TRUSTED CHIPS

John BOGGIE Head of Cybersecurity Certification

DECEMBER 2022

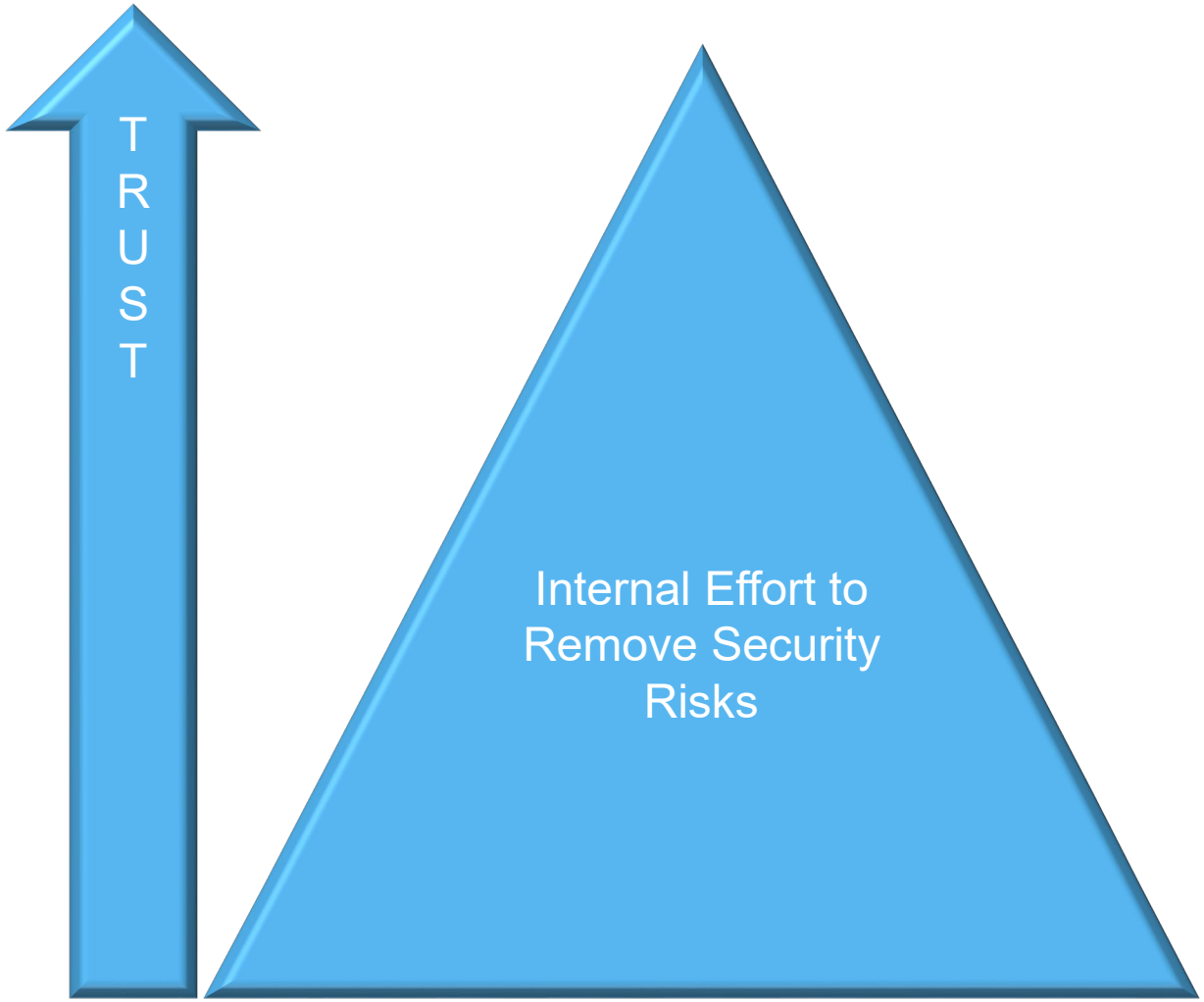
SECURE CONNECTIONS
FOR A SMARTER WORLD

EXTERNAL

TRUST IN A SUPPLY CHAIN PARTNER

Trust is mitigation of risk

If trust is low a company then has to spend internal effort to mitigate the risk



RISK MODEL FOR SEMICONDUCTORS AND COMMON MITIGATION

Back doors
- 3rd Party IP
- Malicious functionality Added during production

Bad Engineering
- Test Modes left unprotected
- Bad coding/design

Weak security
- Security as an add on
- Bypass of Security Features
- Spurious Security Claims
- Customer support on Security issues/Ownership

Cloning
- IP Theft
- Lack of digital ID

Trusted Supply Chains

Need to Know

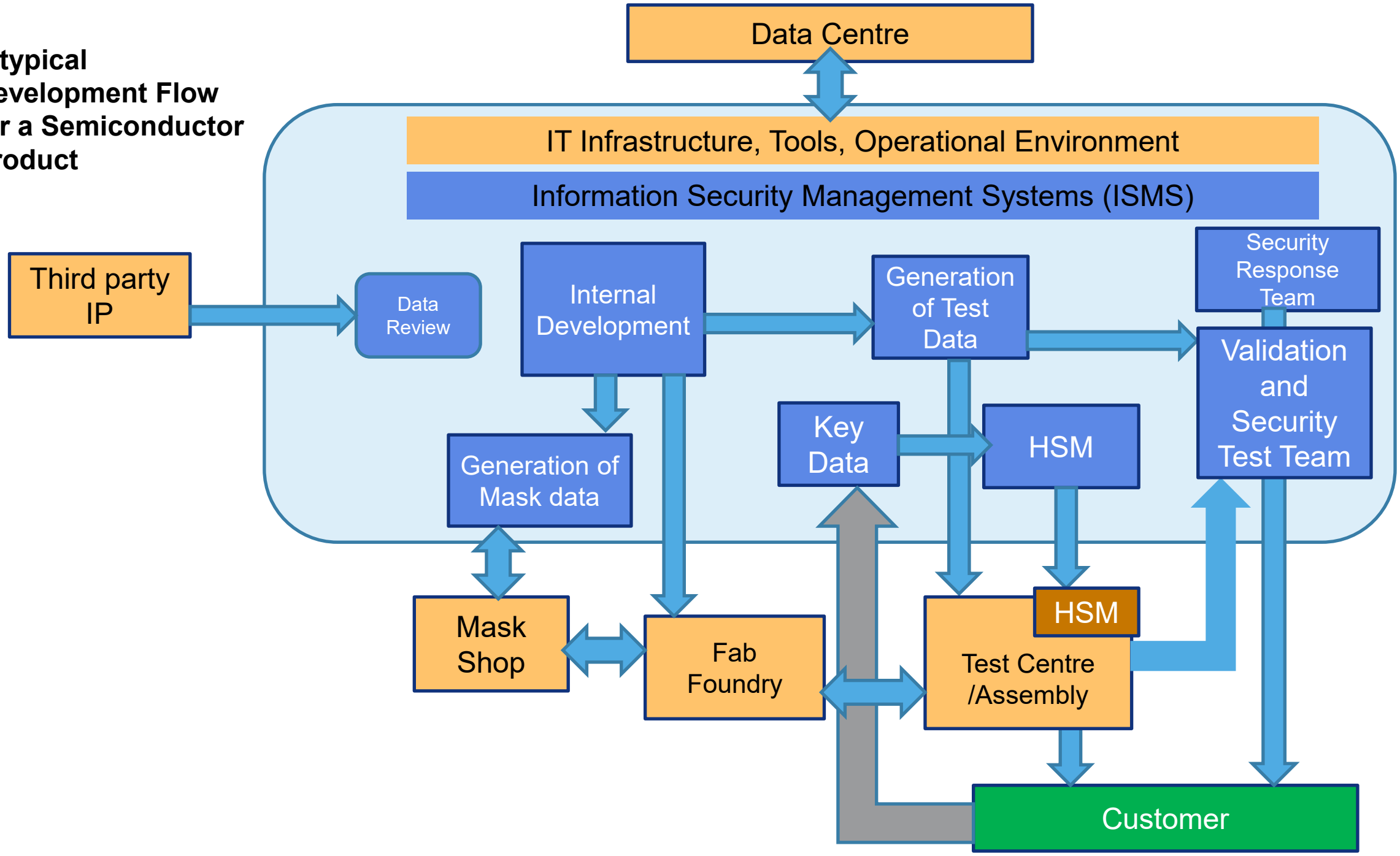
Security By Design

Security Testing and Verification

Strong Digital ID

Responsibility for Security Issues

A typical Development Flow for a Semiconductor Product



Risk Mitigation for External Partners

Data Centre

IT Infrastructure, Tools, Operational Environment

- External Suppliers Are Normally Security Audited by the Company Security Team
- They are often also audited and certified using The Common Criteria by the Governmental Cyber-agencies (ECCG)
- ISMS are usually certified using ISO 27001
- Third Party IP is audited for integrity

Third party IP

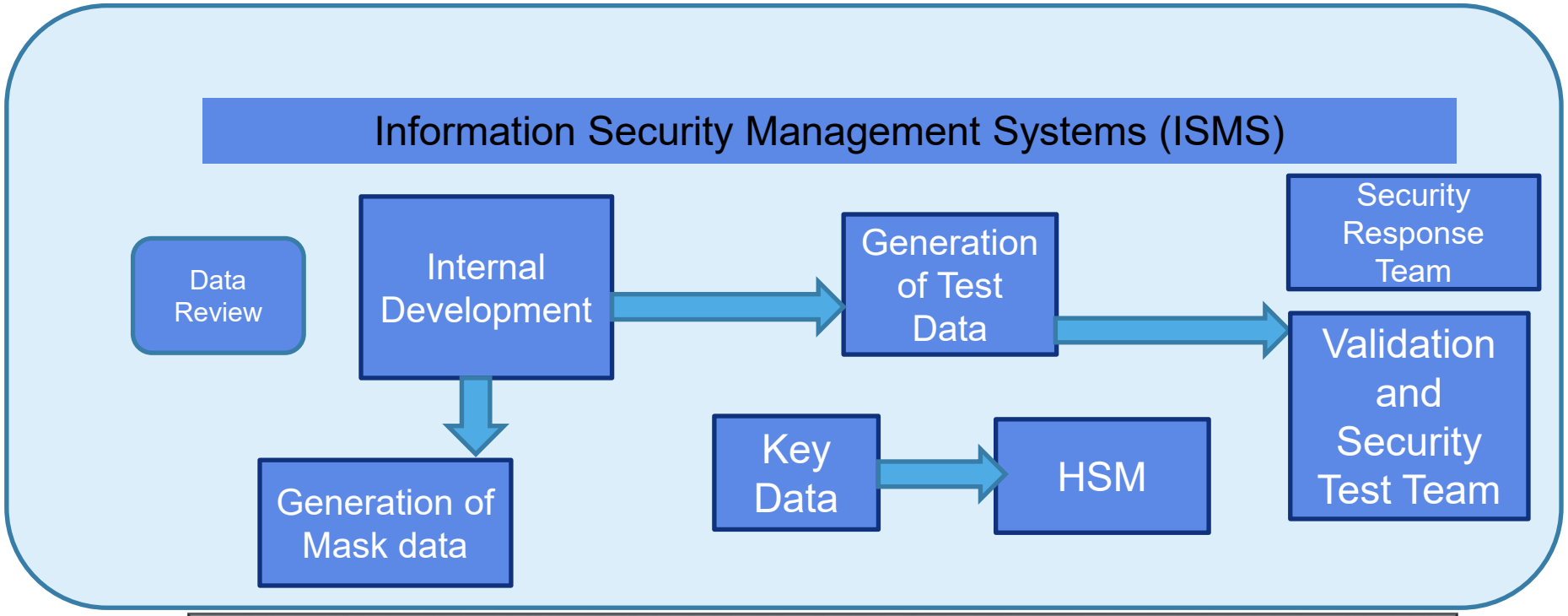
Mask Shop

Fab Foundry

HSM

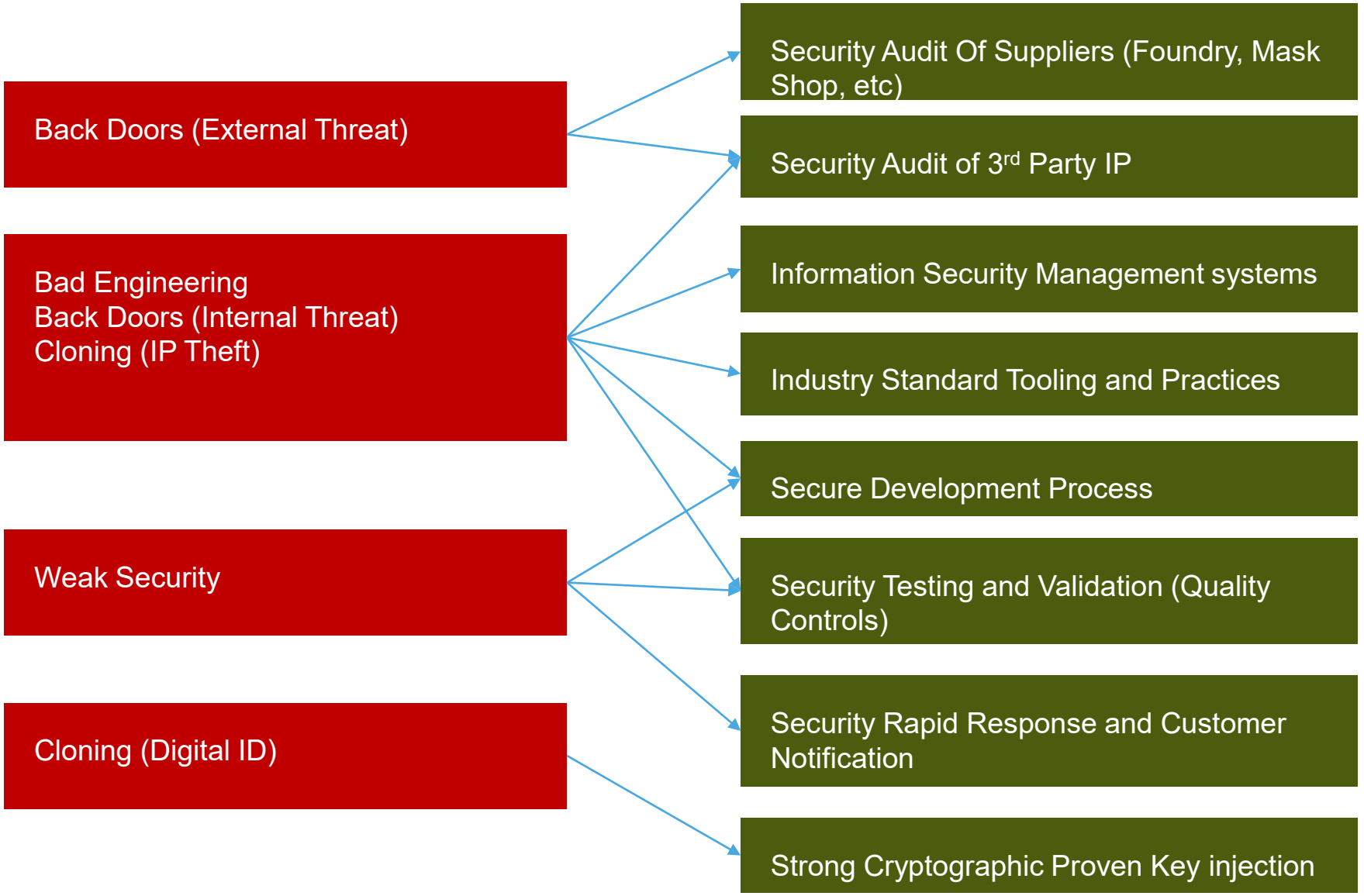
Test Centre /Assembly

Risk Mitigation for Company Internal Processes



- The Companies ISMS is certified using ISO27001
- Development Process and procedures and locations are certified using
  - Common Criteria
  - Process Certifications (e.g. ISO 21434, IEC 62443)
- The chip has a strong digital identity injected use strong cryptographic key material

THREATS VS KEY RISK MITIGATION



SECURE CONNECTIONS
FOR A SMARTER WORLD