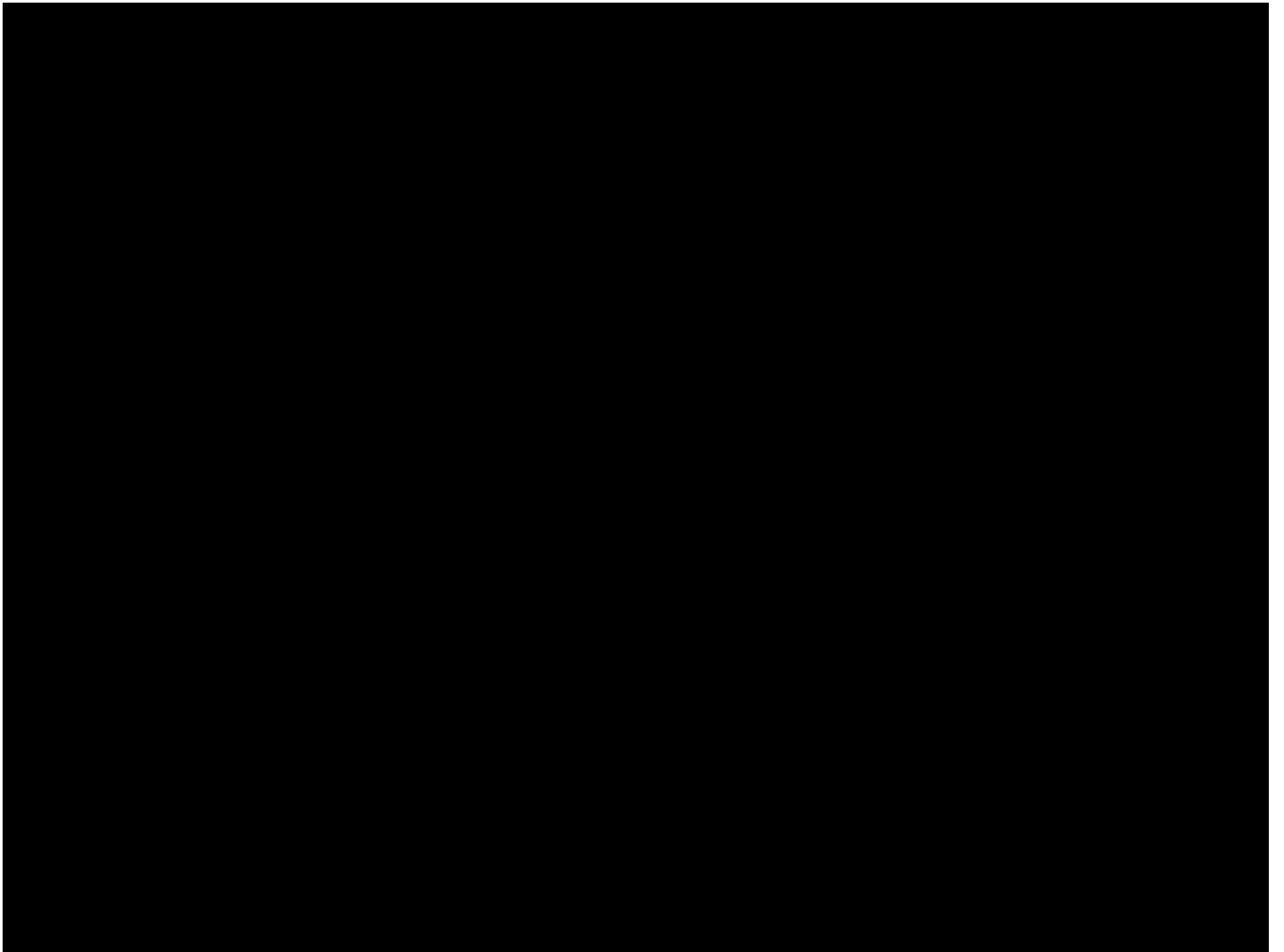




Integrating IT Security into Business Projects: A Case Study

Tim Cook



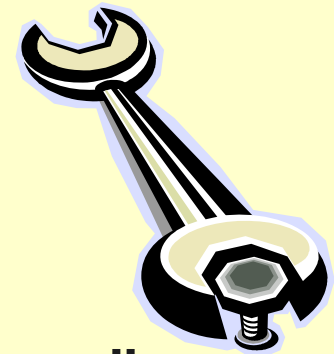
Hypothesis



- Business doesn't want poor security outcomes
- Business expect subject matter experts (SME) to manage security issues and risk on their behalf
 - at minimum cost
 - maintain risk at acceptable level (to business)
- Best way to do this is to 'integrate' security into all aspects of the business
- How SME do this is up to them!

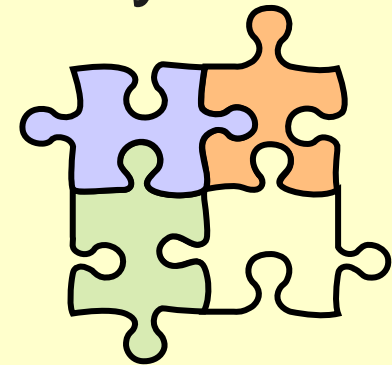
Bolt-On Security - 'The Problem'

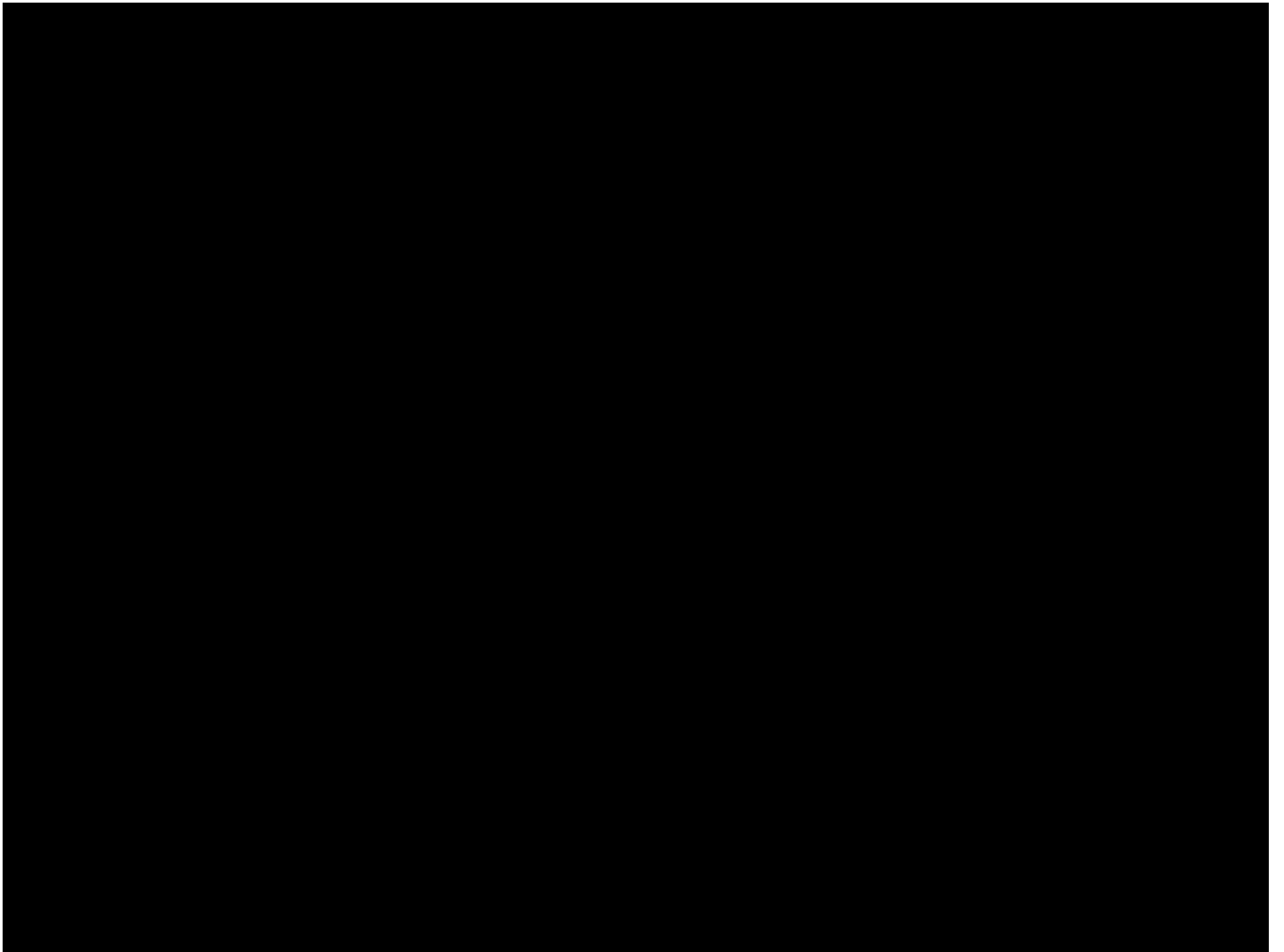
- Vulnerability audit then 'bolt-on' fix
- Assumption is that all flaws are identified
- Does not wholly address security architecture issues
- Technology focus
- Culture of "security is not my problem"
- Outcomes = frustration and through-life costs



Built-In Security – ‘The Solution’

- Policy, architecture and design centric
- Reduces cost
- Joint ownership of security outcomes
- Risk-based focus – balances security and functionality
- Holistic – not just technical
- Outcome = integrated security







Project Security Governance Framework

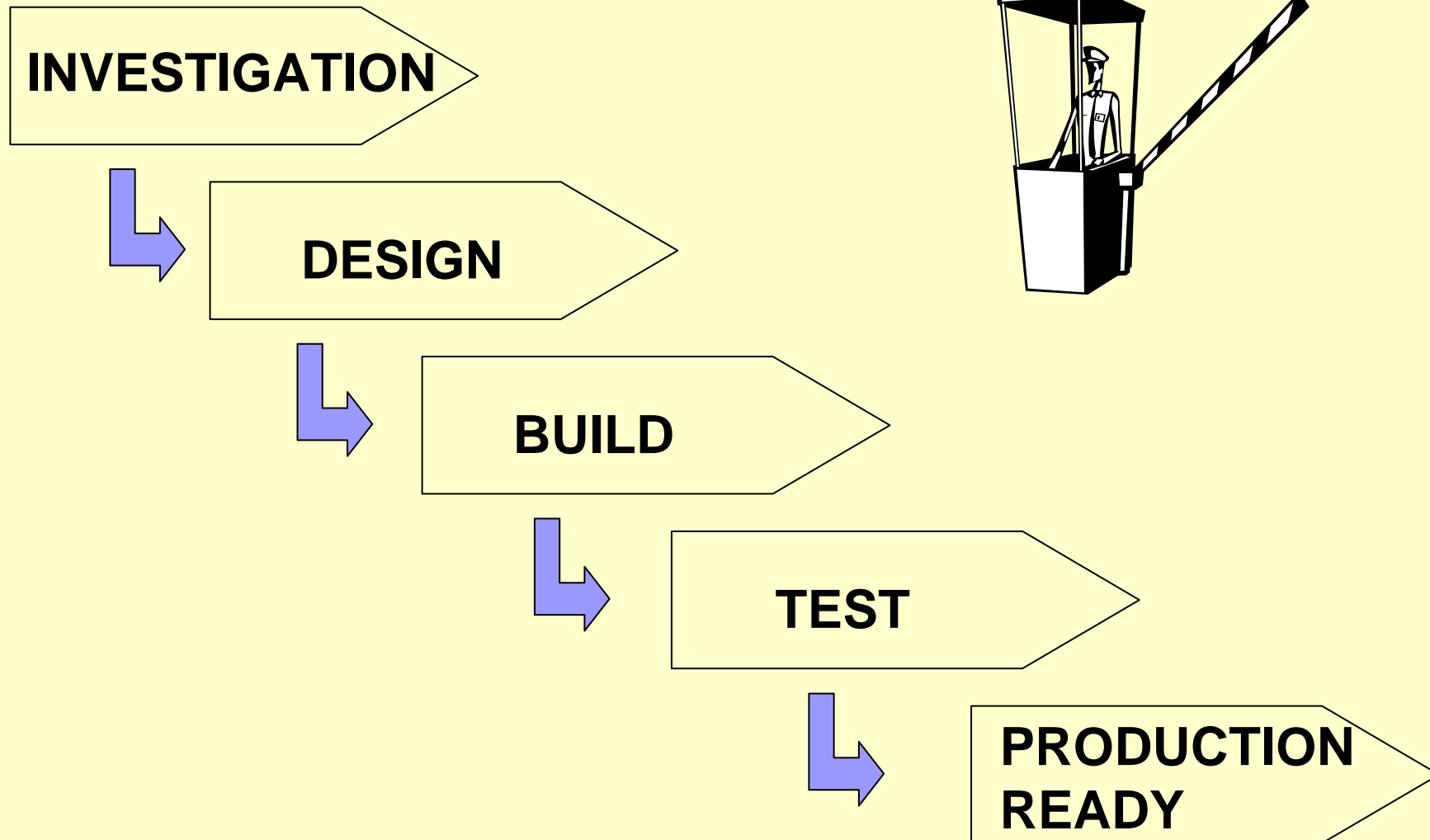
- Policy Framework

- ☐ 'Design Principles for Secure Systems'
- ☐ 'Security Requirements for External Suppliers'
- ☐ host of other policies and standards...

- Gating

- ☐ IT and Corporate Projects Division

Project Gates



Investigation Gate Criteria

- Have legal and regulatory requirements been identified?
- Have time and resources allocated for security tasks?
- Has the role of External Suppliers been addressed?
- Does the Conceptual Solution comply with security policies?



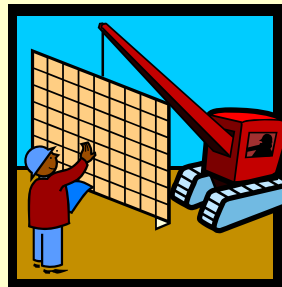
Design Gate Criteria



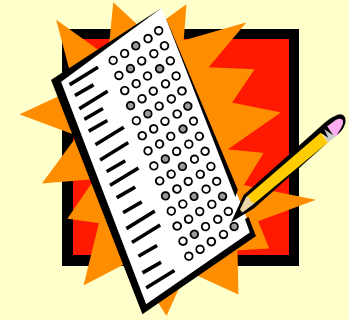
- Have the system 'hardening' documents been developed and endorsed?
- Has the Detailed Design included security technical requirements?
- Do the deliverables include security administration procedures?
- Does the solution use standard user IDs and passwords?

Build Gate Criteria

- Has 'hardening' been implemented?
- Have generic vendor passwords been removed?
- Does the build reflect the agreed security design?



Test Gate Criteria

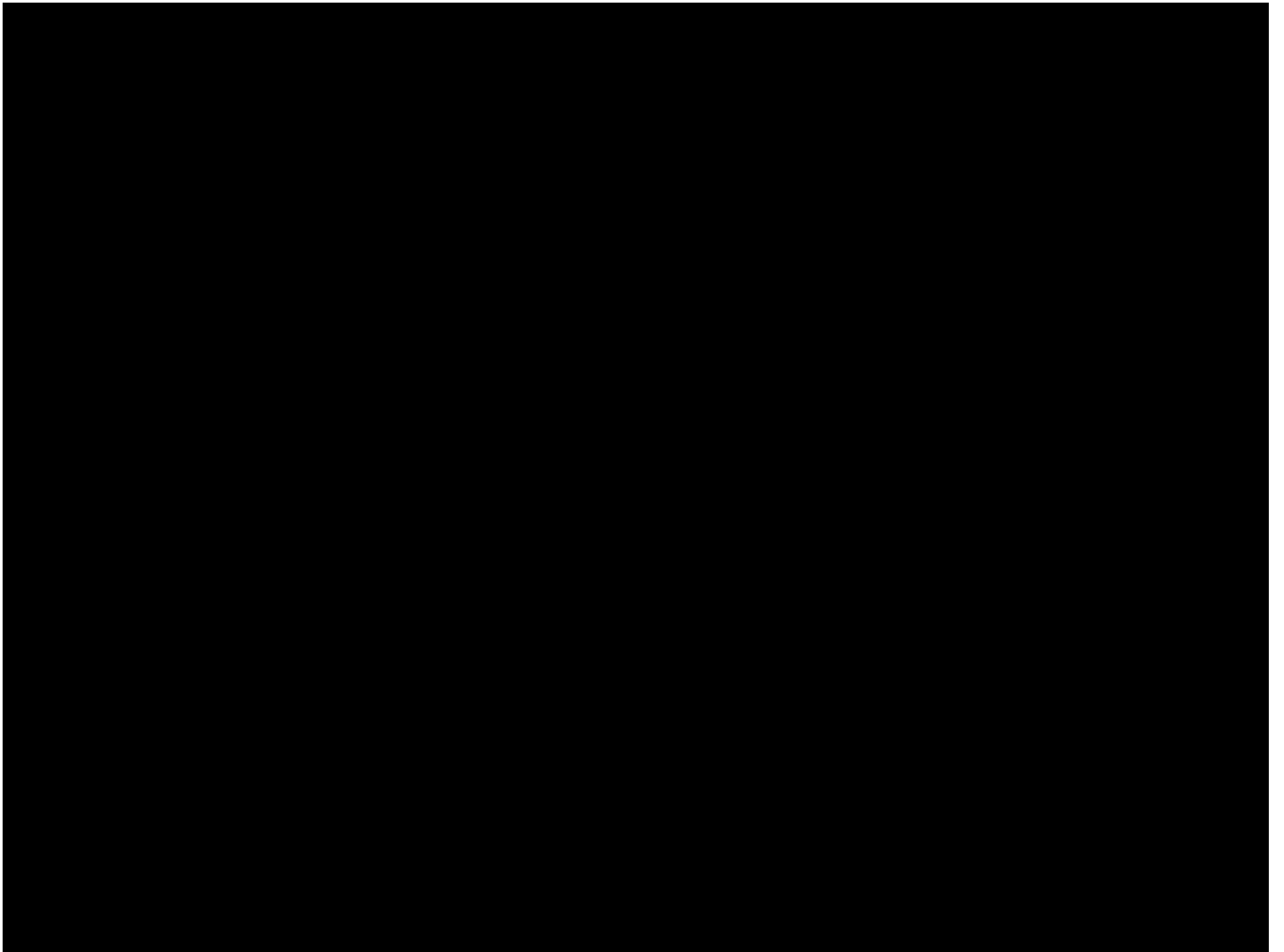


- Has a technical security audit been conducted?
- Are the appropriate application and user access controls in place for the system?
- Have required security procedures and training been provided to the security administration team?
- Have design documents been updated?

Production Ready Gate Criteria

- Is Manager IT Security happy?





Establishing the Framework

- Need 'allies' (especially architects)
- Big Bang
- Needs senior management support (IT and business)
- Painful





Outcomes

- Security requirements are transparent, repeatable and agreed up-front
- Security costs are known
- Risk-based decisions are made in advance
- Costs and risks of retro-fitting security are minimised
- IT security is integrated into every business project



Lessons

- Without policy, there is nothing to gate
- Gating enforces good PM practice
- Criteria needs to be tuned as the business changes (and technology to some extent)
- Criteria applied on a case-by-case otherwise becomes cumbersome
- Needs to align with corporate culture
- Tough decisions need to be made

