Cell-based Organisations:

Cell-based Organisation for Security

DRAFT

So DRAFT that I haven't completed
the middle or the end!
– Tony Richards

Introduction to Cell-Based Organisational Structures

Cell-based Organisations:
The Rules

1. All work is defined by fitness functions (rules of engagement, user needs, mechanism of measurement etc)
2. All work is done by small cells (i.e. teams or squads of less than 12) providing services / products etc to others. Each squad is covered by its own fitness function and has total autonomy over how it does things.
3. All interaction is through service / product interfaces. These act as the boundary, the promises one group makes to others.
4. A tribe is a logical grouping of one or more cells. It has an executive responsible.
5. The executive in charge of a unit is responsible for measuring, defining and refining fitness functions of all cells within their tribe.
6. As cells become too big (i.e. greater than 12), they are subdivided into new squads within the tribe. Each squad will have their own fitness functions.
7. As a tribe becomes too big it is subdivided into new tribes, each with their own executive and fitness function.

Please note, this approach is based fundamentally on a focus on user needs as opposed to financial value.

** Reference: @SWardley*

Cell-based Organisations:

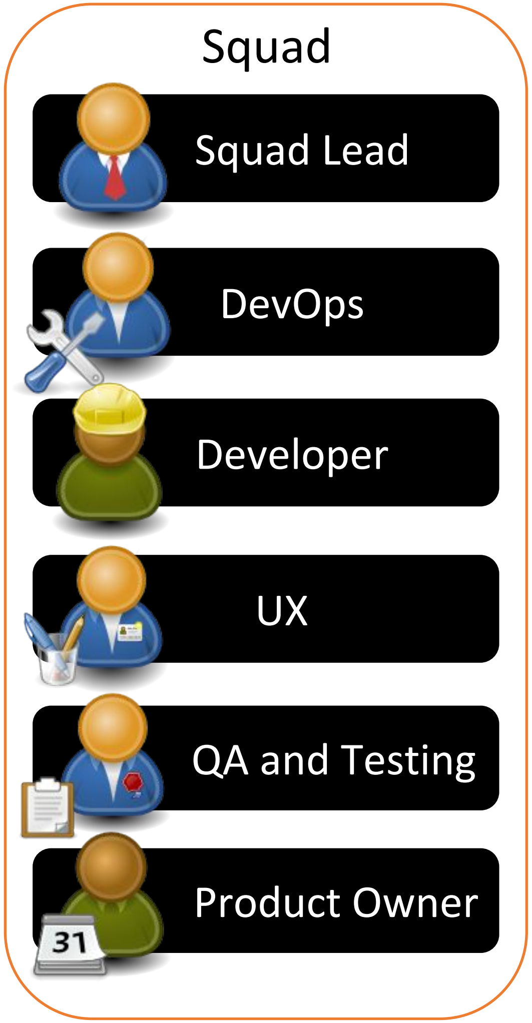
Agile Organisations

Cell-based Organisations:
Agile Organisations:
Anatomy of a: Squad/Team

A Squad is a fully autonomous, cross functional team that has full responsibilities and little to no dependencies on others, built around a single clear mission. Once the mission has been fulfilled the Squad will be re-distributed.

Ideally squads should be around 4 to 8 people in size. This ensures that they can be easily managed and any meetings can be kept efficient, any smaller and there is no real value and any larger the team becomes more difficult to manage.

The objectives of these teams is a great way to promote teamwork, collaboration and innovation, as well as giving team members ownership and a sense of enablement.

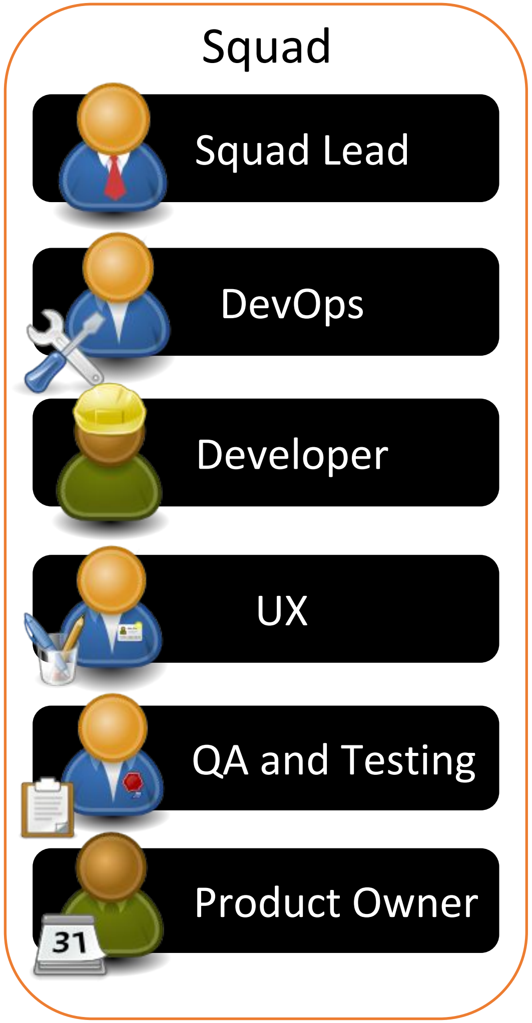


Cell-based Organisations:
Agile Organisations:
Anatomy of a: Squad

Squad lead. This role, called "Scrum Master" in Scrum or Agile Coach in other methods, is responsible for facilitating the team, obtaining resources for it, and protecting it from problems.

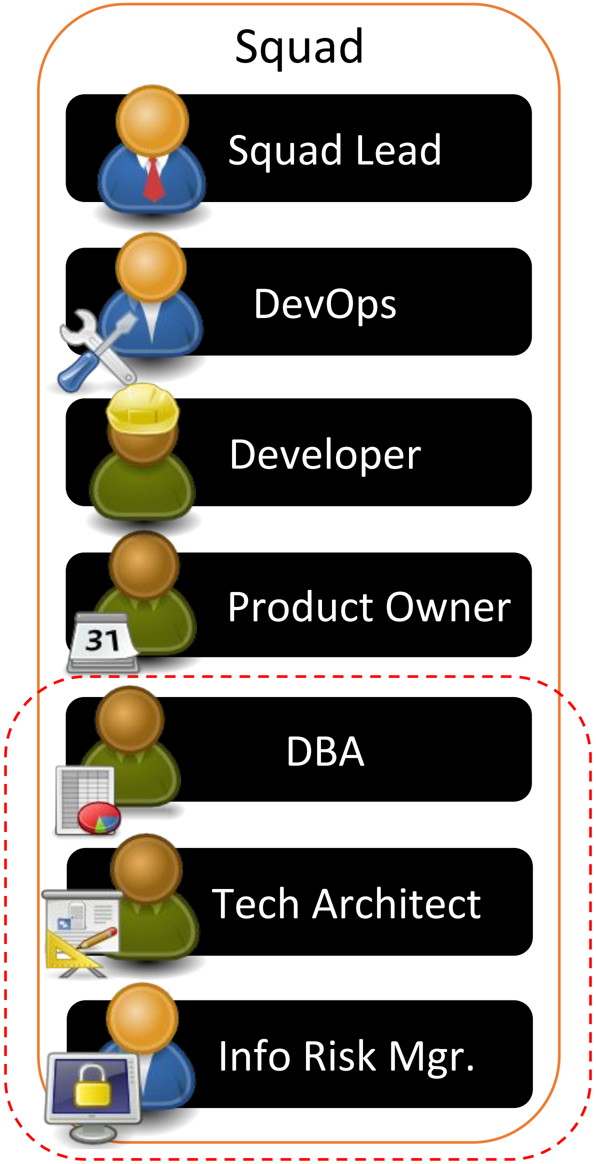
Product owner. The product owner, represents the stakeholders. This is the one person responsible on the squad, who is responsible for the prioritized work item list (called a product backlog in Scrum), for making decisions in a timely manner, and for providing information in a timely manner.

Team member. This role, sometimes referred to as developer or programmer, is responsible for the creation and delivery of a system. This includes modeling, programming, testing, and release activities, as well as others.

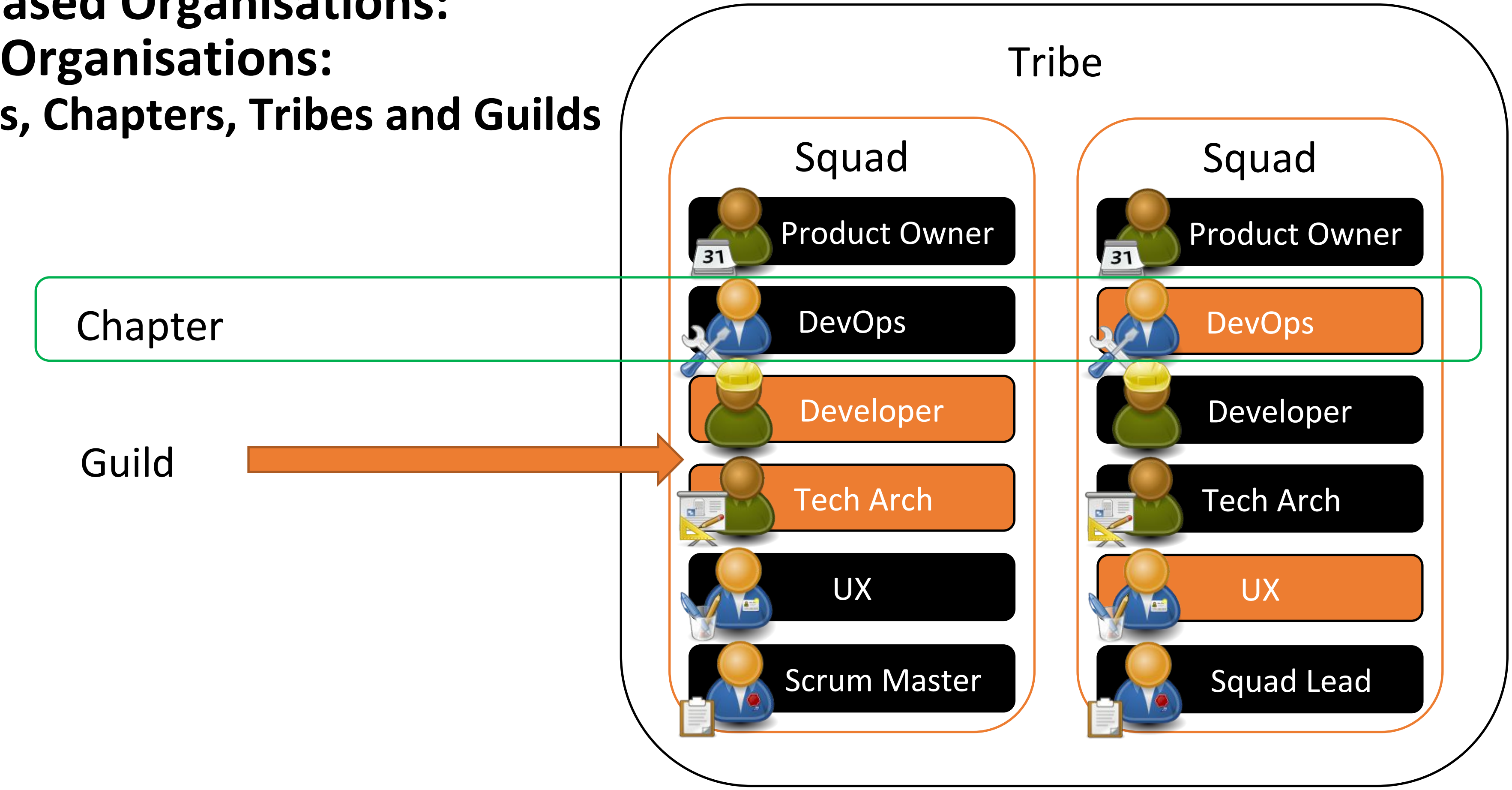


Cell-based Organisations:
Agile Organisations:
Anatomy of a: Squad

Technical experts. Sometimes the squad needs the help of technical experts, such as an agile DBA to help design and test their database, a Technical Architect responsible for facilitating architectural decisions or a Information Risk Manager responsible for managing the risks and vulnerabilities. Technical experts are brought in on an as-needed, temporary basis, to help the team overcome a difficult problem and to transfer their skills to one or more developers on the team.

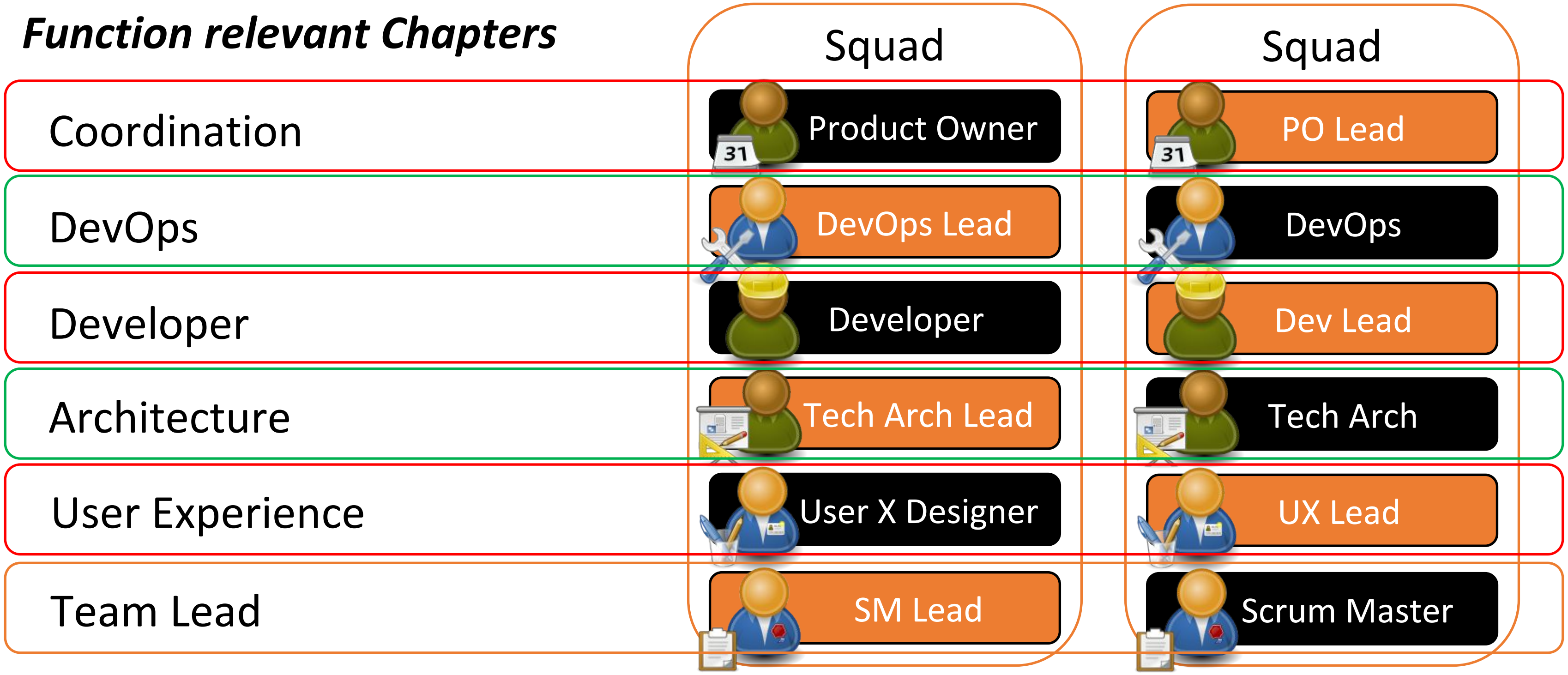


Cell-based Organisations:
Agile Organisations:
Squads, Chapters, Tribes and Guilds



Spotify took this further, grouping Squads with similar missions into Tribes.
https://labs.spotify.com/2014/03/27/spotify-engineering-culture-part-1/

Cell-based Organisations:
Agile Organisations:
Anatomy of a: Chapter

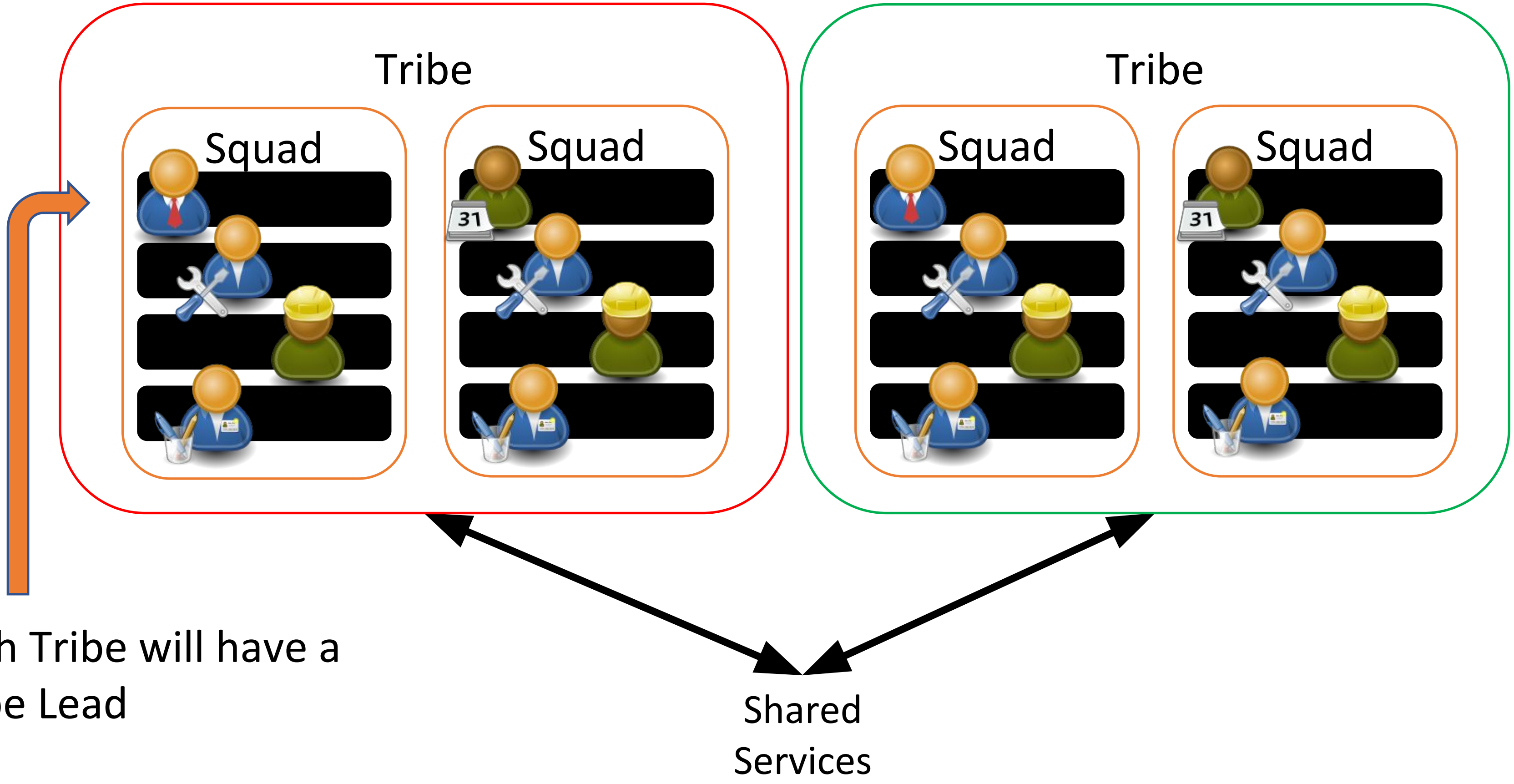


Function relevant Chapters	Squad	Squad
Coordination	Product Owner	PO Lead
DevOps	DevOps Lead	DevOps
Developer	Developer	Dev Lead
Architecture	Tech Arch Lead	Tech Arch
User Experience	User X Designer	UX Lead
Team Lead	SM Lead	Scrum Master

A Chapter is an across Squad specialism group. Each Chapter has a Lead, whose role is to provide line-management to the Chapter members, including mentoring, grade setting and professional development. Chapters should meet monthly.

Cell-based Organisations:
Agile Organisations:
Anatomy of a: Tribe

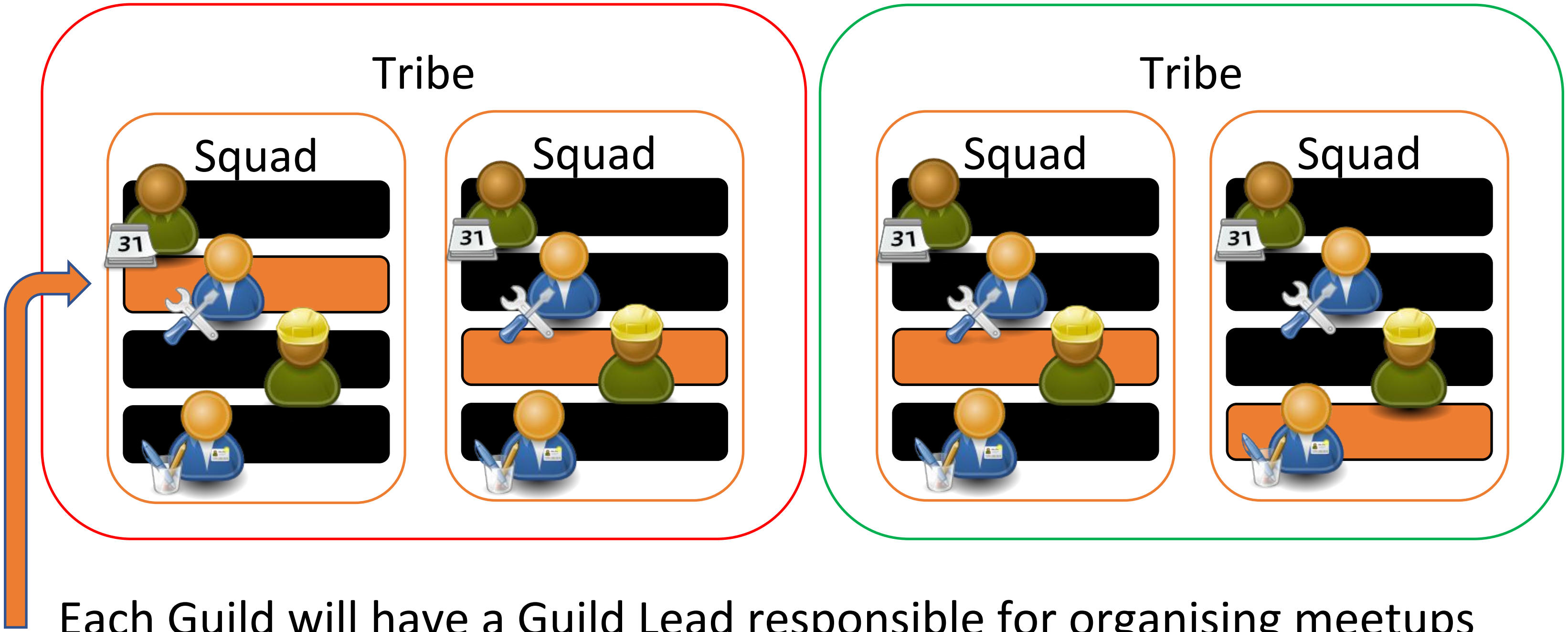
A Tribe is a collection of squads that share a common theme, and use shared services with other Tribes.



Each Tribe will have a Tribe Lead

Cell-based Organisations:
Agile Organisations:
Anatomy of a: Guild

A guild is a community of members with shared interests. These are a group of people across the organisation who want to share knowledge, tools, code, and practices. Guilds should meet quarterly, to discuss and present on the subject of interest. An example of a Guild would be around Block-chain.



Each Guild will have a Guild Lead responsible for organising meetups and as a point of contact for the guide.

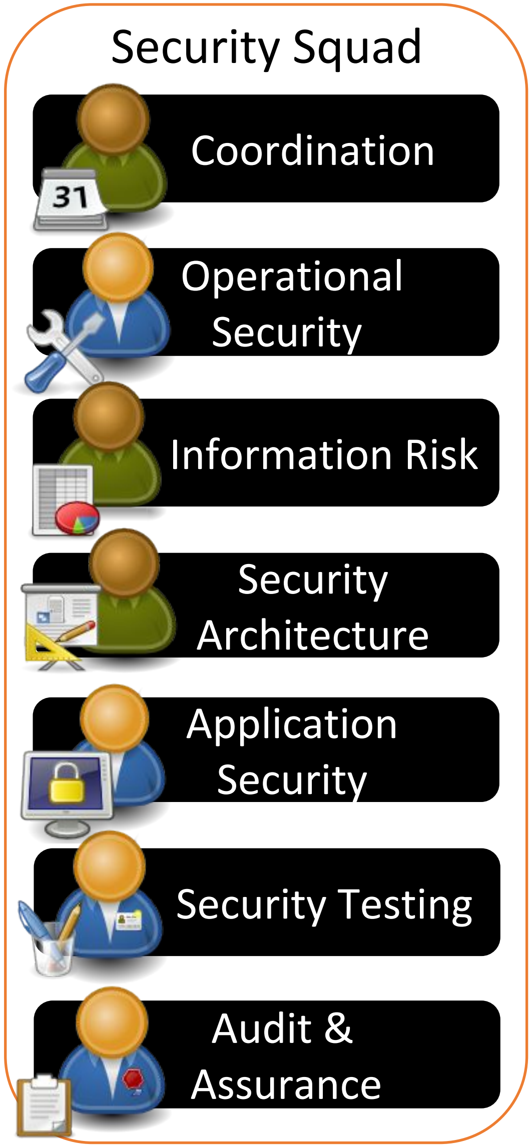
Cell-based Organisations:

Agile Organisations: Building Security into an Agile Organisation

Cell-based Organisations:
Agile Organisations:
Anatomy of a: Central Security Squad

A Central Security Squad is a fully autonomous, cross functional team that has full responsibilities and little to no dependencies on others, built around providing security subject matter expertise across the organisation in a range of security disciplines.

Ideally the squad should be between 4 and 8 people in size. This ensures that they can be easily managed and any meetings can be kept efficient, any smaller and there is no real value and any larger the team becomes more difficult to manage. Not all Security Squads are equal and there can be variations between or across organisations.



Security Squad

Coordination

Operational Security

Information Risk

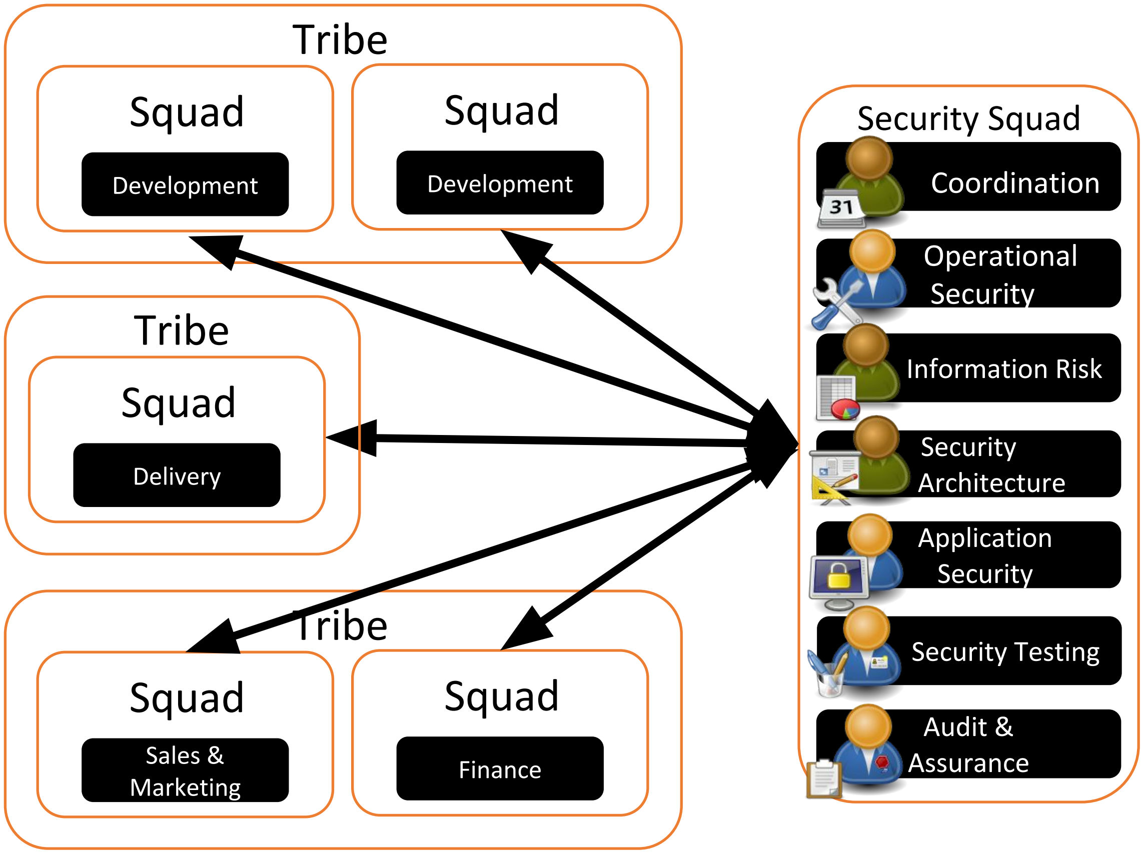
Security Architecture

Application Security

Security Testing

Audit & Assurance

Cell-based Organisations:
Agile Organisations:
Anatomy of a: Central Security Squad



The Central Security Squad, supports other Squads and provides security expertise across the organisation.

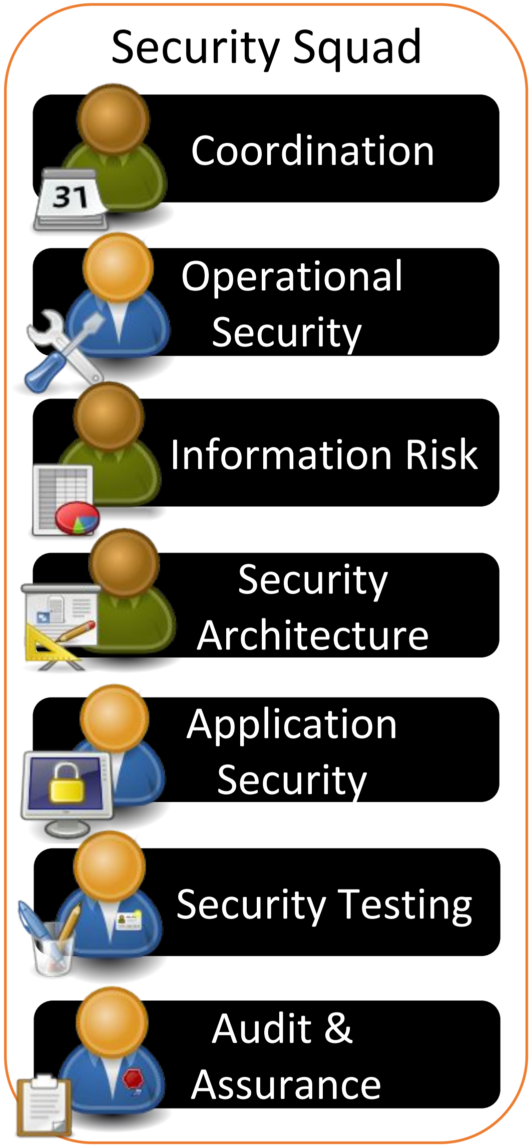
It is also is responsible for organisation wide security functions, such as:

- Governance, Risk and Compliance;
- Data Protection;
- Business Continuity; and,
- Incident Management.

Cell-based Organisations:
Agile Organisations:
Anatomy of a: Central Security Squad

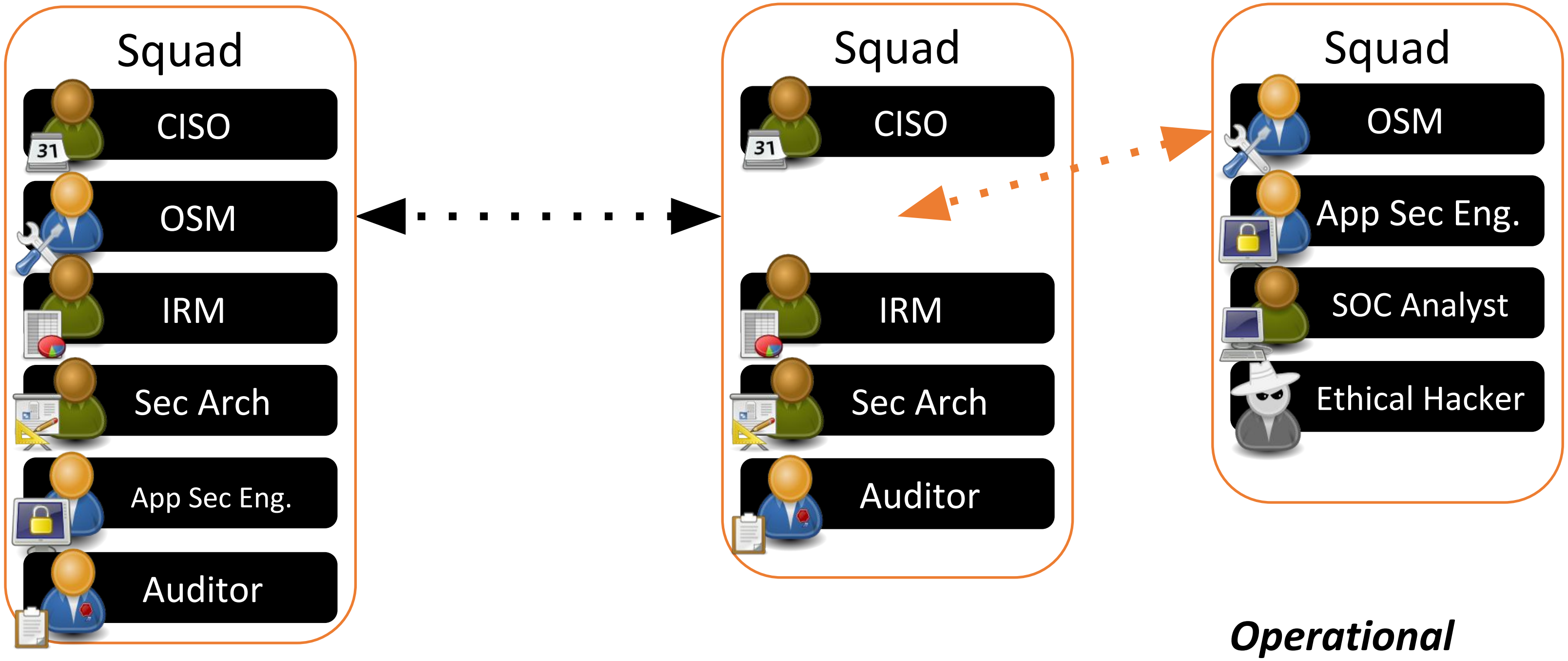
Coordination/Management. This function acting as a “Squad Lead” can be a Chief Information Security Officer (CISO), or Information Security Officer at some organisations, is responsible for facilitating the team, obtaining resources for it, protecting it from problems, and to prioritize tasks and jobs. They also, represent the organisation's stakeholders, and will report to the Board and/or Risk and Audit Committees.

Team member. These functions, which can be number of different security specialisms, are responsible for providing subject matter expertise within the function domain and general security support to the business. This includes risk management, security architecture, security testing, and audit activities, as well as others.



Cell-based Organisations:
Agile Security Organisation:
Cell Division

If a Squad is required to increase in size, in regards to an increased functional need, then a second Squad is created to fulfill the mission of the expanded function. AWS uses the 2 pizza rule (12 people), but squads can be as small as 4 members.



Operational Security Mission

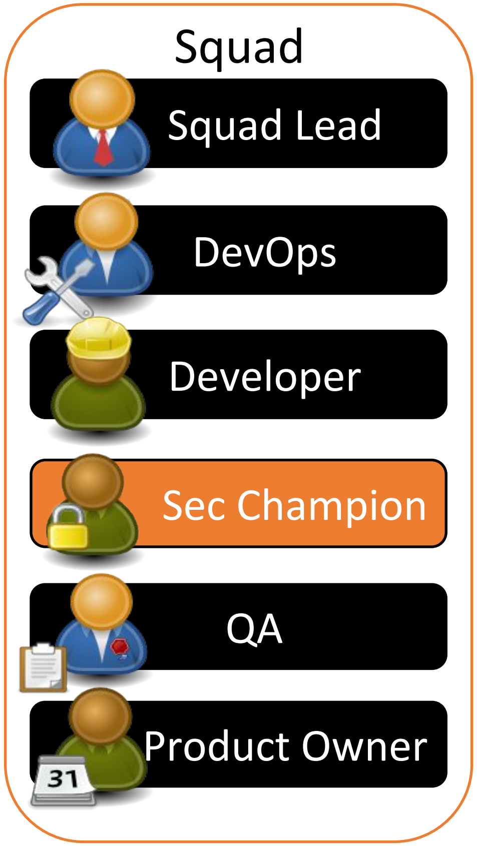
Cell-based Organisations:
Agile Organisations:
Anatomy of a: Security Champion

What is a Security Champion?

- Security Champions are active members of a Squad with a dotted line to the Central Security Squad or function.
- Act as the "voice" of security for the given product or Squad.
- Security Champions provide visibility to the central security function.

OWASP Recommendations

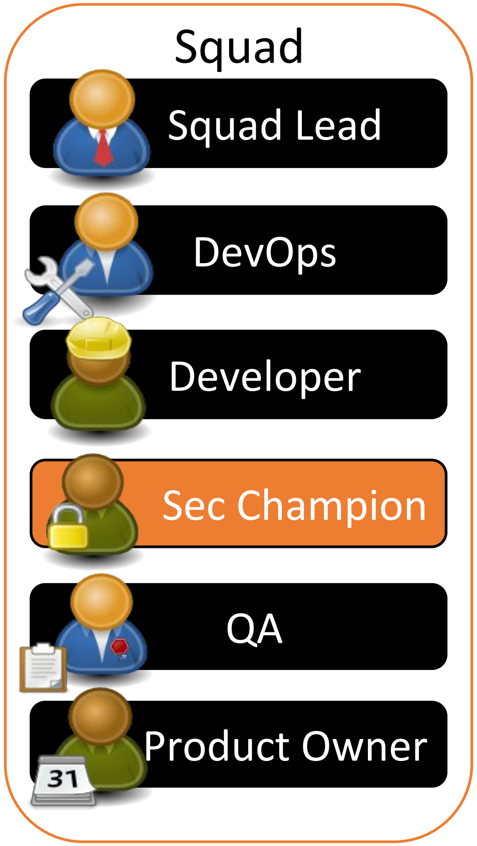
- Security Champions are a model that has been used successfully.
- A group of Security Champions should be formed into a Security Guild or network and attend weekly meetings.
- The Security Champions network or guild needs energy from the Central Security Squad.



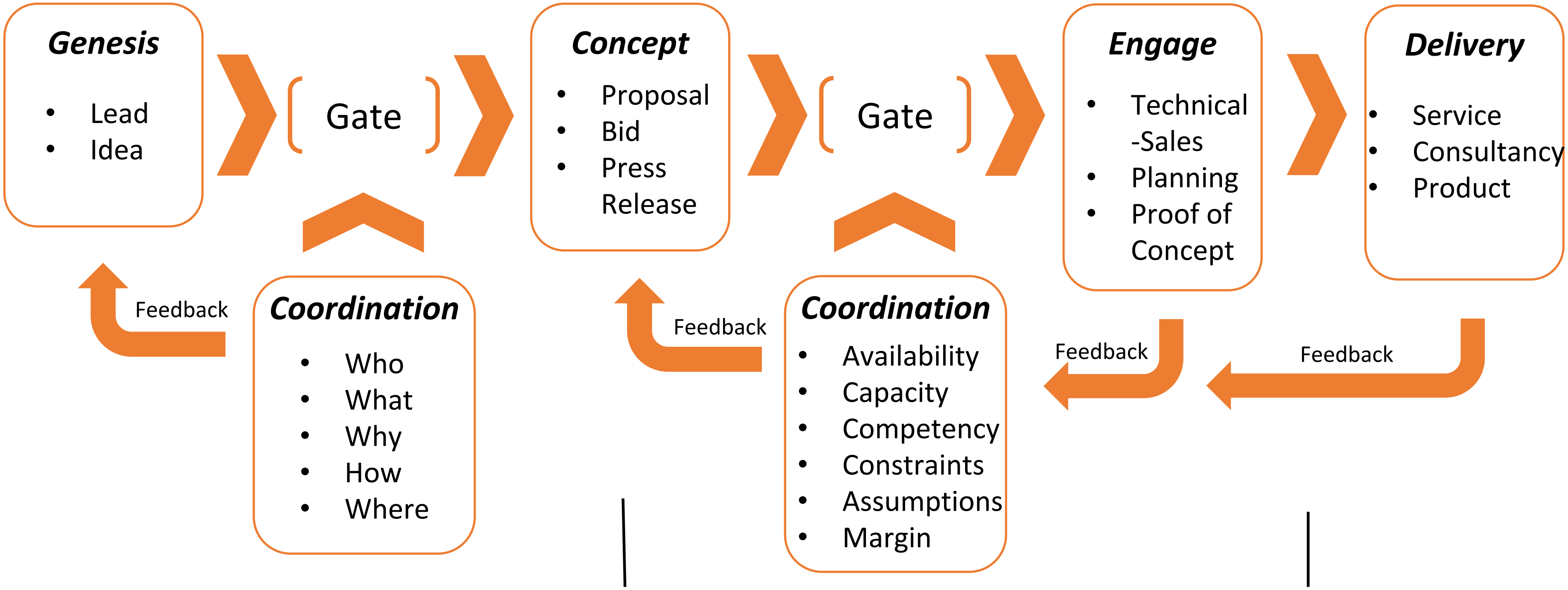
Cell-based Organisations:
Agile Organisations:
Anatomy of a: Security Champion

What do they do?

- Assist in the triage of security issues for their squad or area.
- Collaborate with other security champions.
- Review impact of ‘breaking changes’ made in other projects.
- Are the single point of contact for their assigned team.
- Ensure that security is not a blocker.
- Assist in making security decisions for their team:
    - Low-Moderate security impact:
        - Empowered to make decisions.
        - Document decisions made in bugs or wiki.
    - High-Critical security impact:
        - Work with Security Squad on mitigation strategies.
- Help with QA and Testing:
    - Write Security Tests (from Unit Tests to Integration tests).
- Help with development and security of CI/CD (Continuous Integration/Continuous Delivery) environments.



Cell-based Organisations:
Common Project Process



Genesis

- Lead
- Idea

Gate

Concept

- Proposal
- Bid
- Press Release

Gate

Engage

- Technical -Sales
- Planning
- Proof of Concept

Delivery

- Service
- Consultancy
- Product

Feedback

Coordination

- Who
- What
- Why
- How
- Where

Feedback

Coordination

- Availability
- Capacity
- Competency
- Constraints
- Assumptions
- Margin

Feedback

Feedback

- Assign an Owner
- Assign relevant multi-disciplinary Team

- Evolve Multi-disciplinary Team to meet needs

Tony Richards

Cell-based Organisations:

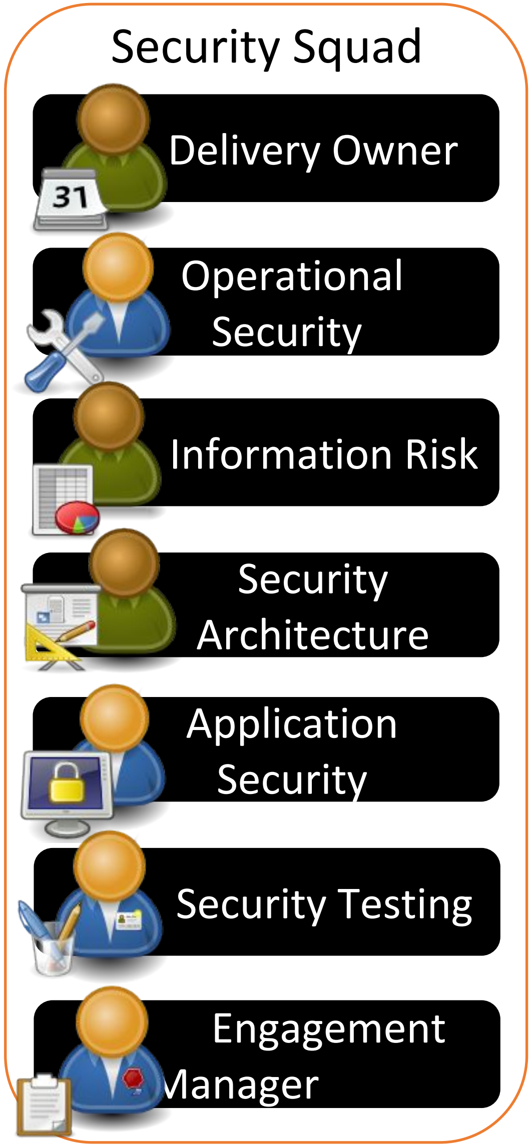
Agile Security Consultancy

Cell-based Organisations:
Agile Security Consultancy:
Anatomy of a: Security Consultancy Squad

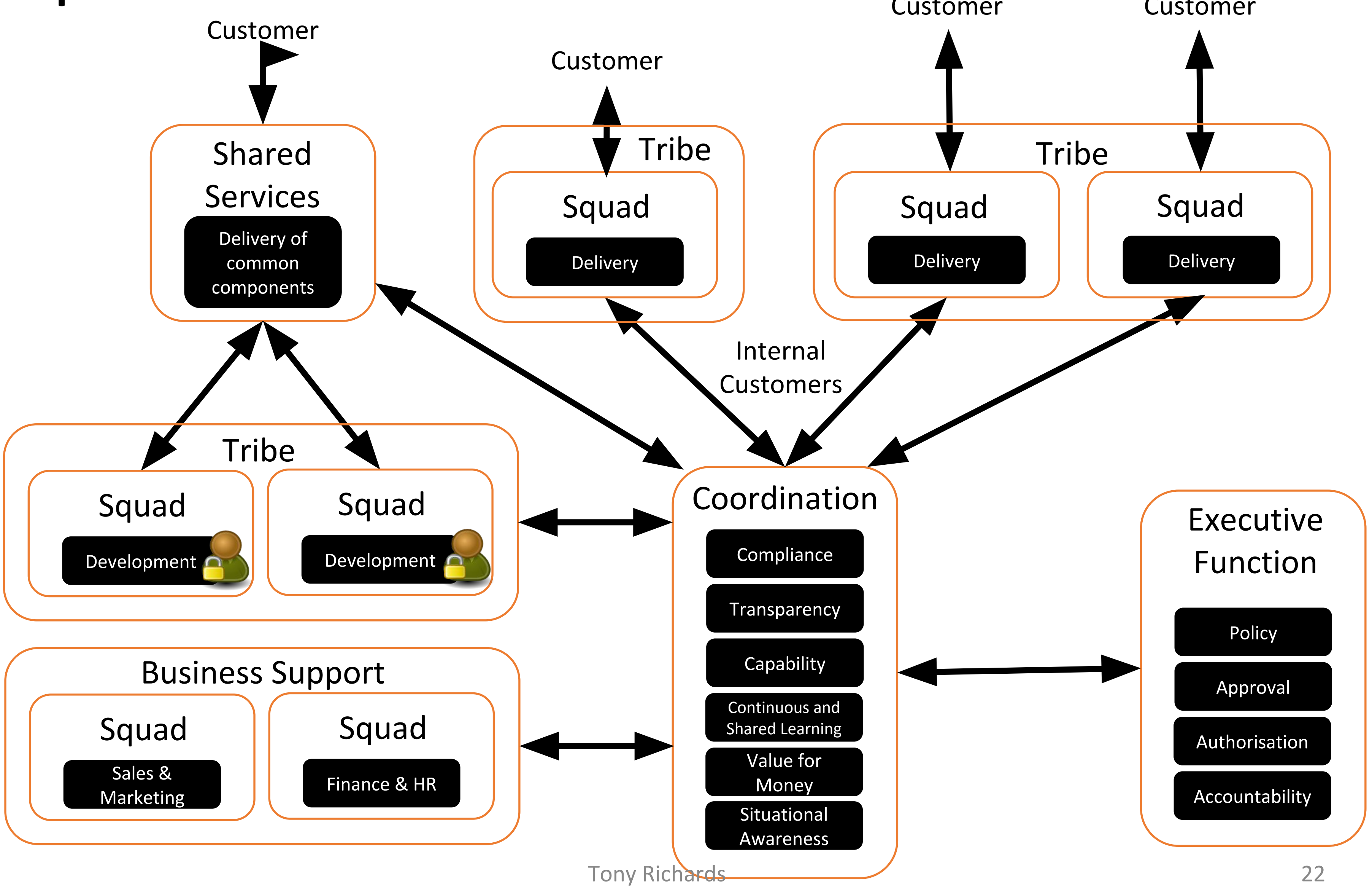
Delivery Owner. This function acts as a “Squad Lead” or information Security Officer at some organisations, is responsible for facilitating the team, obtaining resources for it, and protecting it from problems.

Engagement Manager. The engagement manager, represents the stakeholders. This is the one person responsible for the prioritized work item list (called a product backlog in Scrum), for making decisions in a timely manner.

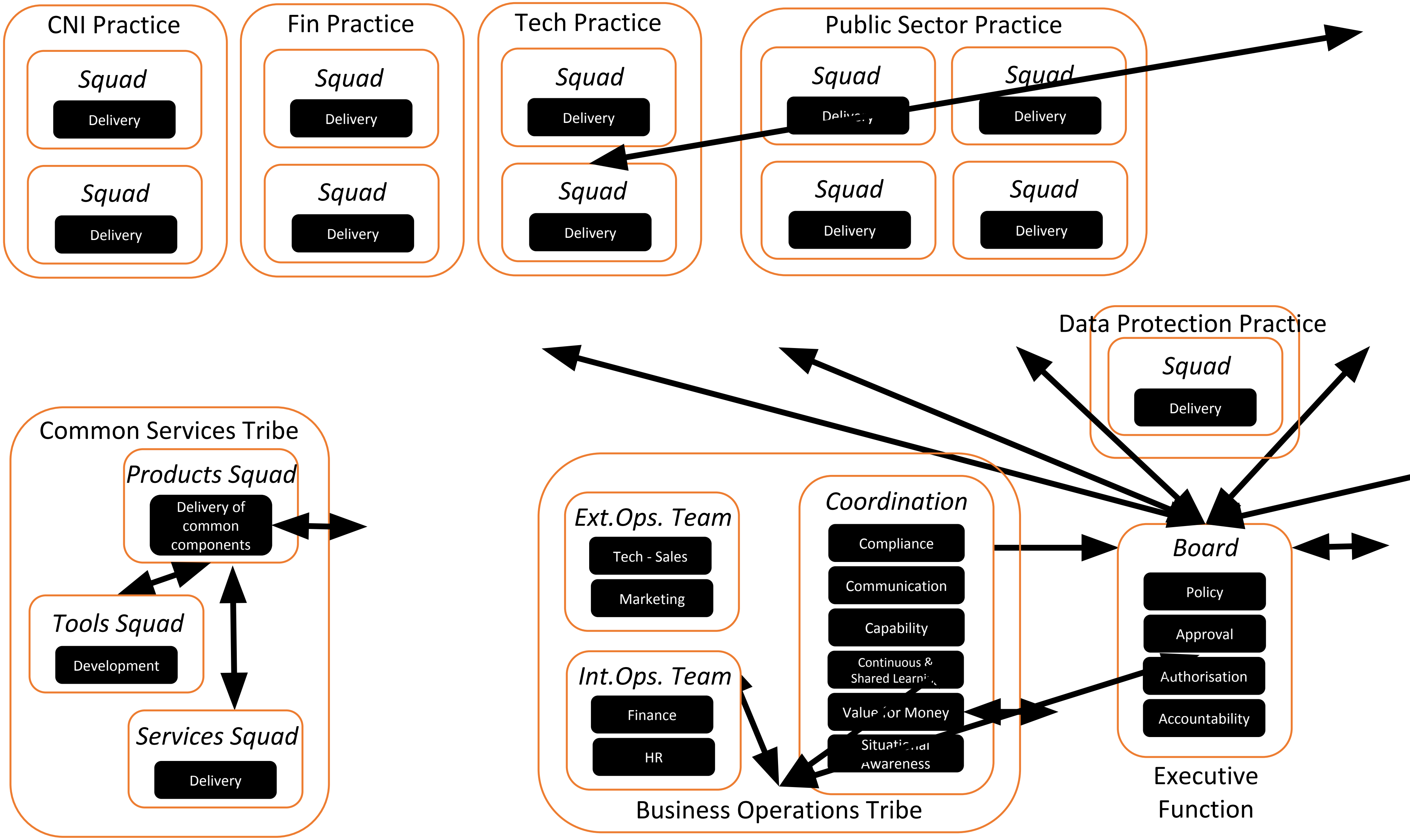
Team member. These functions, which can be number of different security specialisms, are responsible for providing subject matter expertise within the function domain and general security support to the business. This includes risk management, security architecture, security testing, and audit activities, as well as others.



Cell-based Security Organisation Example



Cell-based Organisations:Security Company



CNI Practice

Squad

Delivery

Squad

Delivery

Fin Practice

Squad

Delivery

Squad

Delivery

Tech Practice

Squad

Delivery

Squad

Delivery

Public Sector Practice

Squad

Delivery

Squad

Delivery

Squad

Delivery

Squad

Delivery

Data Protection Practice

Squad

Delivery

Common Services Tribe

Products Squad

Delivery of common components

Tools Squad

Development

Services Squad

Delivery

Ext.Ops. Team

Tech - Sales

Marketing

Int.Ops. Team

Finance

HR

Coordination

Compliance

Communication

Capability

Continuous & Shared Learning

Value for Money

Situational Awareness

Business Operations Tribe

Board

Policy

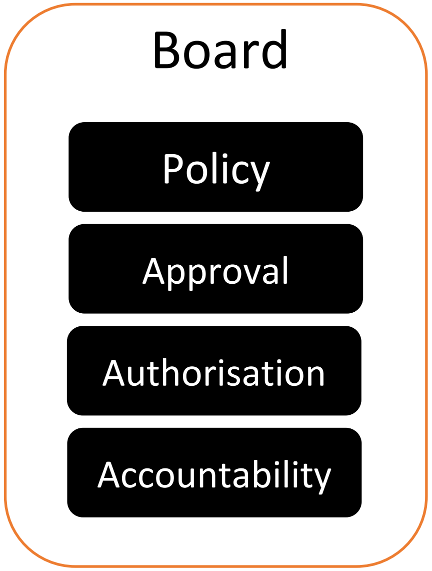
Approval

Authorisation

Accountability

Executive Function

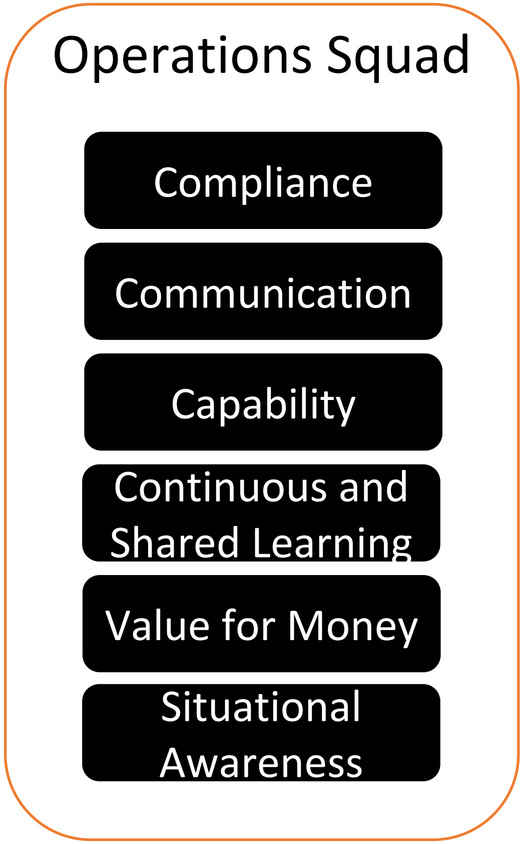
Cell-based Organisations:
Security Company:
Board ----Draft



Executive Function

Within a Security Company's Cell Structure, the Boards role as an executive function is to be responsible and accountable for setting policy, approving approaches and authorising deviations.

Cell-based Organisations: Security Company: Coordination



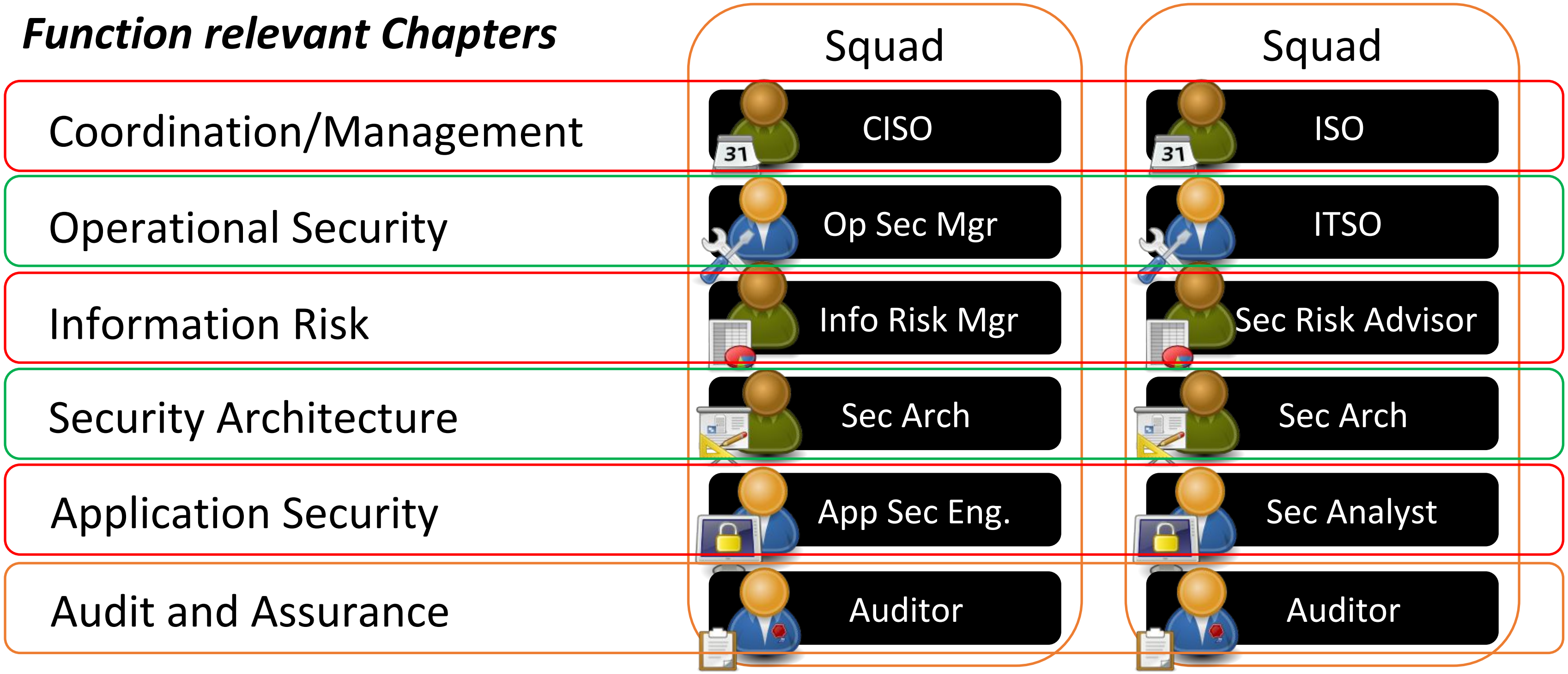
Co-ordination

Within the company's Operations Squad, the co-ordination capability can respond to requests from a Squad, either advising them to use components from another Squad or a common service or challenging how the project is being built or how to comply with a general policy. Any new project or request to spend significant sums is examined by spend control and analysed through an analysis group.

Operations is not only your learning function but enabler, ensuring continuous, discovery and dissemination of examples of good practice and common solutions. It does so in an iterative manner, improving its understanding of the landscape with each request (and map). When potential common services are identified, this is passed to the Common Services Squad. This team ensures delivery of common services and components and provides a registry of common services online

The capability function is involved in developing the squads and ensuring they not only have aptitude but the right attitude in place.

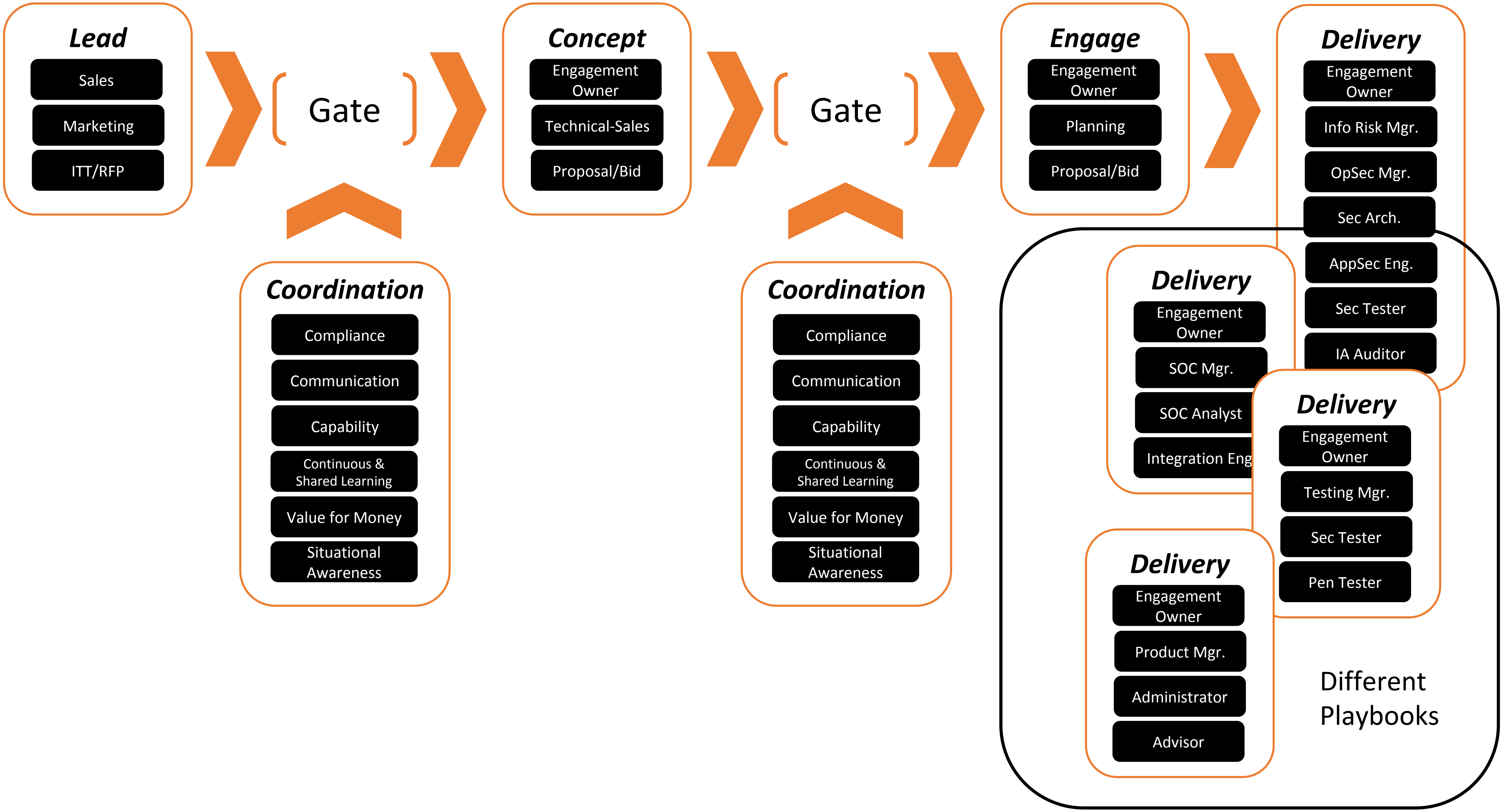
Cell-based Organisations:
Agile Security Organisation:
Anatomy of a: Security Chapter



Function relevant Chapters	Squad	Squad
Coordination/Management	CISO	ISO
Operational Security	Op Sec Mgr	ITSO
Information Risk	Info Risk Mgr	Sec Risk Advisor
Security Architecture	Sec Arch	Sec Arch
Application Security	App Sec Eng.	Sec Analyst
Audit and Assurance	Auditor	Auditor

A Chapter is an across Squad specialism group. Each Chapter has a Lead, whose role is to provide line-management to the Chapter members, including mentoring, grade setting and professional development. Chapters should meet monthly.

Cell-based Organisations:
Client Engagement Playbooks



Lead
- Sales
- Marketing
- ITT/RFP

Gate

Coordination
- Compliance
- Communication
- Capability
- Continuous & Shared Learning
- Value for Money
- Situational Awareness

Concept
- Engagement Owner
- Technical-Sales
- Proposal/Bid

Gate

Coordination
- Compliance
- Communication
- Capability
- Continuous & Shared Learning
- Value for Money
- Situational Awareness

Engage
- Engagement Owner
- Planning
- Proposal/Bid

Delivery
- Engagement Owner
- Info Risk Mgr.
- OpSec Mgr.
- Sec Arch.
- AppSec Eng.
- Sec Tester
- IA Auditor

Delivery
- Engagement Owner
- SOC Mgr.
- SOC Analyst
- Integration Eng

Delivery
- Engagement Owner
- Testing Mgr.
- Sec Tester
- Pen Tester

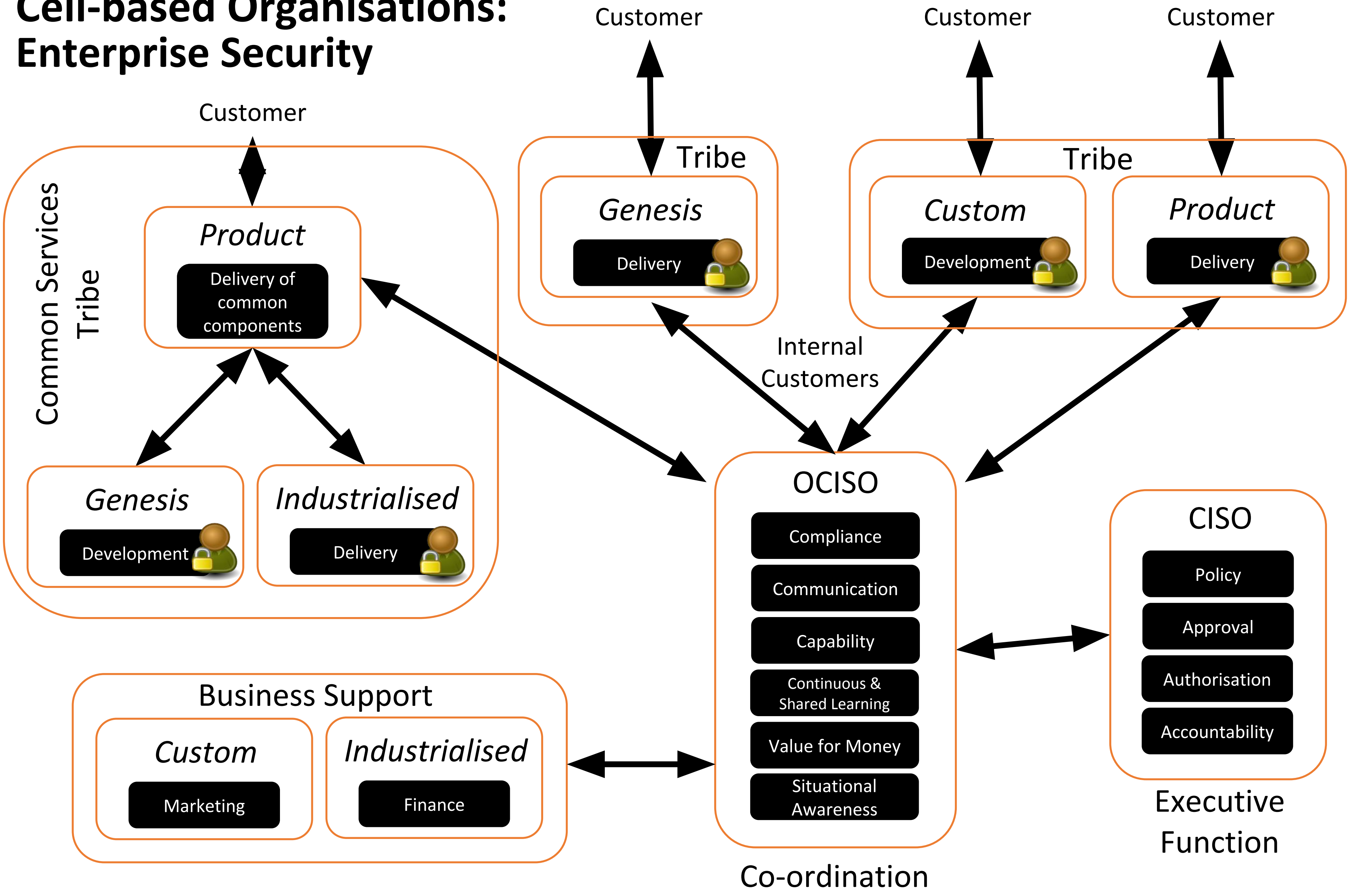
Delivery
- Engagement Owner
- Product Mgr.
- Administrator
- Advisor

Different Playbooks

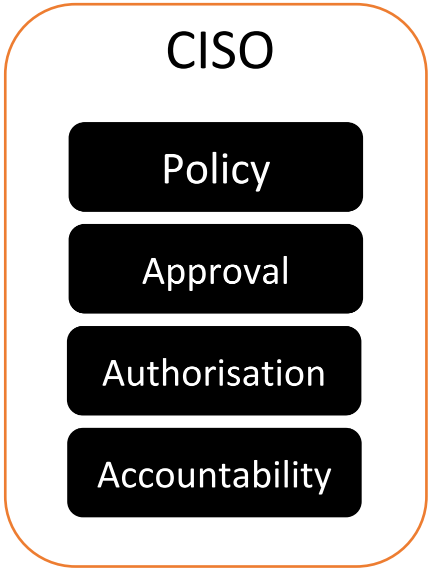
Cell-based Organisations:

Cell-based Enterprise Security Organisation

Cell-based Organisations: Enterprise Security



Cell-based Organisations:
Enterprise Security:
CISO ----Draft

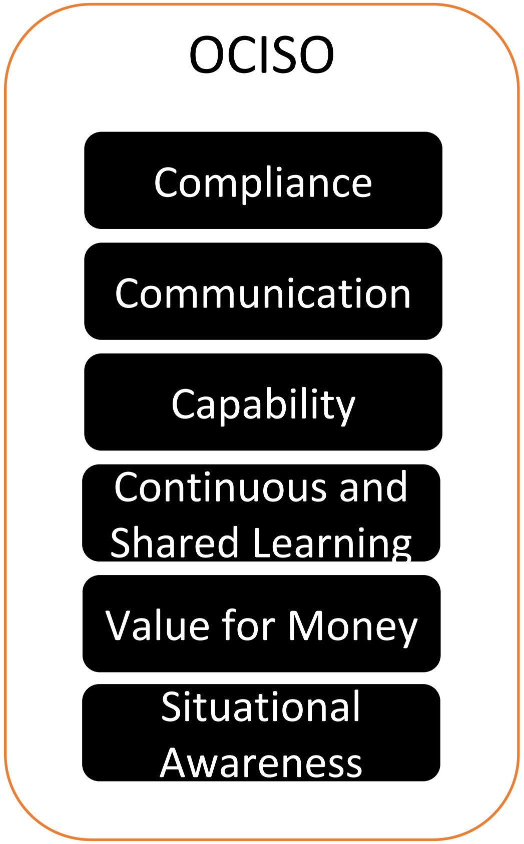


Executive Function

The role of the Chief Information Security Officer, is as a senior-level executive responsible for establishing and maintaining the enterprise vision, strategy, and information security program, to ensure information assets and technologies are adequately protected from both internal and external threats.

Within the Enterprise Security Cell Structure, the CISO role is an executive function that is responsible and accountable for setting policy, approving approaches and authorising deviations.

Cell-based Organisations: Enterprise Security: Office of the CISO



OCISO

Compliance

Communication

Capability

Continuous and Shared Learning

Value for Money

Situational Awareness

Co-ordination

Within Office of the CISO (OCISO), the co-ordination capability can respond to requests from a Squad, either advising them to use components from another Squad or a common service or challenging how the project is being built or how to comply with a general policy. Any new project or request to spend significant sums is examined by spend control and analysed through an analysis group.

OCISO is not only a learning function but enabler, ensuring continuous, discovery and dissemination of examples of good practice and common solutions. It does so in an iterative manner, improving its understanding of the landscape with each request (and map). When potential common services are identified, this is passed to the Common Services Squad. This team ensures delivery of common services and components and provides a registry of common services online

The capability function is involved in developing the squads and ensuring they not only have aptitude but the right attitude in place.

Cell-based Organisations:
Cell-based Enterprise Security

Placeholder

Cell-based Organisations:

Co-ordination: Fitness Functions

Cell-based Organisations:
Cell Co-ordination: Fitness Functions

The coordination squad will manage the various Tribes and Squads through agreeing and monitoring a range of fitness functions:

- Purpose and User Need
- Mission Scope
- Deliverables and Outcomes
- Metrics and Milestones
- Dependencies
- Limitations and Constraints

Cell-based Organisations:
Tribe Fitness Function: The Rules of Engagement

Purpose and User Need:
The purpose of the Tribe mission and the user group it serves must be described in a clear and brief statement.
Mission Scope:
The scope of the Tribe mission describes the client grouping or operational function that the mission deals with or to which it is relevant.
Metrics and Milestones:
Clearly define any agreed types of metrics used to report on the status of the Tribe.
Dependencies:
List any elements that the mission is dependent on for a successful delivery and outcome, such as information, people or services.
Limitations and Constraints:
Define any constraints or areas that the engagement is limited too.

Cell-based Organisations:
Squad Fitness Function: The Rules of Engagement

Purpose and User Need:
The purpose of the squad mission and the user needs it meets must be described in a clear and brief statement.

Mission Scope:
The scope of the squad mission describes the area or subject matter that the mission deals with or to which it is relevant.

Deliverables and Outcomes:
A statement setting out the outcomes expected from the engagement and any defined deliverables or articles that need to be produced or developed.

Metrics and Milestones:
Clearly define any agreed progression milestones or types of metrics used to report on the status of the engagement.

Dependencies:
List any elements that the mission is dependent on for a successful delivery and outcome, such as information, people or services.

Limitations and Constraints:
Define any constraints or areas that the engagement is limited too.

Cell-based Organisations:

Attitudes: Pioneers, Settlers and Town Planners

Cell-based Organisations:
Attitudes: Pioneers

The **Pioneers** will deal with the chaotic and uncertain world of genesis (or the “**innovation**” of novel and new). They are our artisans, our “creative” minds. They use appropriate techniques such as agile, rapid development, minimal viable system with a focus on experimentation and trying things out. The group understands implicitly that the future value of something is inversely proportional to the certainty we have over it, gambling is a must. As there is no defined market, there are no customers to listen to only gut. Failure is accepted as a norm, rewards are built on future successes and rapid change is the “standard operating procedure”. In order to achieve the speeds necessary, use of component sub systems becomes essential.

Cell-based Organisations:
Attitudes: Pioneers

Type	Creative Mind	Path Finder

Deals with	Happy with	Methods
Rare	Failure	Agile
Poorly Understood	Gambling and Gut Feel	Common Components
Differential & Novel	Experimentation	Speed above all
High Future Value	Uncertainty	
Constantly Changing	Exploration	
Undefined Market		

Pioneers/Thinkers, finding new solutions and providing future value

Security Aptitude Pioneers

Role examples	Security Strategist	Security Architect

Deals with	Happy with	Methods
New	Minimum Viability	Agile
Poorly Understood	Gambling and Gut Feel	Common Solutions
Differential & Novel Tech	Experimentation	Minimum Necessary
Constantly Changing Dev.	Uncertainty	Continuous Risk Management
Undefined Threats	Innovation	Simple Vuln. Assessment

Cell-based Organisations: Attitudes: Settlers

The **Settlers** cover the custom built to product stage and focus on **leveraging** what exists. This group steals from the Pioneers whether internal or external (in the wider ecosystem). The act of stealing (or eating the ecosystem) forces those Pioneers to get on with the act of Pioneering. The Settlers in the mean time concentrate on productisation or provision as rental services. The Settler’s focus is on listening to customers and meeting their needs, developing metrics and feedback, incremental improvement, driving a component to feature completeness, maximizing profitability and reducing cost of production. They grow ecosystems, they nurture them and they exploit them. This group is where most of the games of strategy are played e.g. do we open source a component to undermine a competitor or do we slow down evolution through a dark art (branding etc.)?

Settlers tend to use a blend of methods, part science / part art, they are more “cunning” than “creative” and are rewarded on profitability. They tend to be very good at spotting patterns (a necessary requirement for productisation of the novel and new). Similar games are played whether the component is something produced for sale or consumed by the organization. When consumed the focus is on driving down cost, driving it to more of a commodity etc.

Cell-based Organisations:
Attitudes: Settlers

Type	Tactical Mind	Machiavellian
Deals with	**Happy with**	**Methods**
Growing	Constant Improvement	Lean
Increasing Education	Market Analysis	Mines / Nurtures Ecosystems
Feature Differentiation	Feedback	Makes Success Happen
High Profitability	Trend Spotting	
Maturing Products	Listening	
Growing Market		

Settlers/Builders, growing the solutions and leveraging form new and old

Security Aptitude
Settlers

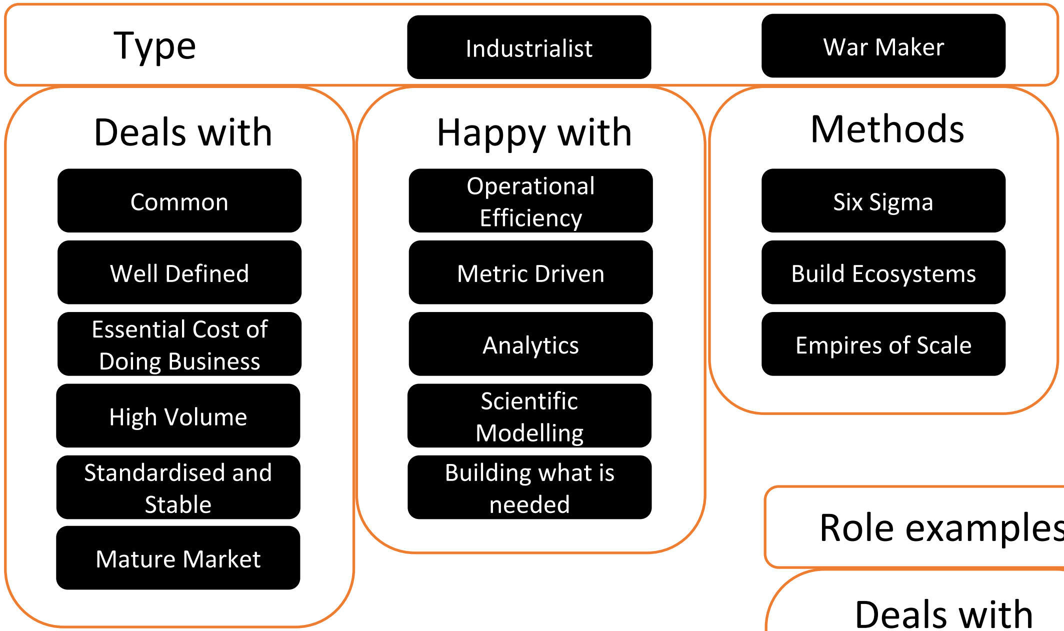
Role examples	Info Risk Manager	Ethical Hacker
Deals with	**Happy with**	**Methods**
Growing	Constant Improvement	Security Outcomes
Increasing Complexity	Changing Practice	Risk based Security Controls
Feature Differentiation	Under Assessment	User Security Needs
Maturing Products	Trend Spotting	Continuous Risk Management
Assessed Threats	Review and Assurance	Continuous Vuln. Assessment

Cell-based Organisations:
Attitudes: Pioneers

The **Town Planners** cover the commodity and utility stages and focus on **commoditization** and building of “**platforms for innovation**”. This group steals from the Settlers and builds the common components that the Pioneers use. The act of stealing is essential due to inertia that Settlers will build up through past success. Hence stealing forces them to move onwards. The Town Planners are almost exclusively metric driven - it’s all about volume, efficiency, resilience, cost and performance and woe betide anyone who turns up without data. Methods are about minimizing deviation, repeatability and continuous operational improvement, such as Six Sigma and Kaizen.

When it comes to listening to customers, this group is focused on providing volume operations of exceptionally efficient good enough standard components. They know what is needed better than the customer does. They also know how the customer suffers from inertia and becomes deluded over the need for customization. Rewards for Town Planners should be based on operational performance, cost efficiency and reliability. As a business you want to accept this is going to be a low margin but stable area.

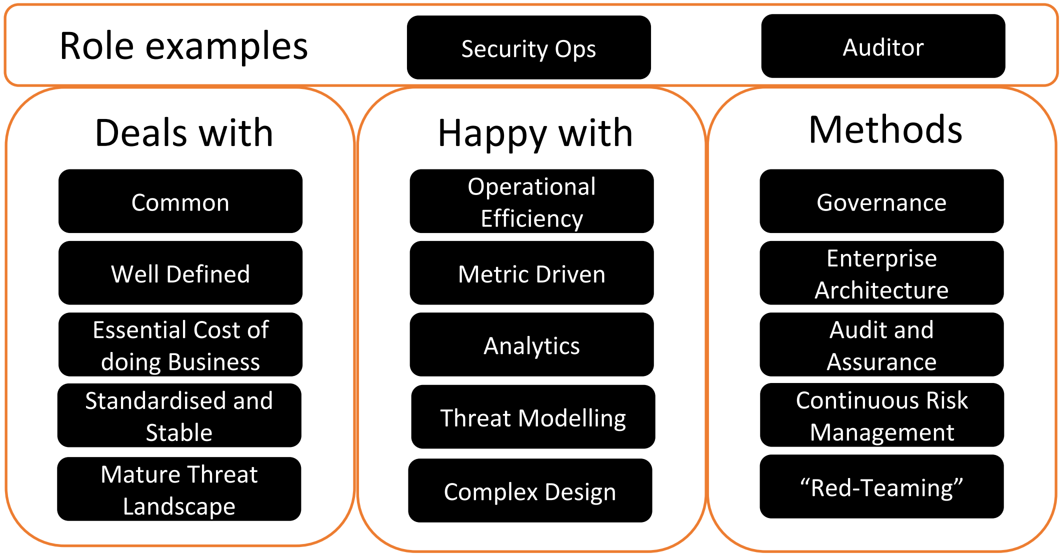
Cell-based Organisations: Attitudes: Town Planners



Type	Industrialist	War Maker
Deals with	**Happy with**	**Methods**
Common	Operational Efficiency	Six Sigma
Well Defined	Metric Driven	Build Ecosystems
Essential Cost of Doing Business	Analytics	Empires of Scale
High Volume	Scientific Modelling	
Standardised and Stable	Building what is needed	
Mature Market		

Town Planners/Producers, industrialising existing solutions and providing resilient stable infrastructure

Security Aptitude
Town Planners



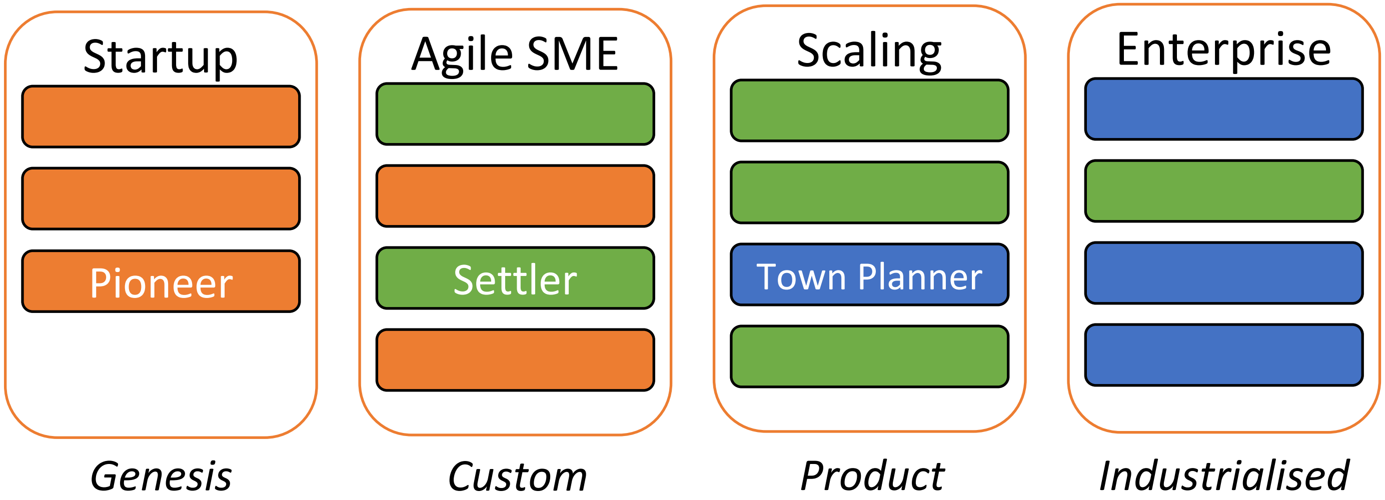
Role examples	Security Ops	Auditor
Deals with	**Happy with**	**Methods**
Common	Operational Efficiency	Governance
Well Defined	Metric Driven	Enterprise Architecture
Essential Cost of doing Business	Analytics	Audit and Assurance
Standardised and Stable	Threat Modelling	Continuous Risk Management
Mature Threat Landscape	Complex Design	“Red-Teaming”

Cell-based Organisations:
Attitudes within Squads

Different organisations need different formations of Squad Attitudes and the attitudes required will be significantly dictated by the size, maturity, and organisational structure.

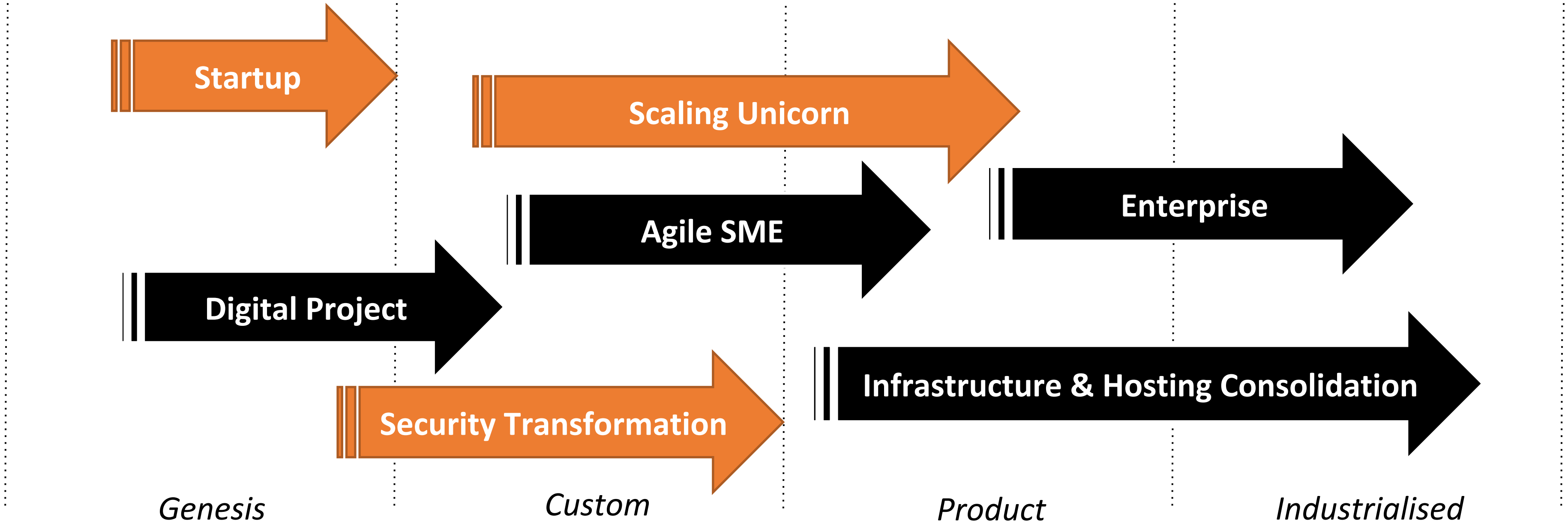
From *Genesis* Startups, comprised of Pioneers, through to *Custom* Agile SME businesses made up of a mix of Pioneer and Settler attitudes. *Product* organisations will inevitably be formed of a mixture of Settlers and and the odd Town Planner, as they streamline and scaling up, with *Industrialised* Enterprise organisations, mostly comprising of Town Planners with a few Settlers.

Squad Attitudes



Cell-based Organisations:
Attitudes within Squads over time

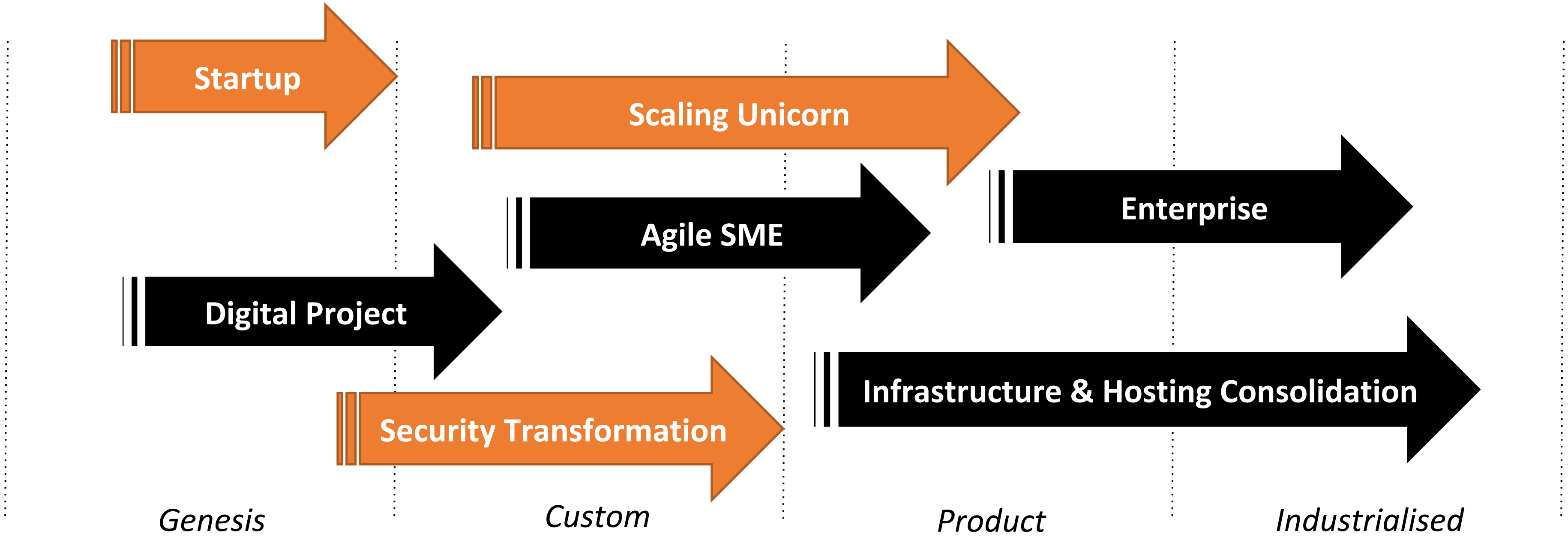
The Attitudes required by Squads will evolve over time as the organisations changes. As a *Genesis* Startup, staffed by Pioneers, evolves into a *Custom* Scaling Unicorn, the Attitudes will need to change to a mix of Pioneers and Settlers, as the organisation starts to scale up, eventually changing to a *Product* Scaling Unicorn, as the Pioneers move out and Towner Planners are brought in, to streamline and mature the operations.



Cell-based Organisations:
Attitudes within Enterprise Squads

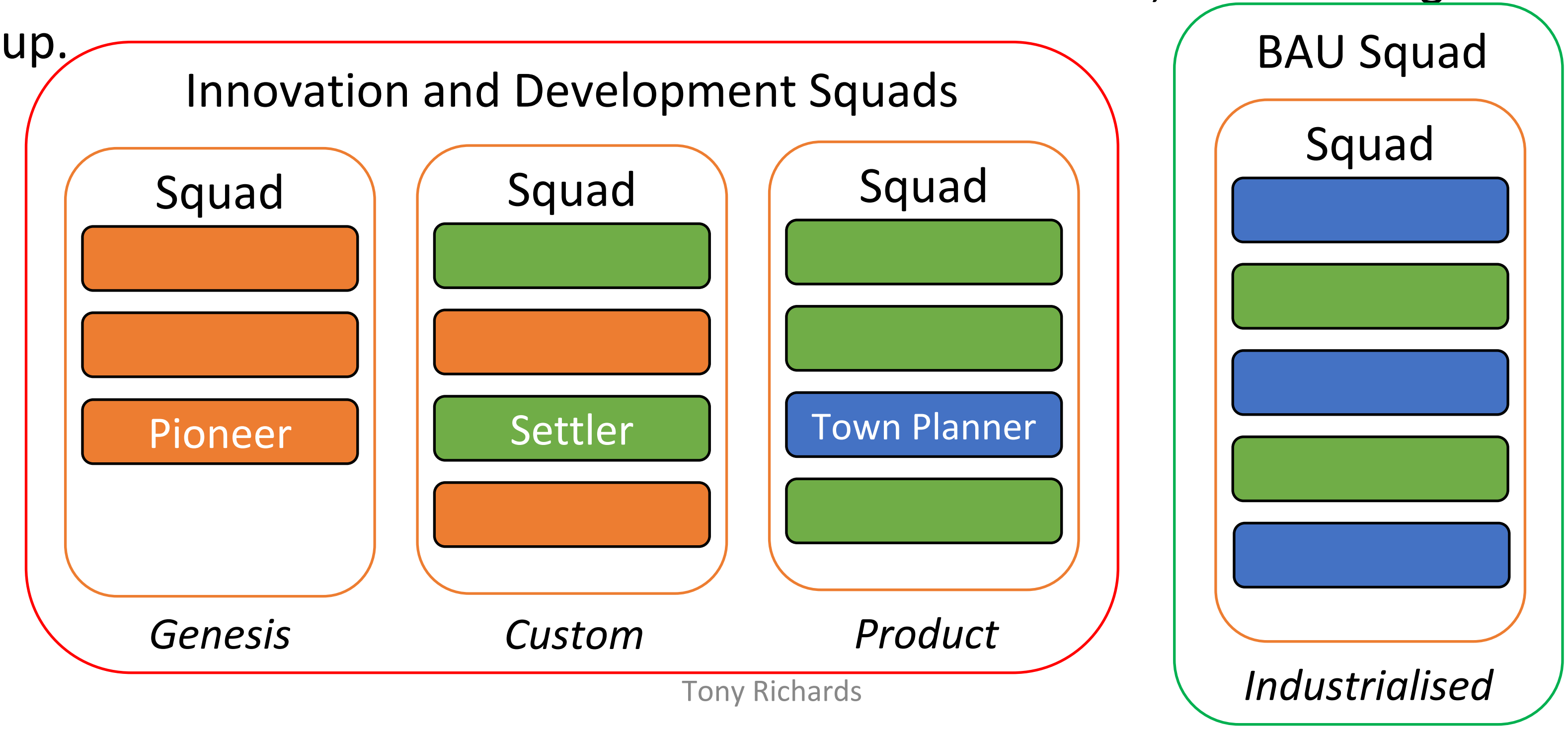
The Attitudes required by Squads in large enterprises will be diverse, depending on the projects and programs starting or underway.

Genesis Digital projects will inevitably require Pioneers, while *Custom* Security Transformation Programs will need a mix of Pioneers and Settlers to innovate and implement the transformation of the organisation. *Product* and *Industrialised* projects such as infrastructure builds or hosting consolidations will require Towner Planners to streamline and mature the operations.



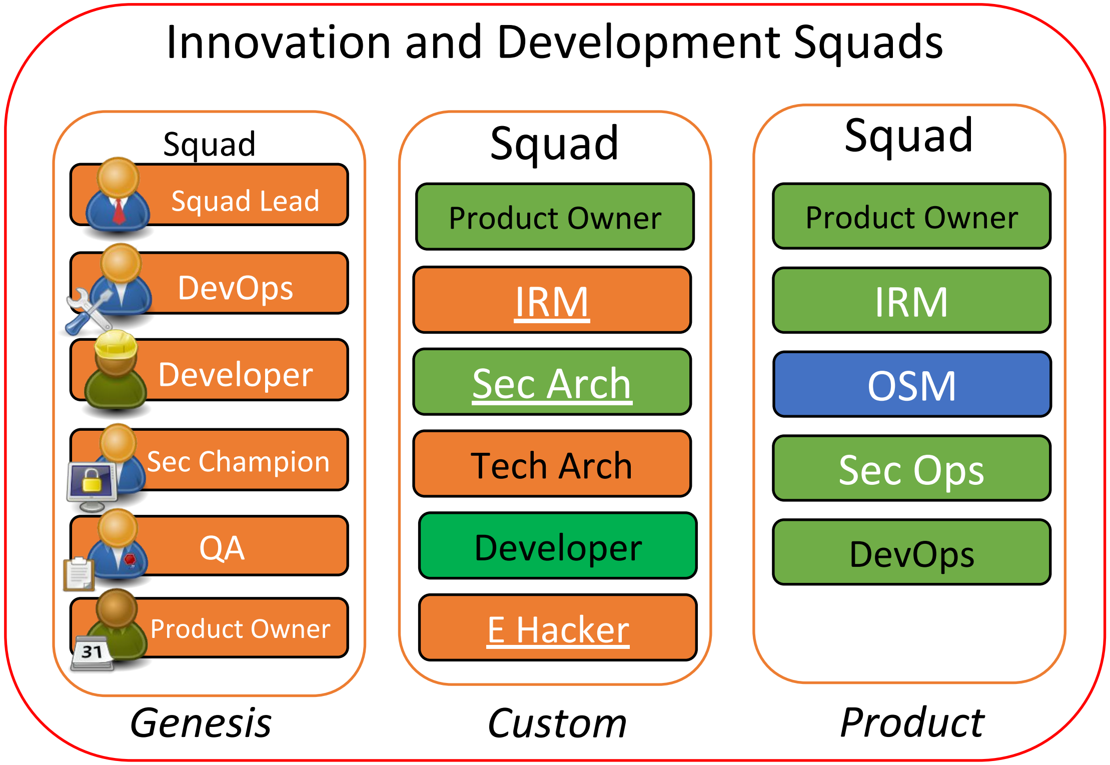
Cell-based Organisations:
Attitudes within Development Squads

As Development Squad missions evolve over time, the makeup of the squads roles and attitudes will change. Starting with initial *Genesis* Squads, comprised of Pioneers, who discover the User Needs, develop agile MVPs (Minimum Viable Product) and deliver the Alpha phase. These will morph into *Custom* Squads, who start to mature the development through Beta phases into early Live and could be made up of a mix of Pioneer and Settler attitudes. *Product* Squads will inevitably be formed of a mixture of Settlers and and a few Town Planners, streamlining and scaling up.



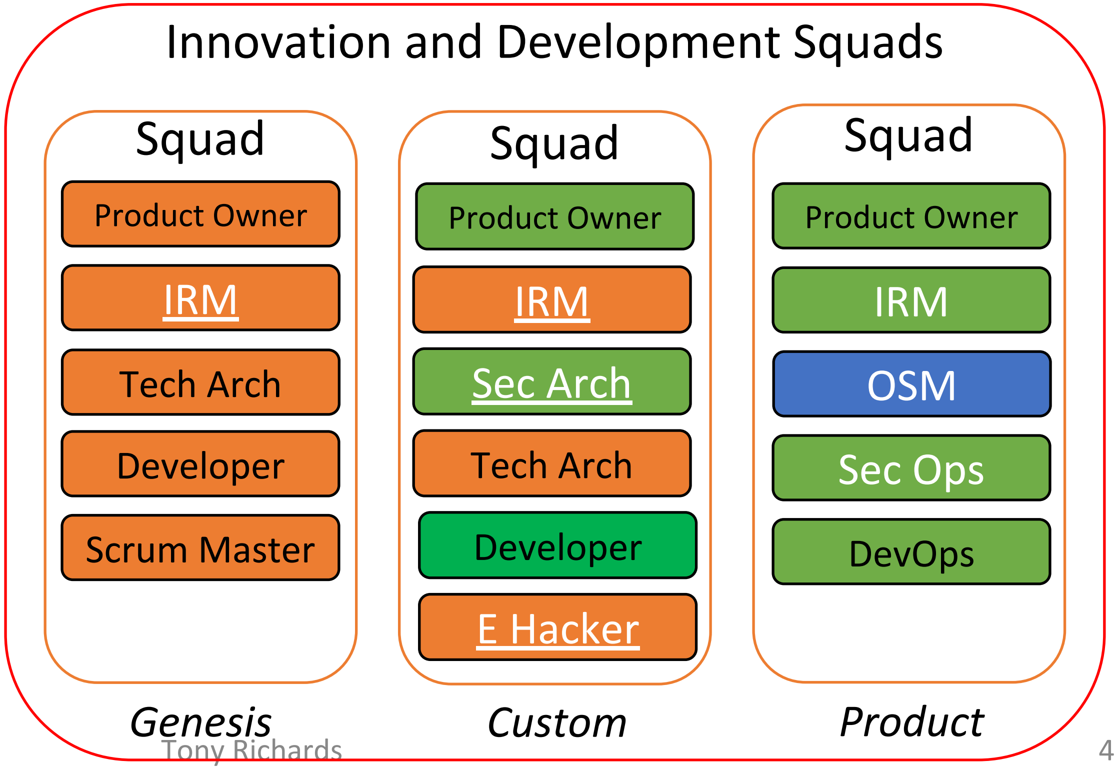
Cell-based Organisations: Security Aptitudes and Attitudes within *Genesis* Development Squads

Working within initial *Genesis* Squads who discover User Needs, develop agile MVPs and deliver the Alpha phase, the Security Aptitude Roles will consist of Pioneer Attitudes who are required to understand the risk environment, develop the initial User Security Needs, to develop the Minimum Viable Security outcome needed.



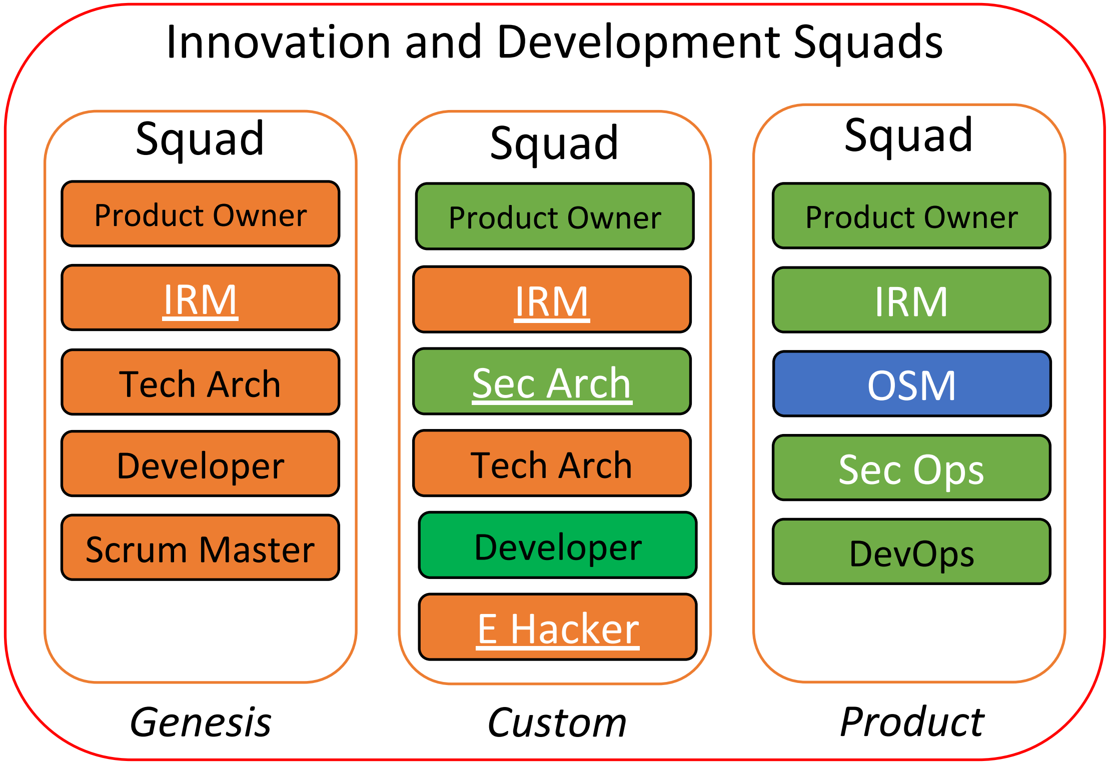
Cell-based Organisations: Security Aptitudes and Attitudes within *Custom* Development Squads

As the program evolves, *Genesis* Squads will morph into *Custom* Squads, who start to mature the development through Beta phases into early Live. The Security Aptitude Roles involved in the development will increase, involving a more diverse range of skills, and attitudes will evolve into a of mix of Pioneers and Settlers, as aspects of the design are stablised, elements assured, but with development still evolving.



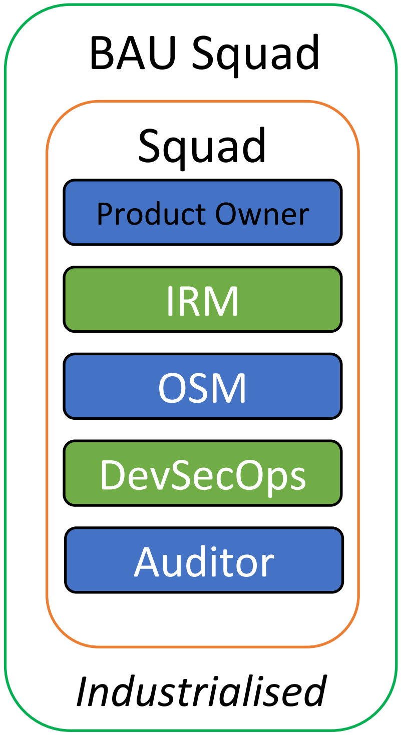
Cell-based Organisations:
Security Aptitudes and Attitudes
within *Product* Development Squads

Product Squads will inevitably be formed of a mixture of Settlers and a few Town Planners, streamlining the service and scaling up, or out, the program. The Security Aptitude Roles will start to include mature security services, such as Security Operations, and incorporate Standardised practices.



Cell-based Organisations: Security Aptitudes and Attitudes within Industrialised Development Squads

Product Squads will eventually evolve into a *Industrialised* Squad, staffed with Town Planners and maybe the odd Settler. The program will be mature and efficient, and undoubtedly be following standardised and mature practices such as ITIL. The Security Aptitude Roles will include mature security services, such as scheduled auditing.



Cell-based Organisations:

Aptitudes and Security Functions (DRAFT)

Cell-based Organisations:
Security Attitudes and Aptitudes

Security Functions		Attitudes		
		Pioneers	Settlers	Town Planners
Aptitudes	Coordination	Agile / Scrum	Lean / Prince2	Six Sigma / ITIL
	Information Risk	Service Provider Security / Common Solutions	Common Solutions / Risk Assessment & Controls	Risk Assessment & Controls / Threat Tree Analysis
	Operational Security			SOC/SIEM
	Sec. Architecture	Principles / Stories	Best Practice / Patterns	TDA/ SABA / TOGAF
	Application Security	Security Stories / MVS	Security EPICS / External Requirements	Security Requirements
	Security Testing	Automated Tools / Continuous Testing	Continuous / Multi-level Testing / Pen-Testing	Continuous / Multi-level / Red Teaming / Integrated SOC
	Audit & Assurance	Assurance / Benchmark	Definition of Done / Control Library	Controls / Standards / Compliance
	Security Culture			
Development Phase		Discovery / Alpha	Beta / Live	Live / Legacy
		Pilot / MVP	Scaling / Maturing	Industrial / Platform

Tony Richards

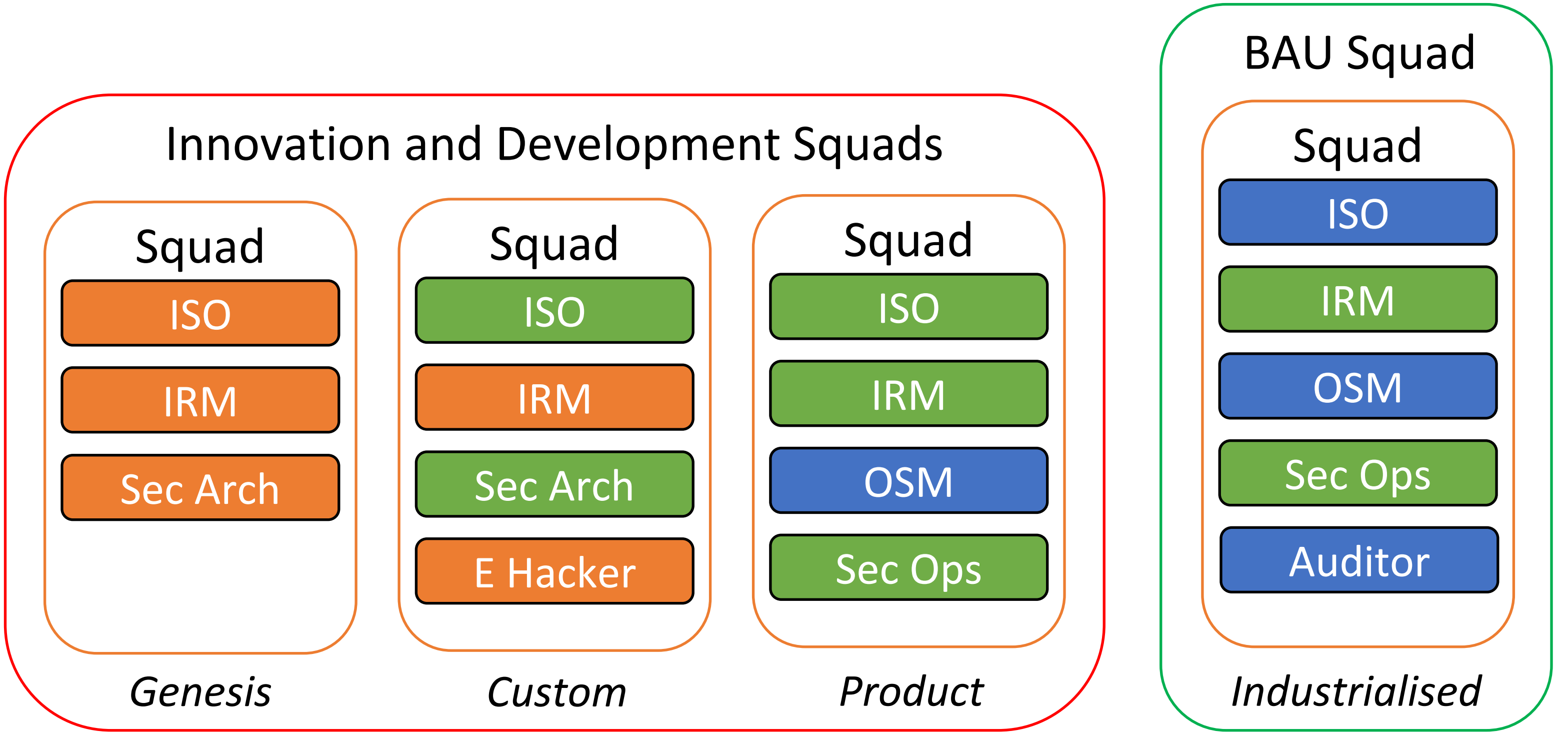
Cell-based Organisations:
Security Functions

Security Functions	Function Grades		
Coordination / Management	-	-	Squad Coordinator
Information Risk	Risk Analyst	Risk Advisor	Risk Manager
Operational Security	OpSec Analyst	OpSec Advisor	OpSec Manager
Security Architecture	-	Security Architect	Senior Security Architect
Application Security	Security Specialist	Security Engineer	Senior Security Engineer
Security Testing	-	Team Member	Team Leader
Audit / Assurance / Compliance	Security Reviewer	Auditor	Senior Auditor
Chapters			

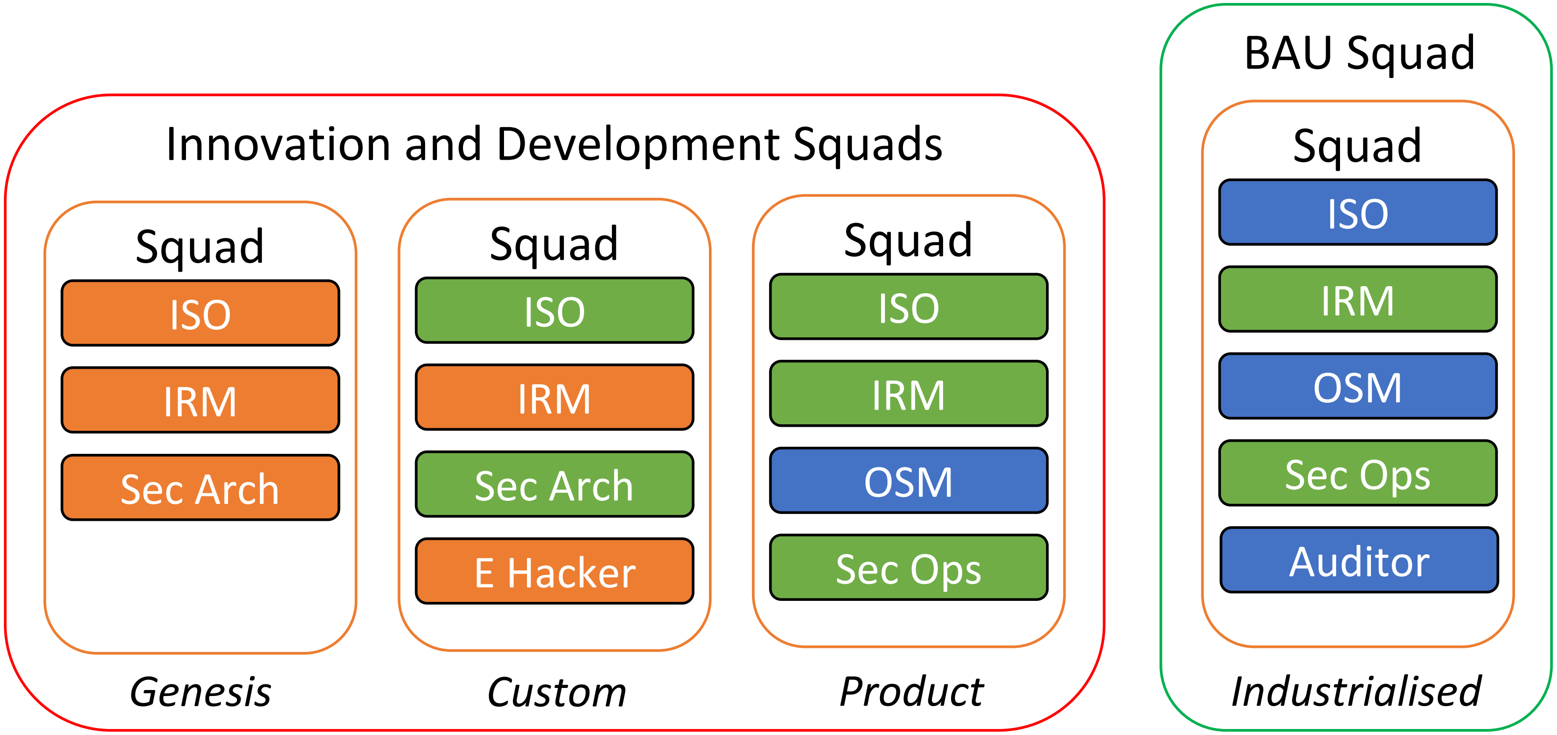
Security Aptitudes and Attitudes (DRAFT)

Cell-based Organisations: Security Aptitudes and Attitudes within a *Genesis* Security Team Mission - DRAFT

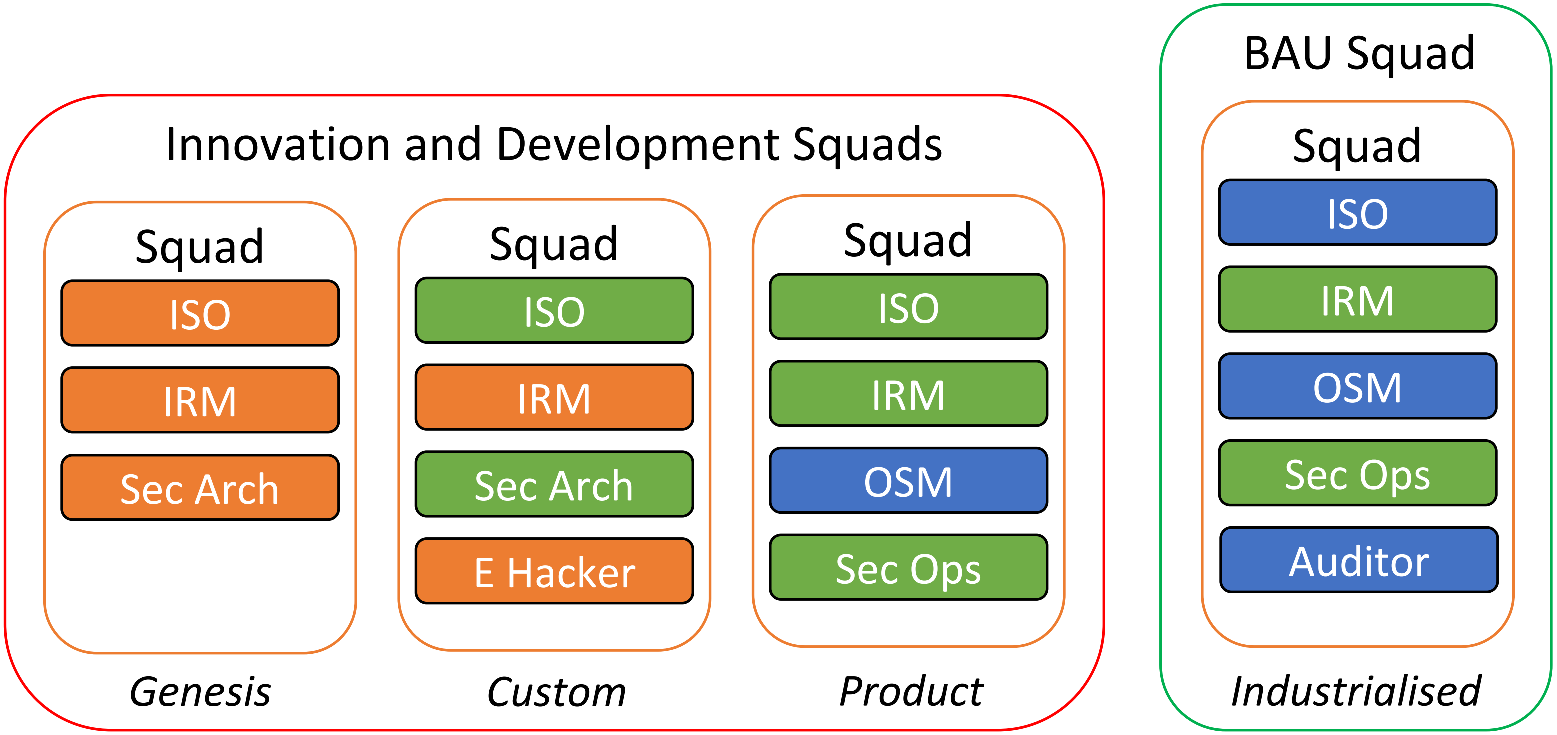
As Squad missions evolve over time, the makeup of Squad security roles and attitudes will change.



Cell-based Organisations:
Security Aptitudes and Attitudes within a *Custom* Security Team Mission - DRAFT



Cell-based Organisations:
Security Aptitudes and Attitudes within a *Product* Security Team Mission - DRAFT



Cell-based Organisations:

Continuous Risk Management (DRAFT)

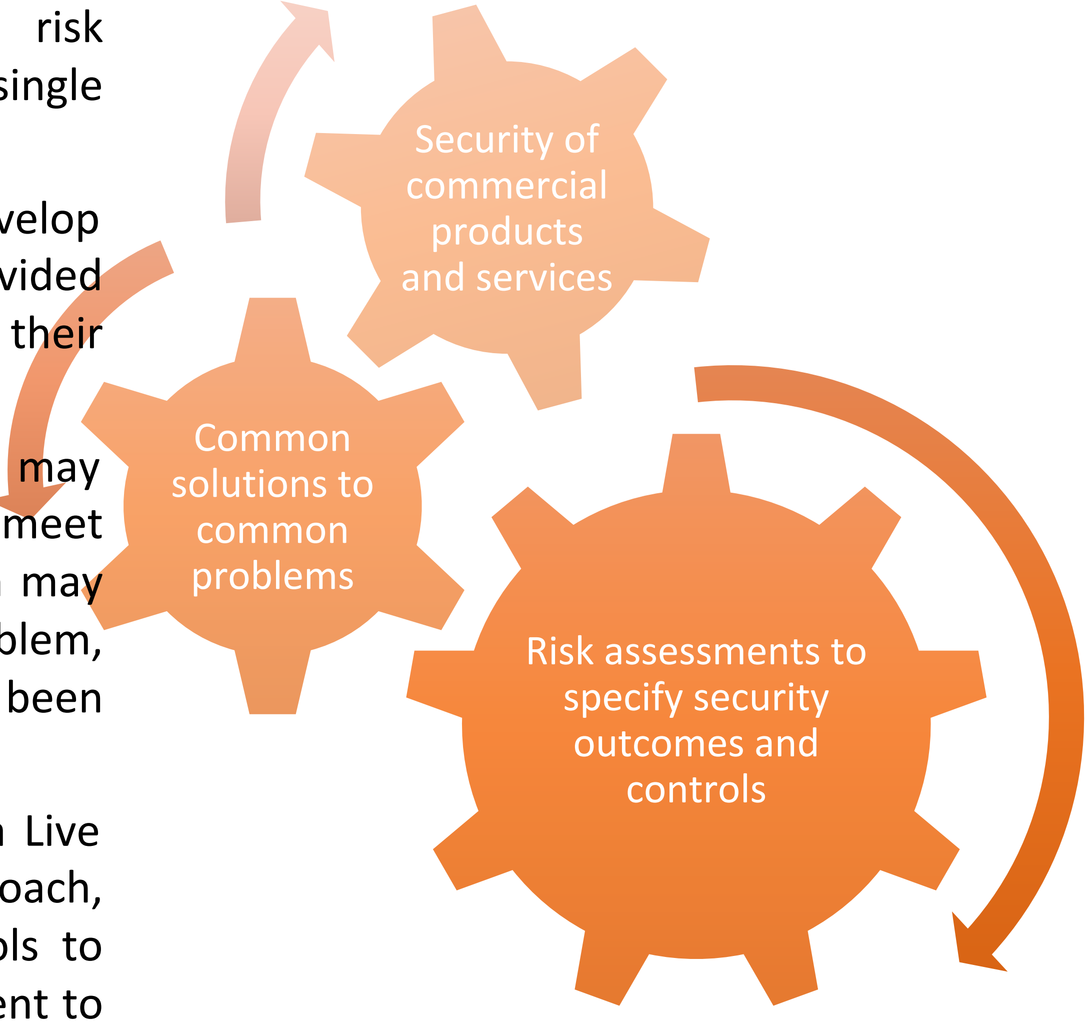
Cell-based Organisations:
Using Continuous Risk Management with Squads

To provide continuous information risk management in evolving environments, no single risk approach is suitable. As examples:

A *Genesis* Squad in an Alpha Phase can develop an MVP, relying on the inherent security provided by a commercial cloud platform to meet their initial User Security Needs.

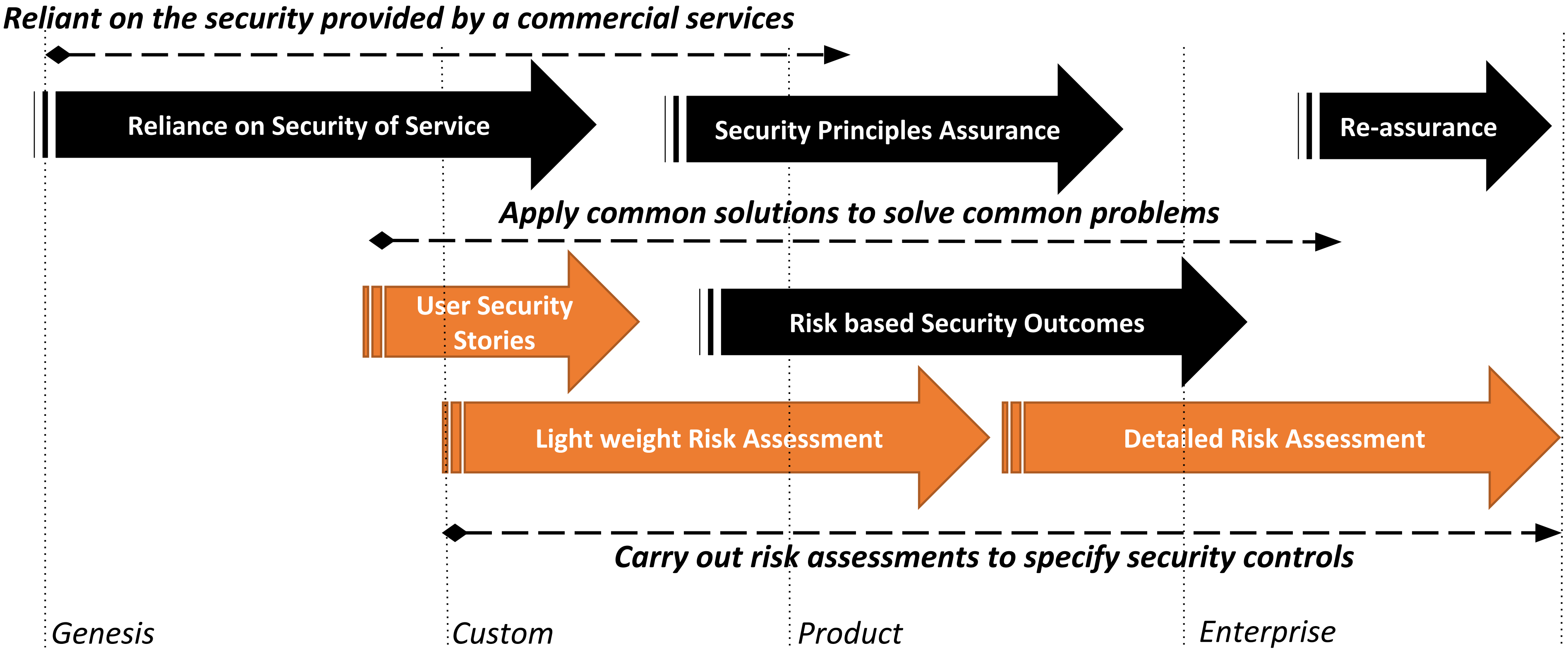
A *Custom* Squad however, in a Beta Phase, may require more assurance of the solution, to meet external security requirements, and as such may apply a common solution to a common problem, as sufficient security assurance has been conducted by another entity.

A *Product* Squad on the other hand, with a Live service, will need a stable and mature approach, therefore defining a set of security controls to meet the outcomes of a risk based assessment to meet known threats.


Security of commercial products and services
Common solutions to common problems
Risk assessments to specify security outcomes and controls

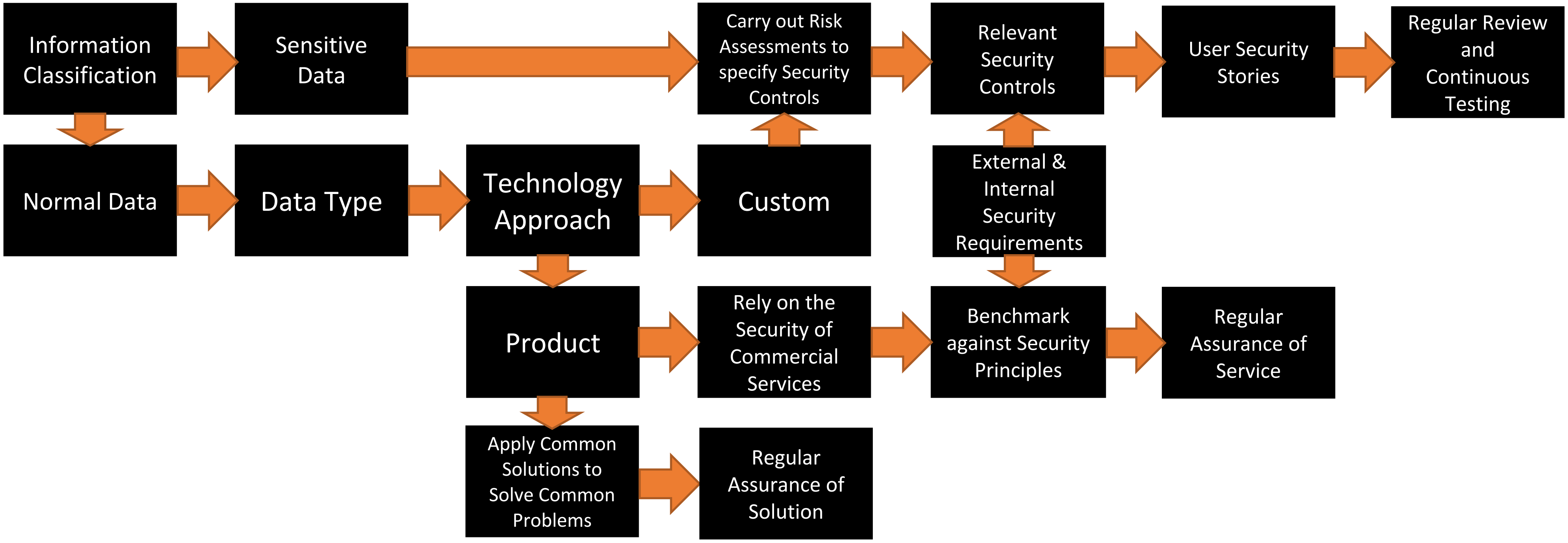
Cell-based Organisations: Continuous Risk Management Evolution

To provide continuous, information risk management in evolving environments, no single risk assessment approach is suitable. A range of different approaches relevant at the point in time of the project can be used.


Reliant on the security provided by a commercial services
Reliance on Security of Service
Security Principles Assurance
Re-assurance
Apply common solutions to solve common problems
User Security Stories
Risk based Security Outcomes
Light weight Risk Assessment
Detailed Risk Assessment
Carry out risk assessments to specify security controls
Genesis
Custom
Product
Enterprise

Cell-based Organisations:
Continuous Risk Management Approach

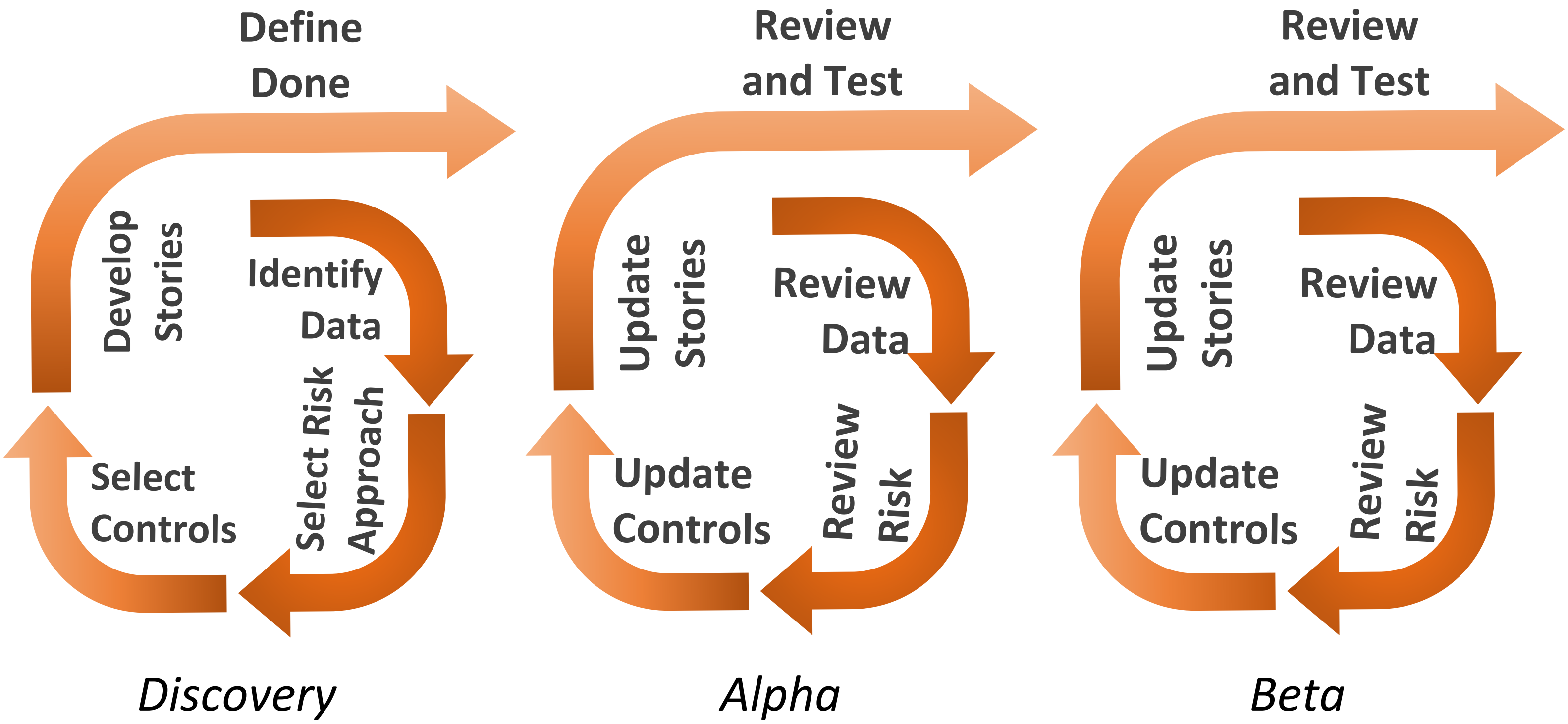
To identify the most appropriate risk management approach to use, the business context must be understood.



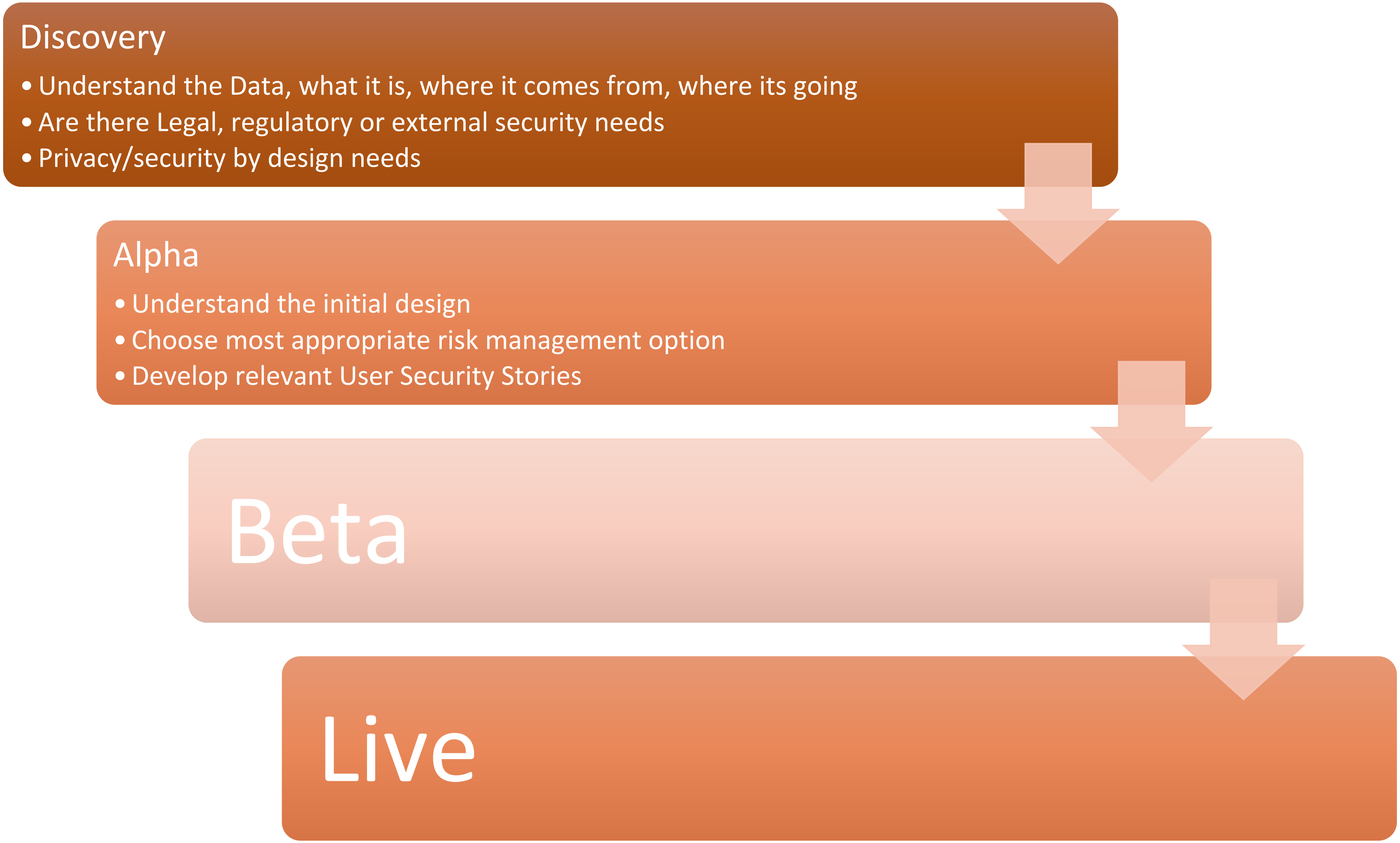
Information Classification
Sensitive Data
Carry out Risk Assessments to specify Security Controls
Relevant Security Controls
User Security Stories
Regular Review and Continuous Testing
Normal Data
Data Type
Technology Approach
Custom
External & Internal Security Requirements
Product
Rely on the Security of Commercial Services
Benchmark against Security Principles
Regular Assurance of Service
Apply Common Solutions to Solve Common Problems
Regular Assurance of Solution

Cell-based Organisations:
Continuous Risk Management Approach

For each phase of the development cycle, risk must be reassessed and adjustments made.



Cell-based Organisations:



Discovery

- Understand the Data, what it is, where it comes from, where its going
- Are there Legal, regulatory or external security needs
- Privacy/security by design needs

Alpha

- Understand the initial design
- Choose most appropriate risk management option
- Develop relevant User Security Stories

Beta

Live