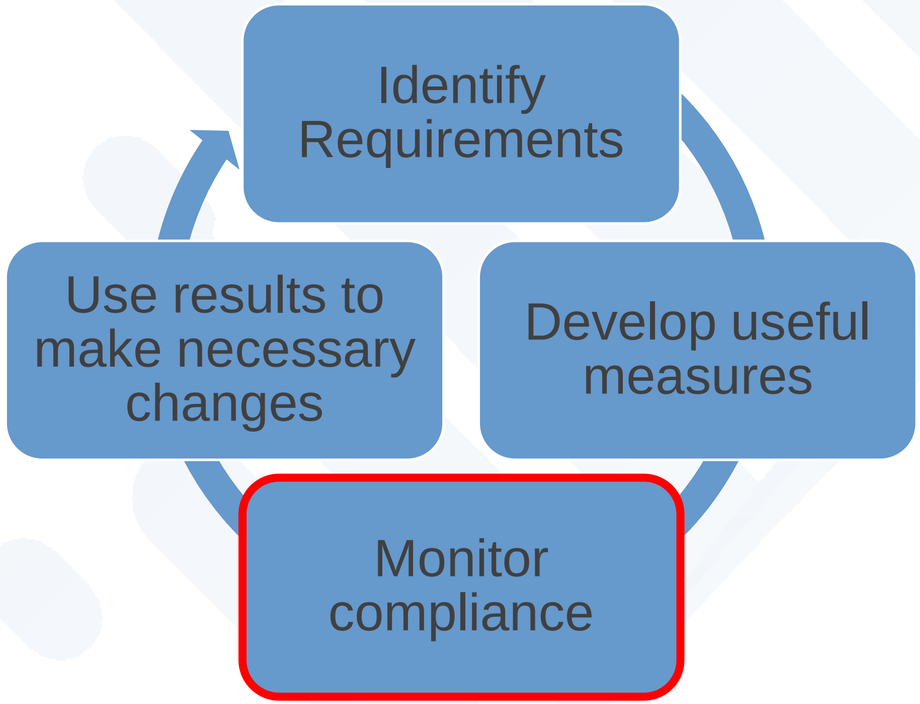
EXAMPLE EFFECTIVENESS MEASURES

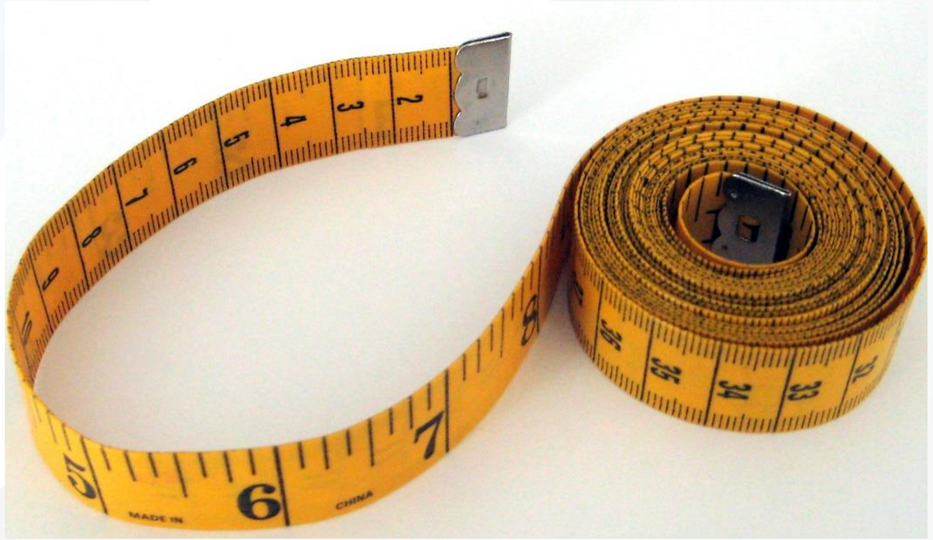
- External dependencies risks or potential risks that remain unresolved
- Open or unresolved high-risk supplier issues
- Aging statement for corrective action reporting
- Count of external entity relationships formed outside of the process
- Emerging threats or risks that may affect key dependencies or suppliers
- Number and frequency of critical service outages traceable to external entities
- Percentage of external entities that have successfully passed third-party audits
- Percentage of missed deliveries or shipping delays from external entities
- Contracts or agreements that did not follow established procedures or policy
- Percentage of SLAs across key external entities (e.g., tier 1 and tier 2 suppliers) that include resilience requirements in their agreements
- Response times and other metrics relating to business continuity or cybersecurity drills conducted with external entities



MONITOR COMPLIANCE

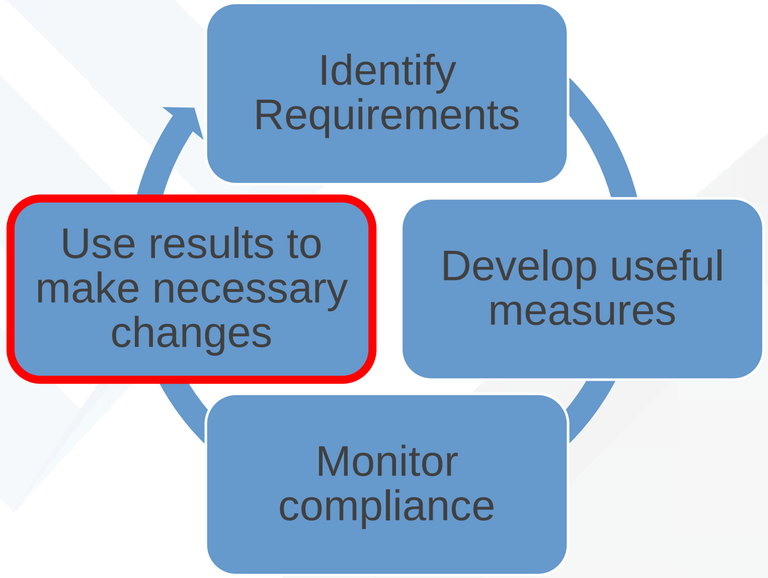
- Use established and agreed measures to monitor the provider
- Measure regularly, not just at the start and end of the relationship





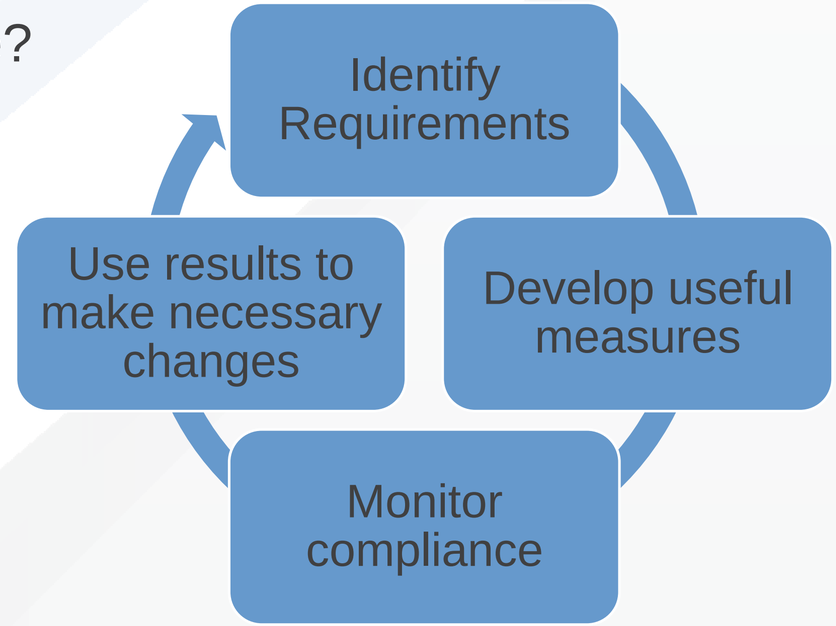
USE THE RESULTS

- Use measures to:
  - Ensure your relationships continue to meet your business needs
  - Identify opportunities to adjust the cybersecurity controls for the service
  - Evaluate your cybersecurity investment and identify where investments can change
  - Select third-party providers



EVALUATE THE PROGRAM

- Are we *actually* implementing the program?
- Are we detecting and correcting process exceptions?
- Is the external dependency management activity effective?
- Do we review the program with our stakeholders?
- Are we improving the plan as needed?



SUMMARY

- Reliance on external suppliers, vendors, and third-party entities have to be managed as a risk.
- SLAs can be leveraged to start the discussion.
- Make sure to specify at the “requirements” or “control objective” level of detail rather than specific controls.

Getting started is as simple as:

- taking an inventory or your current providers
- assessing their importance
- and reviewing current SLAs to see what might be missing

Resources

- NIST Special Publication 800-35-Guide to Information Technology Security Services
- COBIT 5
- ITIL
- ISO/IEC 27002:2005
- FEDRAMP
- Cloud Security Alliance
- CERT Resilience Management Model

Q & A

MIS|TI™ PRESENTS

InfoSec World

Conference & Expo 2018

THANK YOU

PLEASE FILL OUT YOUR EVALUATIONS!

Summer Craze Fowler

Technical Director (Carnegie Mellon | CERT)

@sumfowler

Matthew J. Butkovic

Technical Manager(Carnegie Mellon | CERT)