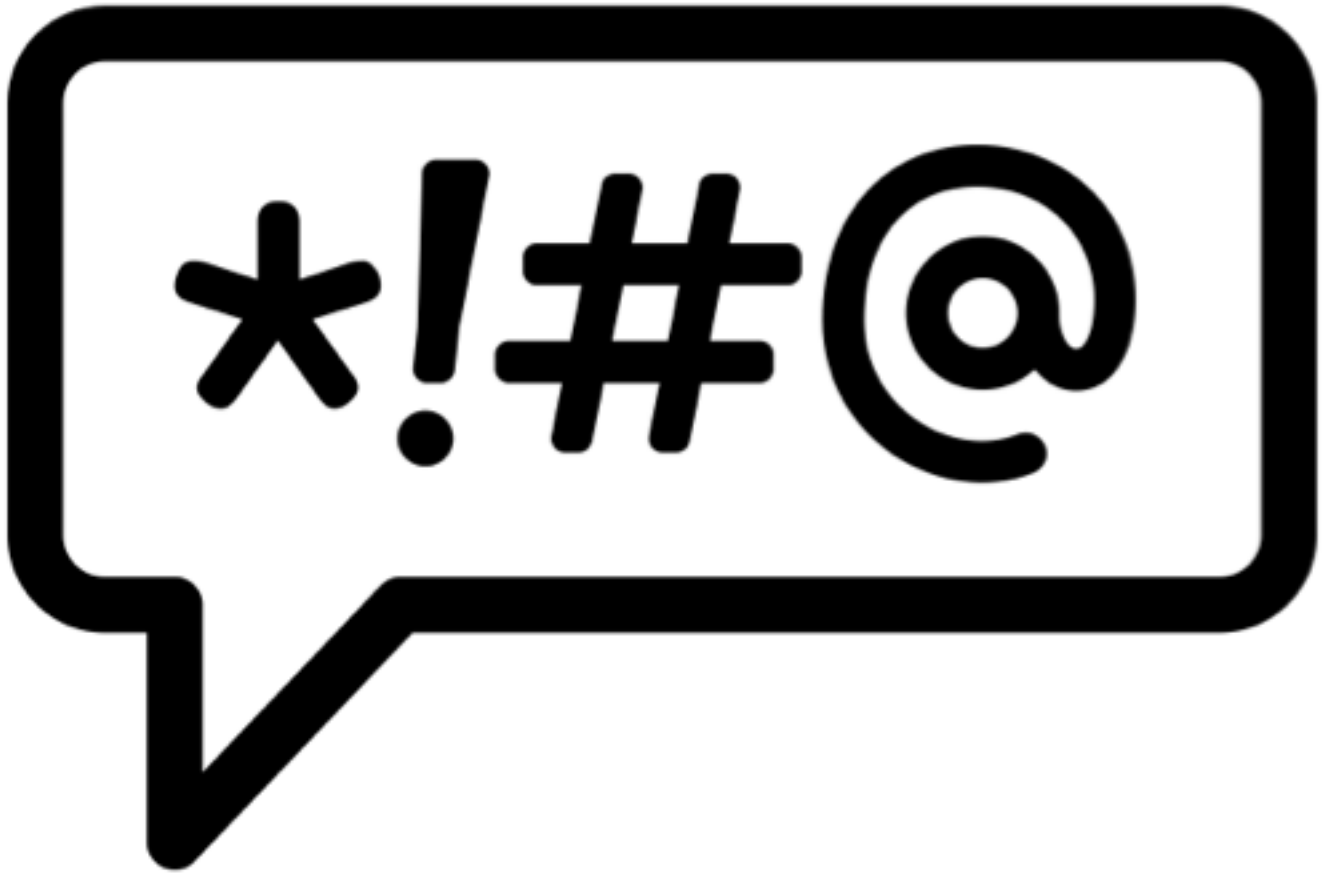
Security to make the CFO Happy

Adam (@sneakernet72), Engineer



curse by Nick Bluth from the Noun Project

NIST SP 800-53
DoD 8570/DoD 8140
CUI - NIST SP 800-171
DFARS clause 252.204-7012
CMMC/CMMI

Whose ears are burning?

- The entire DoD Supply Chain for starters
  - 20,000 Prime contractors
  - 300,000 Subcontractors

Created by Gan Khoon Lay
from Noun Project

Targets …Victims?

- Business Development
- Program Managers
- Finance, QA, and IT managers

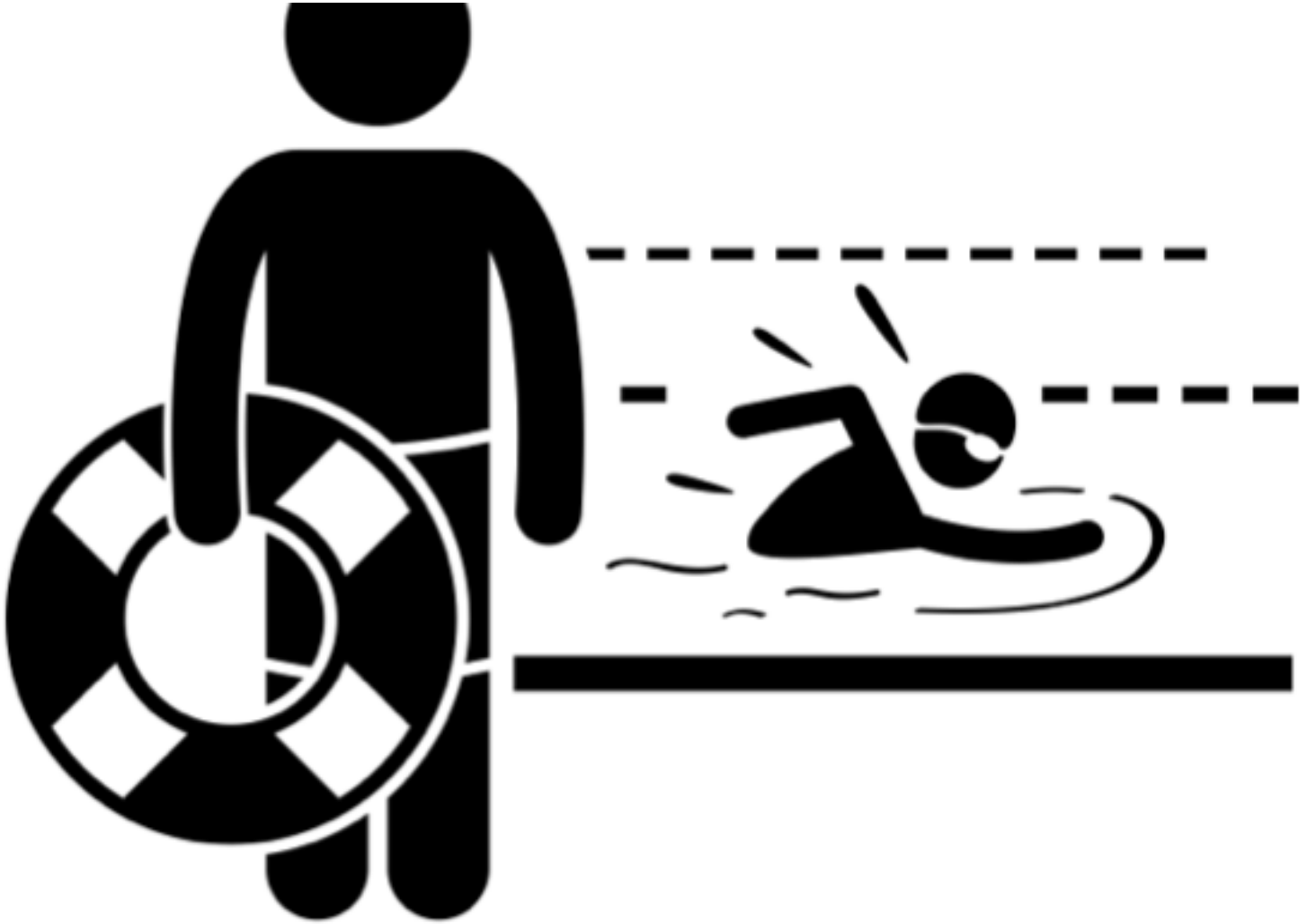
Created by Luis Prado
from Noun Project

Threat Vectors

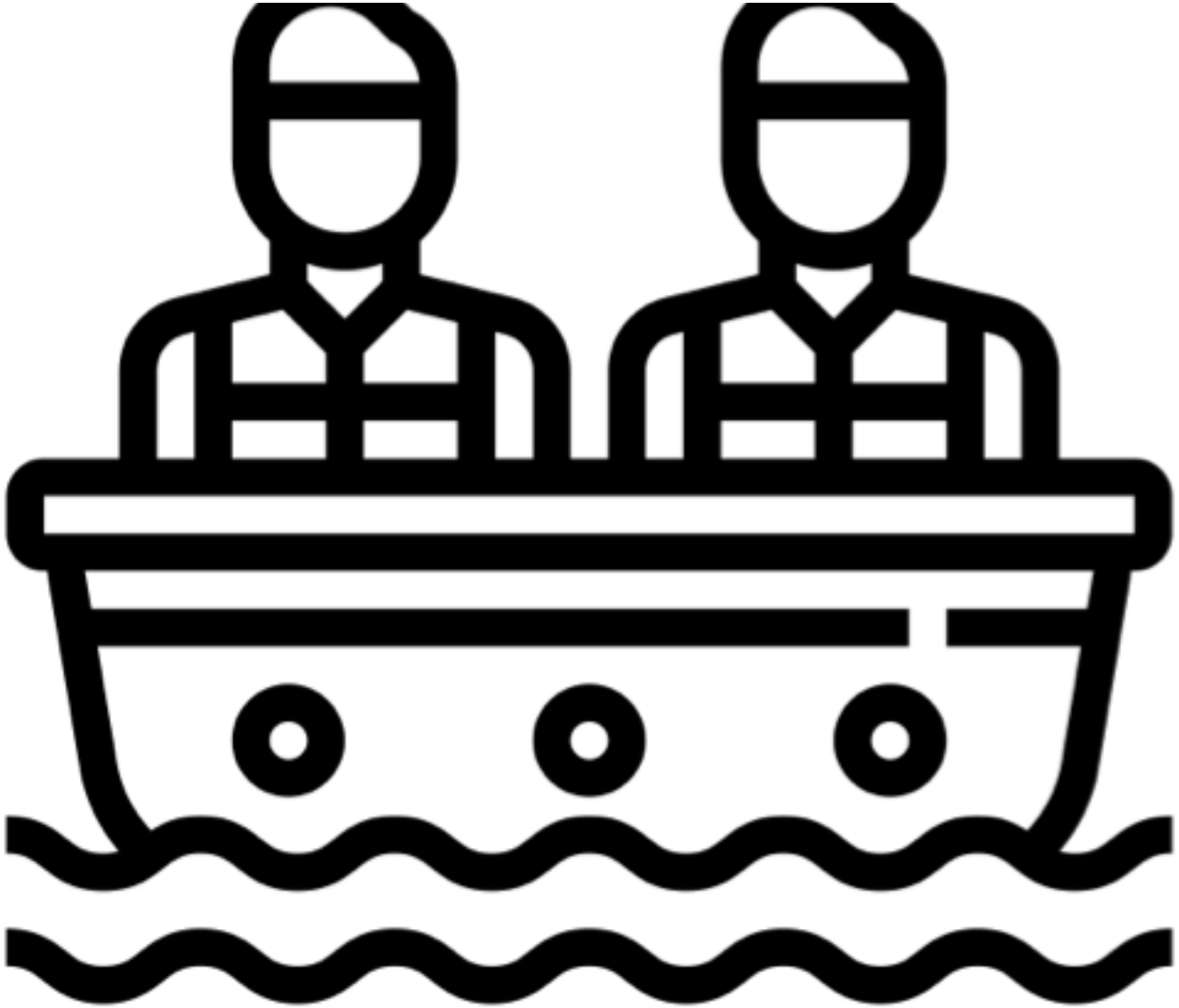
1. Business
   - Data call
   - RF(I|P)
   - SOW/SSOW
2. Organization
   - Certifications
   - Audits
3. The Questionnaire

Pain points

1. Poor communication
2. Security language
3. Unplanned work
4. Unfunded mandates



Created by Gran Khoon Lay From Noun project



Created by Eucalyp from Noun Project

Created by BomSymbols
from Noun Project

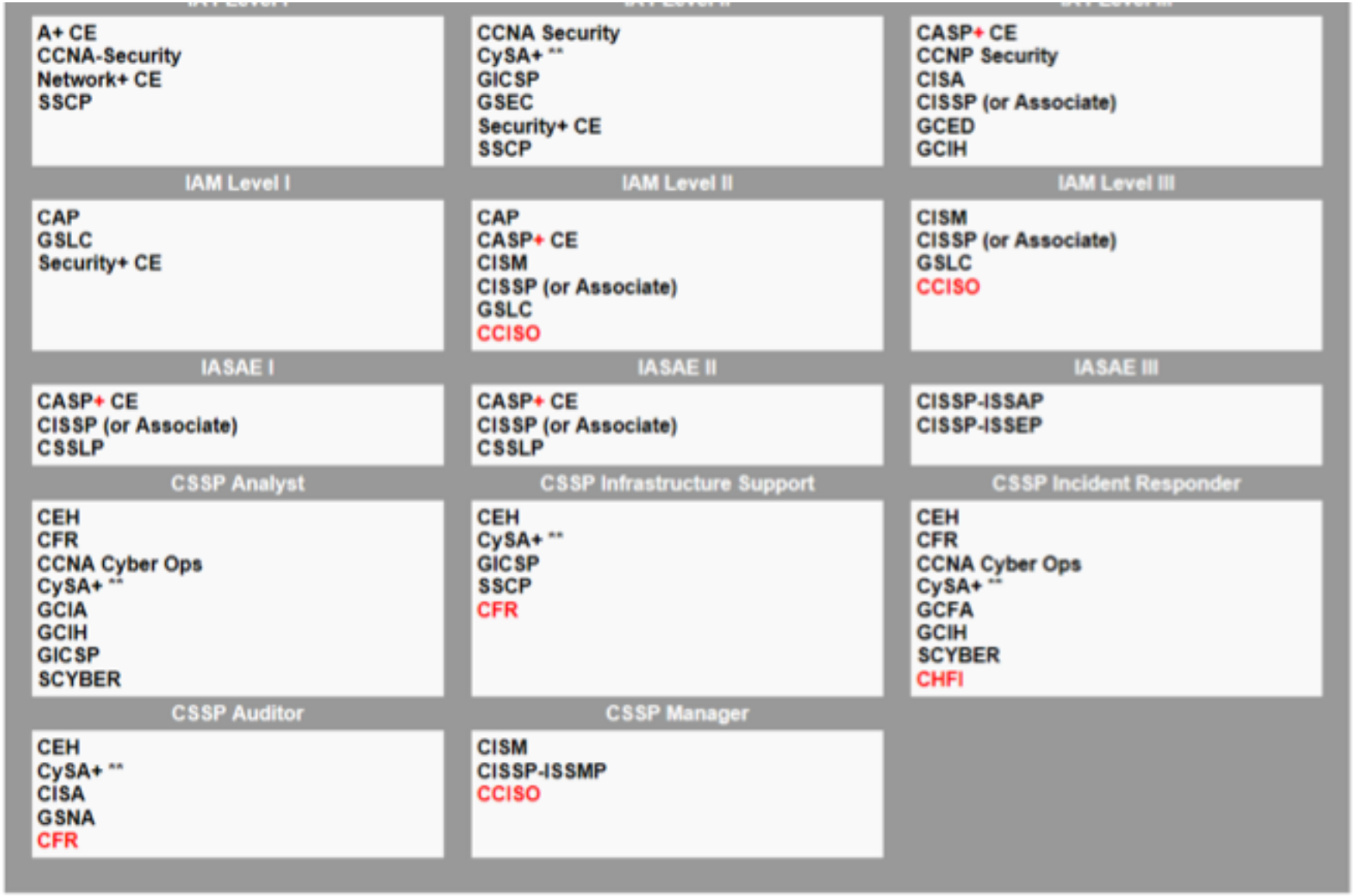
Signs of ~~Old Age~~ Security Maturity

1. Awareness
2. **Literacy**
3. **Engagement**
    1. Tactical
    2. Strategic
4. **Security is a measurable cost**
5. Compliance is a byproduct
6. Security enables quality

History Lesson

History Lesson

- Sarbanes-Oxley
- CMMI / ISO9000
- RMF transitions
- The Phoenix Project (Fiction)



Strategic training dollars

Strategic training dollars

- Compliance dominoes
- Maximize existing contracts

Relationships

Relationships

Created by Icon Lauk
from Noun Project

Relationship #1: Purchasing

Created by ProSymbols
from Noun Project

Relationship: Purchasing

- More than just holding activation keys and accepting PRs …
- Make connections with the right vendor contacts
- Save you from making a purchase the larger org already has

Oh, btw…

- Those purchasing folks – they are super helpful for getting a start on addressing supply chain risk management too.

Relationship #2: Eng & IT

Created by Gregor Cresnar
from Noun Project

Relationship: Engineering and IT

- Join forces around a common security tool or SIEM (Security Information and Event Management)
- SIEM because metrics

Relationship #3: HR

Created by Maxim Kulikov
from Noun Project

Human Resources

- Answer the data call with talent DB
- HR can adapt edu reimb policies to include cyber training.
- Win for HR because the new policy helps attract new talent
- Win for YOU - You get more allies.

Final thoughts

- Time is money
- Literacy saves time
- Team effort
- Don’t throw the baby out with the bath water
- Security enables quality

Questions?

Citations

- https://www.jdsupra.com/legalnews/cost-of-cybersecurity-compliance-now-an-61380/
- https://federalnewsnetwork.com/reporters-notebook-jason-miller/2019/06/why-dods-decision-to-make-cybersecurity-an-allowable-cost-matters/
- https://federalnewsnetwork.com/federal-drive/2019/07/new-rule-about-protecting-controlled-information-to-affect-contractors-other-govt-partners/
- DoD 8570 Chart: https://www.giac.org/certifications/dodd-8570
- Protecting CUI: https://csrc.nist.gov/publications/detail/sp/800-171/rev-1/final
- DFARS clause: https://www.acq.osd.mil/dpap/dars/dfars/html/current/252204.htm#252.204-7012
- CMMC: https://www.acq.osd.mil/cmmc/index.html
- CMMC listening tour: https://www.acq.osd.mil/cmmc/listening-tour.html

Backups

DaaS

- CONOPs
- User/Admin Guides
- Plans!!!
- ~~Code~~ Documentation reuse