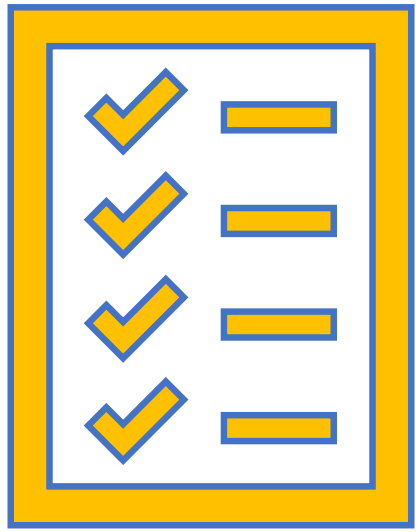
Beyond Compliance
Supplier Assessment Security Considerations

Terence Runge

Head of Security

Illumio



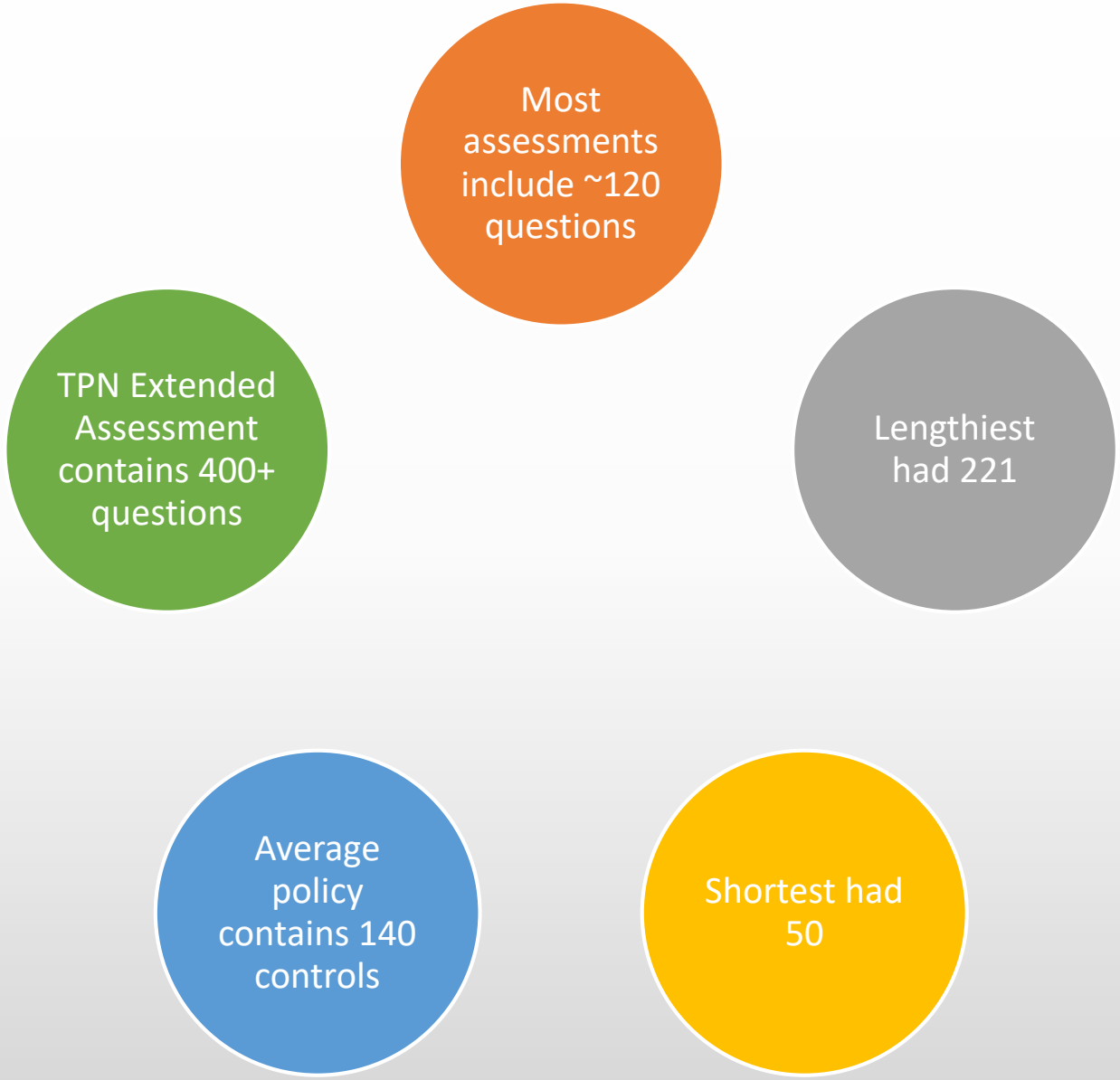
Terence Runge

Head of Security @Illumio

Silicon Valley industry veteran for 20+ years

Former Blackbaud, Salesforce, Symantec, Napster, LogicTier

Active in ISC2, ISACA, IAPP, CA-CSAP, OWASP, Stanford Cyber Initiative



Customer Assessments @Illumio

Past 12 Months

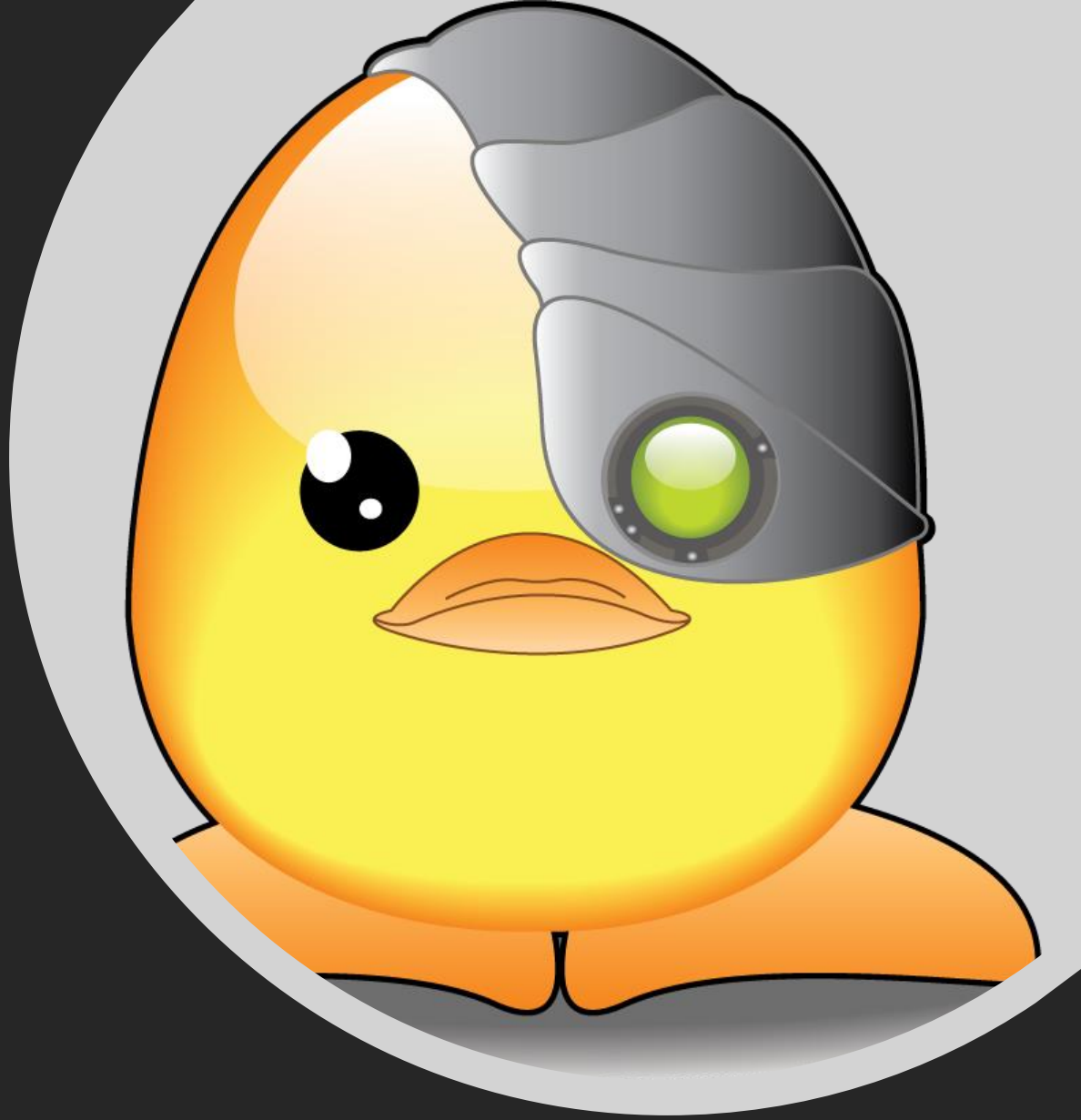
Compliance Oriented

- Closely resemble ISO 27001 standard
  - ❑114 controls in 14 clauses and 35 control categories
- Other normative references include 16 CFR Part 314, HIPAA, GLBA, SOX, PCI DSS, SEC, SSAE 16 & ISAE 3402
- <10% conducted independent penetration testing
- No Red Team, Threat Hunt, Compromise Assessment, or Threat Intelligence Feed questions

Odd Ducks

- Questions that focus on administrative process rather than control performance
- Questions that don’t make sense

  Does the third party comply with 1-200 ABC/AMBCDE Standards for Third Party Connectivity Policy?
- Control statements that aren’t actionable



Control Statement – not actionable

Encryption Policy can be found in Lotus Notes. All information that is determined to be confidential or nonpublic and that is transmitted or placed on removable media, must be encrypted, using either an authorized standard cryptographic technology or a technology that is explicitly approved by the Chief Information Security Officer.

- No access to customer's Lotus Notes
- Data classification labels not defined
- Authorized cryptographic technology not prescriptive
- Which CISO

Well Written Control

All applications which provide services over the internet and all devices which are directly connected to the internet must undergo penetration testing.

Penetration tests:

- ✓Should be performed by an independent organization.
- ✓Must be conducted prior to release into production.
- ✓Must be conducted for major changes.
- ✓Must include a vulnerability scan of the external IP addresses
- ✓Findings rated as “high” or “critical” must be resolved and re-tested

Security Assessment Considerations

1. People are part of the product
2. Open source software vulnerability management - CVE impact
3. Source code repositories & build environment access control & audit
4. Platform dependencies – *aaS outage impact; platform security
5. Suppliers of suppliers– access to information; vetting; supplier changes
6. Product security SLA's – timing; security hot fix triggers
7. Alerting & notifications – public blog post or customer only advisory
8. Coverage and effectiveness of security controls
9. Support portal security – data persistence; access controls; encryption
10. Threat modeling – is it done; when; which framework or methodology
11. Threat Hunting – frequency; type; automated or human; environment
12. Red Team – how often; target types; internal or 3rd party team

Thank you!

Terence Runge
Head of Security
Illumio
terence.runge@Illumio.com