ASIS School of ESRM

Session 3 - Continuous Monitoring and Improvement

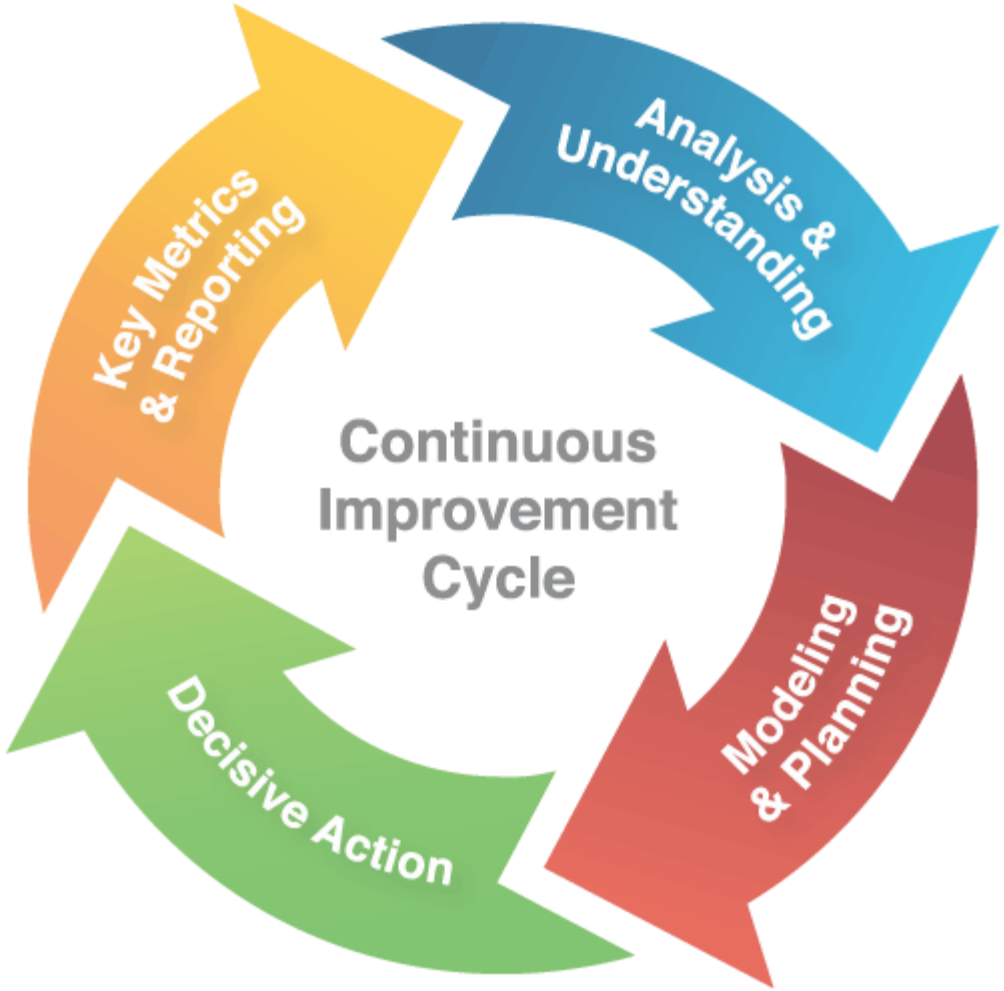
Continuous Improvement

Sources of Continuous Improvement

- **Security risk analysis**
- Incident **Response**
- **Investigation**
- **Information Sharing**

Benefits of Continuous Improvement

- Enhanced **communication**
- Cultivating **relationships**
- Monitoring & communicate of **residual risk**
- **Informed, real time decision making**
- Building **trust**



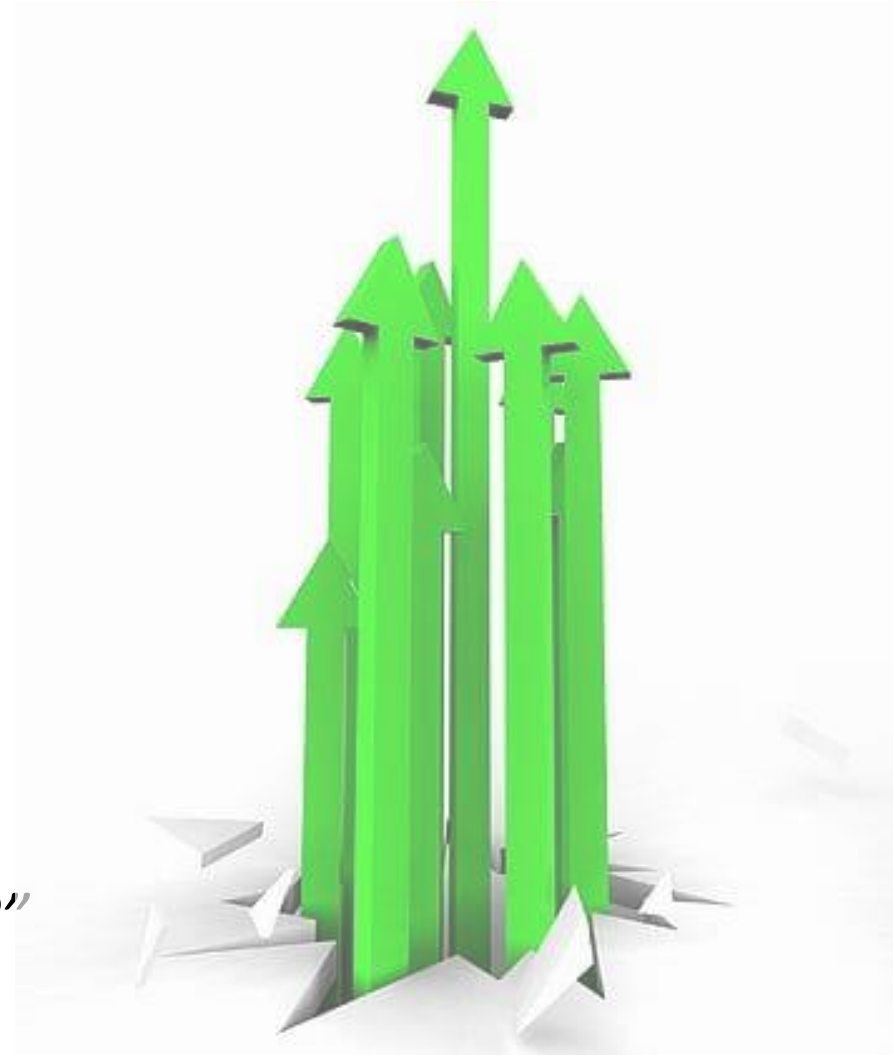
Continuous Improvement

Components of Continuous Improvement:

- Regular contact & **relationship building** with your business partners
- Ask if security is delivering **value**
- Continual **GAP analysis** & business **education**
- Conduct **incident debrief** and share results with **business partners**
- Conduct **tabletop exercises**

“Why do we do these things?”

“What risks am I mitigating by being here right now?”



So, now you can ….

- use a practical approach to **identify risk**
- build a security **risk register** as your **foundation** to ...
- develop effective **mitigation strategies** for each risk in the register and then ...
- **monitor & review** risk and develop adaptive mitigation strategies to support …
- continually **improve your security**

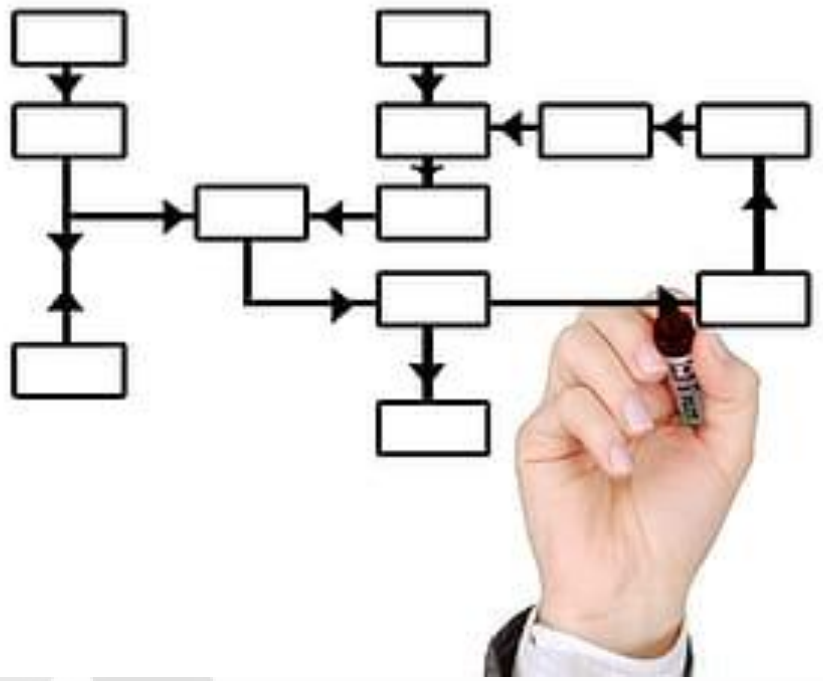
Now what?

Take it slow!

- No security management system can be changed “overnight”.
- Take a **phased approach**.
- Try a **test case** first.
- Remember, you still have to “**do security**” whilst you set the stage for an ESRM approach.

Take Stock of Your Current Security Activities

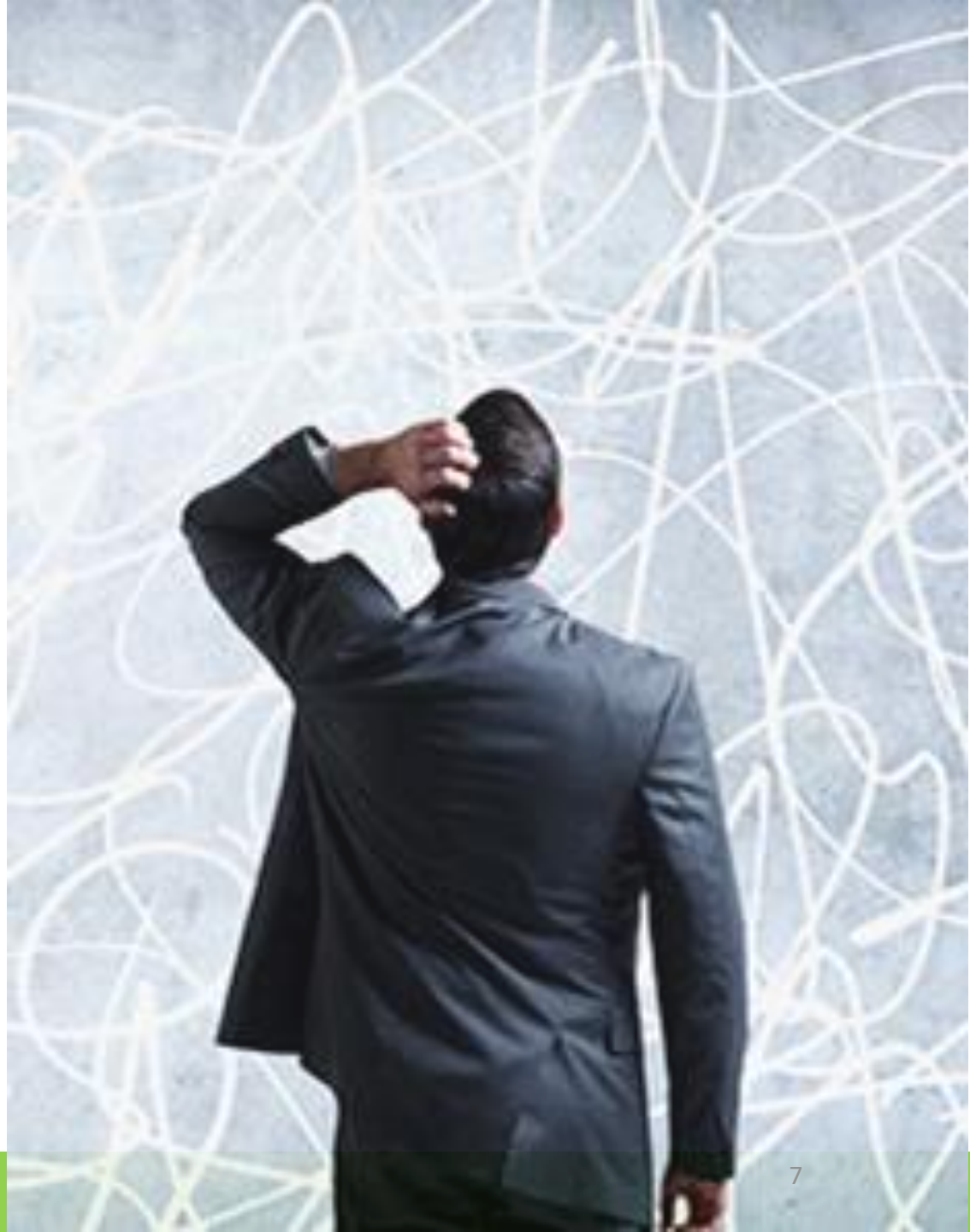
- What are the **current security tasks** in your organisation?
- **Who is responsible** for carrying out these tasks? (HR, FM, Audit)
- Are these **tasks specific** to particular business **assets/objectives**?
- Can you **identify the security risks** that the tasks are mitigating?
- Can you **identify the asset owners** & other key **stakeholders**?
- Where does each existing security task fit in the **ESRM cycle**? Is it **assessing** risk? Is it **mitigating** risk? Is it driving **awareness** of risk?



Understand Your Own Viewpoint on All Current Security Activities

- **Why** are you doing what you are doing?

- **What do YOU THINK is critical** for your organization's security program?
  - Why do you think that?
  - Is there a business driver?
  - Is the activity "what we have always done"?
  - Who is the risk unacceptable to? You? Or Your Stakeholder?



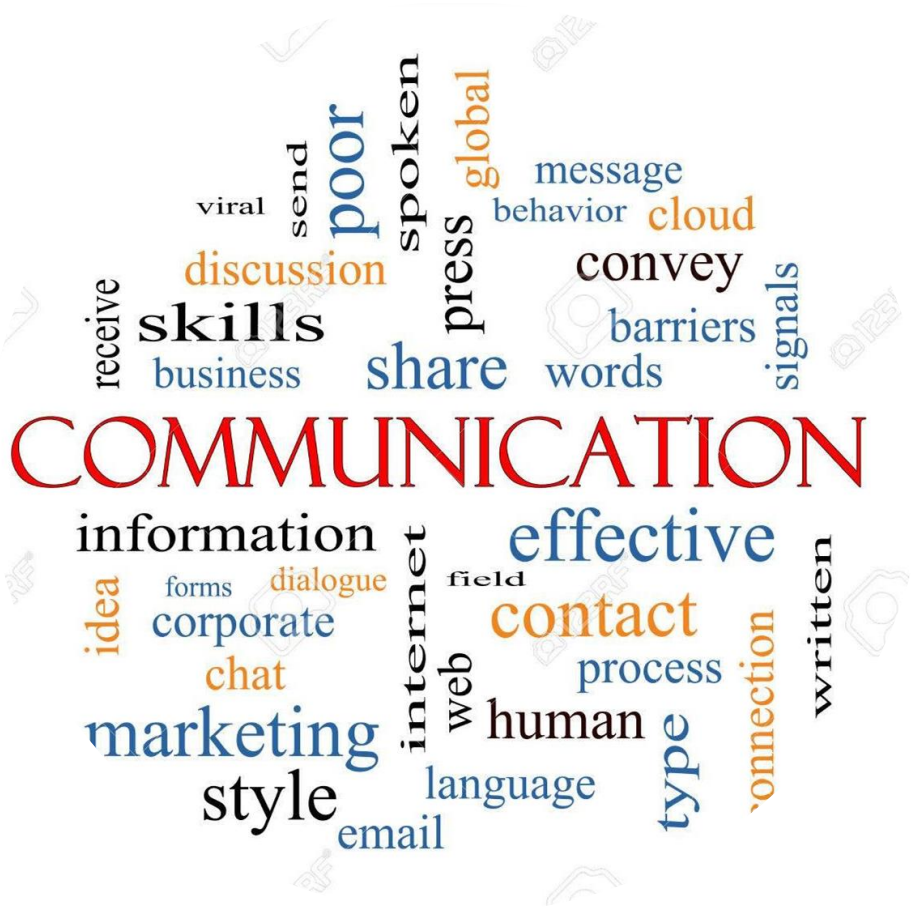
Start a conversation ...

“Tell me about your role. How can security help you manage your challenges?”

- Business leaders
- Asset owners
- Employees
- Stakeholders
- Customers
- Suppliers
- …

Active engagement with the business

- **Educate** internal business partners on the realistic impacts of security risks to assets under their control.
- Present potential **security strategies** to **decision-making business leaders** to mitigate those impacts.
- **Implement** the business leader's security risk mitigation choice, driven by business risk tolerance.



ESRM Toolbox

ESRM Maturity Model

ASIS INTERNATIONAL®

Enterprise Security Risk Management (ESRM) Community

MATURITY MODEL (PROOF OF CONCEPT) 2021

By Paul Mercer, Chair of ASIS Maturity Model Team

ASIS ESRM Community

ASIS SUBJECT AREA COMMUNITY

Enterprise Security Risk Management (ESRM)

https://community.asisonline.org/communities/ESRM

Questions…?