2019 Boston

ANNUAL CONFERENCE
& SHOWPLACE

SOC, ISO, and Additional Cloud Compliance and Assurances | RIHousing

Carl Rotella, Director of Information Technology | RIHousing

NCSHA

SOC, ISO, Cloud Compliance 2019

- Review the State of Regulations
  - Soc 1,2,3 ISO, Cloud [GLBA, GDPR...2019]
  - Soc 1, SSAE 18
- What RIHousing.com did to align the Business to SOC?
- What to focus on?
- What processes are reoccurring to at audit RIHousing?
- Check off list that may help you!

SOC 1®– SOC for Service Organization: ICFR

Report on Controls at a Service Organization Relevant to User Entities' Internal Control over Financial Reporting

SOC 2® - SOC for Service Organizations: Trust Services Criteria

Report on Controls at a Service Organization Relevant to Security, Availability, Processing Integrity, Confidentiality or Privacy

SOC 3®— SOC for Service Organizations: Trust Services Criteria for General Use Report

These reports are designed to meet the needs of users who need assurance about the controls at a service organization relevant to security, availability, processing integrity confidentiality, or privacy, but do not have the need for or the knowledge necessary to make effective use of a SOC 2 Report. Because they are general use reports, SOC 3 reports can be freely distributed.

Regs

- SOC 1,2,3 Sarbanes-Oxley Act 2002 SOX [SSAE 18]
- GLBA Gramm-Leach-Bliley Act [Financial Modernization Act]
- ISO International Standards Organization
- HIPPA Heath Insurance Portability and Accountability Act of 1996
- GDPR General Data Protection Regulations 1998
- CCPA California Consumer Privacy Act 1/1/2020

GDPR Final Text, Council of the European Union. http://data.consilium.europa.eu/doc/document/ST-5419-2016-INIT/en/pdf (accessed December 2017).

Key Question Response SOC Report Type Required

- Will the report be used by your customers and their auditors to plan and perform an audit or integrated audit of your customer's financial statements? Yes SOC 1® Report
- Will the report be used by your customers or stakeholders to gain confidence and place trust in a service organization's systems? Yes SOC 2® or SOC 3® Report
- Do your customers have the need for and ability to understand the details of the processing and controls at a service organization, the tests performed by the service auditor and results of those tests? Yes SOC 2® Report

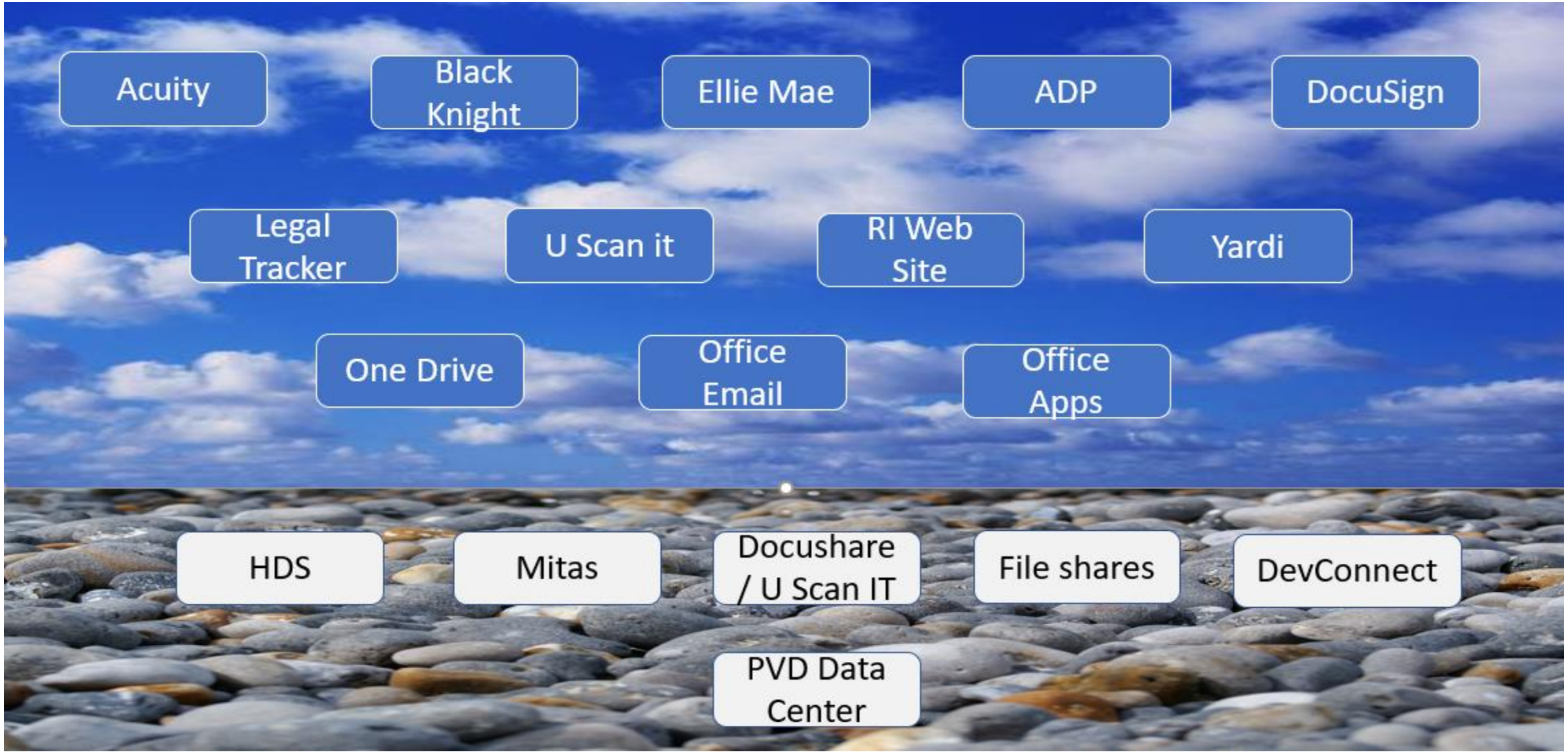
What did RIHOUSING do to align SOC?

- Review the old audits and all consultant reports
  - **Define the Goals/Time** of what is going to take place over the next 6-9 months
- Set the **Executive Team** agenda to match budget
  - Assets, procedures changes, reporting times
- Define what is **first** and what is next, do what we can in parallel
  - Architecture, processes, and SOP's [Do what you say]
  - SECURITY Model vs. Events
    - Protect the clients, business, employee [Test it]
  - Reported monthly to Executive team, how it is going and the help you need
- Involve the Auditing team on updates
- Use the check off list to define "done"

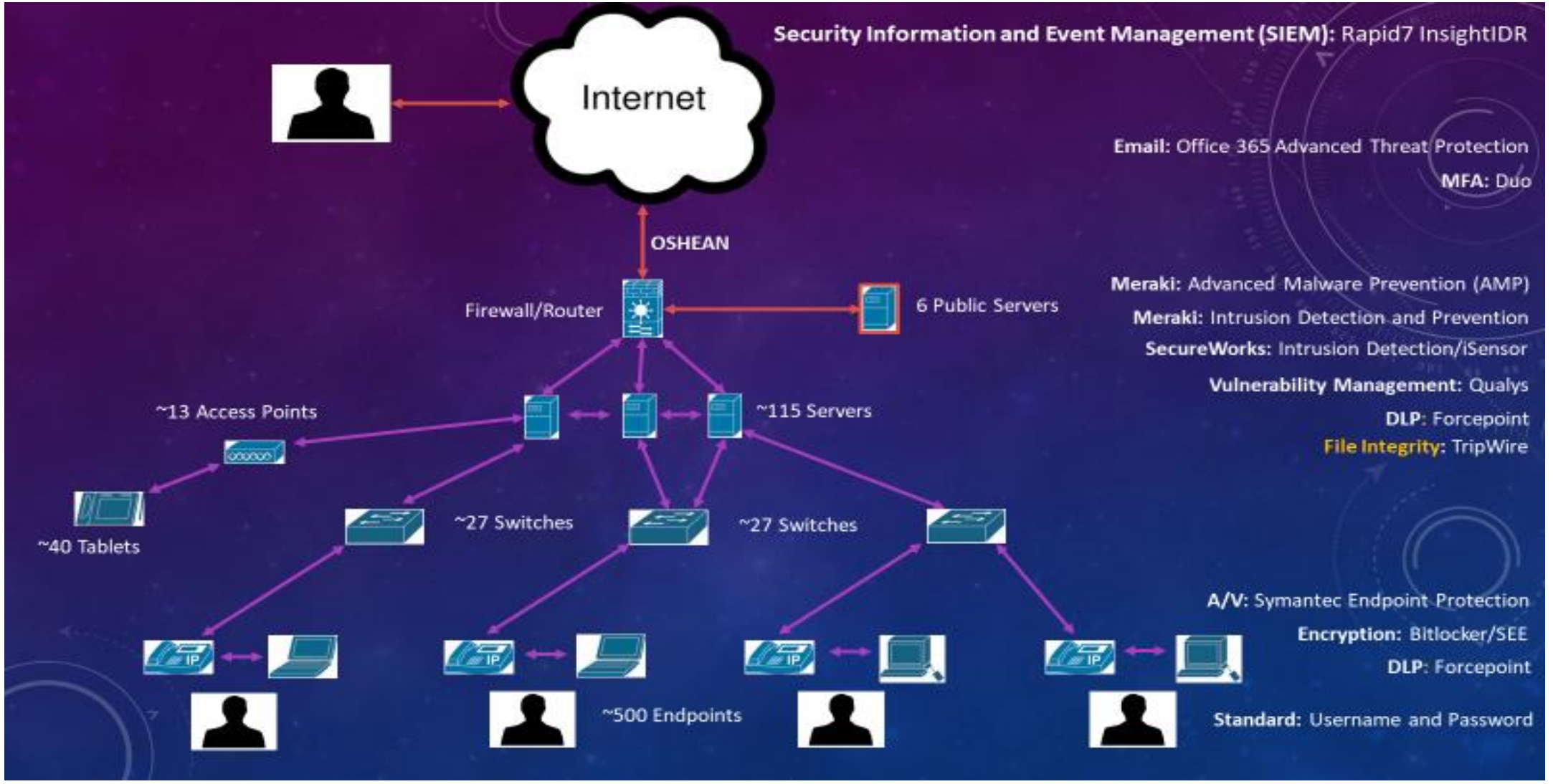
What RIHousing Focused on?

- **IT Org** – Why; because you can control it, if we do it then other employees will
- **Your Policy, Procedures,** SOP's must align. [Do what you say]
  - Re-policies if needed, Procedure do not have wait for policy sign off, get ready for audit
- **Create the Top level architecture drawings:**
  - Current and Future to locate where you are and where you are going.
- **Security Model** from the Top to the Bottom that Executive team can see and touch
- Backup and Recovery processes are working
- Audit with business teams, outside team, and experts
- eDiscovery process, tools, and controls must be in the make over

Top Level – Where are the app's



Security Protection Model



Cloud Partners

- Carrier Partner – Your internet and MPLS Partners
- Google
  - https://privacy.google.com/businesses/compliance/#!?modal_active=none
- AWS
  - https://aws.amazon.com/compliance/programs/
- AZURE
  - https://servicetrust.microsoft.com/Search?command=Download&downloadType=Document&downloadId=4beacf76-58b7-4337-bbb0-e85c83790fe1&keyword=GLBA&pageNumber=0&pageSize=30&searchType=Document

What is the plan for 2020?

- We pass the 2019 July audit
- We are reviewing all the Security application based on PEN TEST
  - Next PEN TEST 11/11/2019 – Second one this year
  - changes are planned for Q1 2020
- Continue to move Business APPs to Cloud after business review
  - We are 61 % done what we planned to move
  - We are reviewing all the on-prem apps to make sure this is correct place for them
- Next Audit
  - Dec 2019
  - Feb 2020

Links

- GLBA
- https://www.ftc.gov/tips-advice/business-center/guidance/how-comply-privacy-consumer-financial-information-rule-gramm

- SOX 1,2,3
- https://uslaw.link/citation/us-law/public/107/204

- Why CCPA
- https://oag.ca.gov/privacy/ccpa

- Bill of CCPA
- https://leginfo.legislature.ca.gov/faces/billTextClient.xhtml?bill_id=201720180AB375