Your fastest way to learn. Why wait?

FIREBRAND

# ISACA

## CISM Certification

## Certified Information Security Manager Courseware

Courseware version 6.2

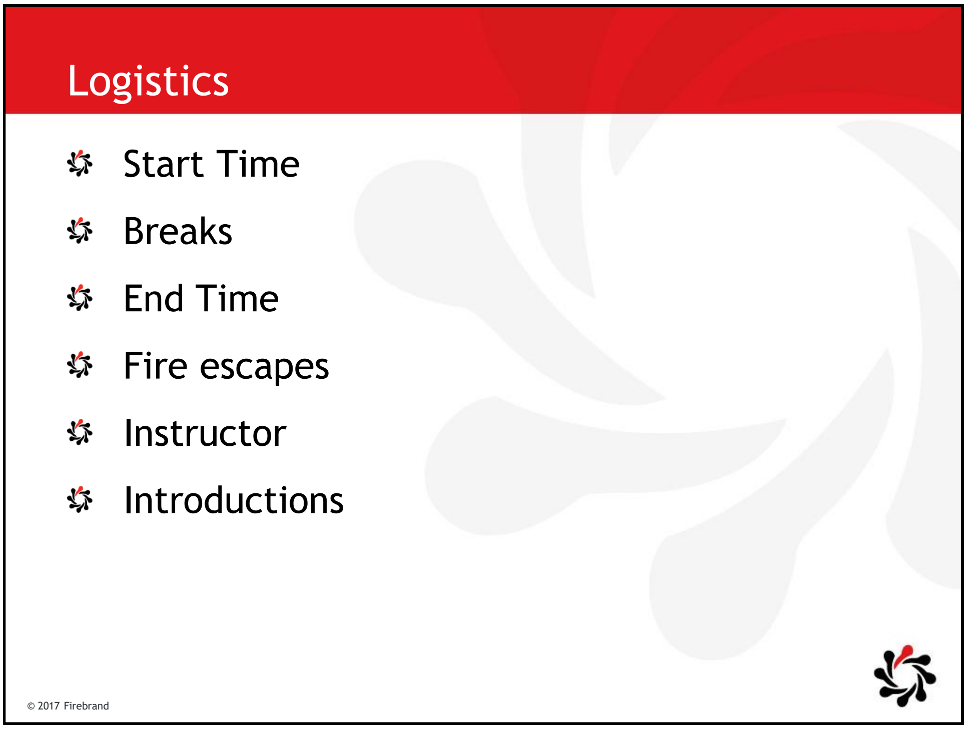
Kit Code: K-106-01

www.firebrandtraining.co.uk

# CISM™

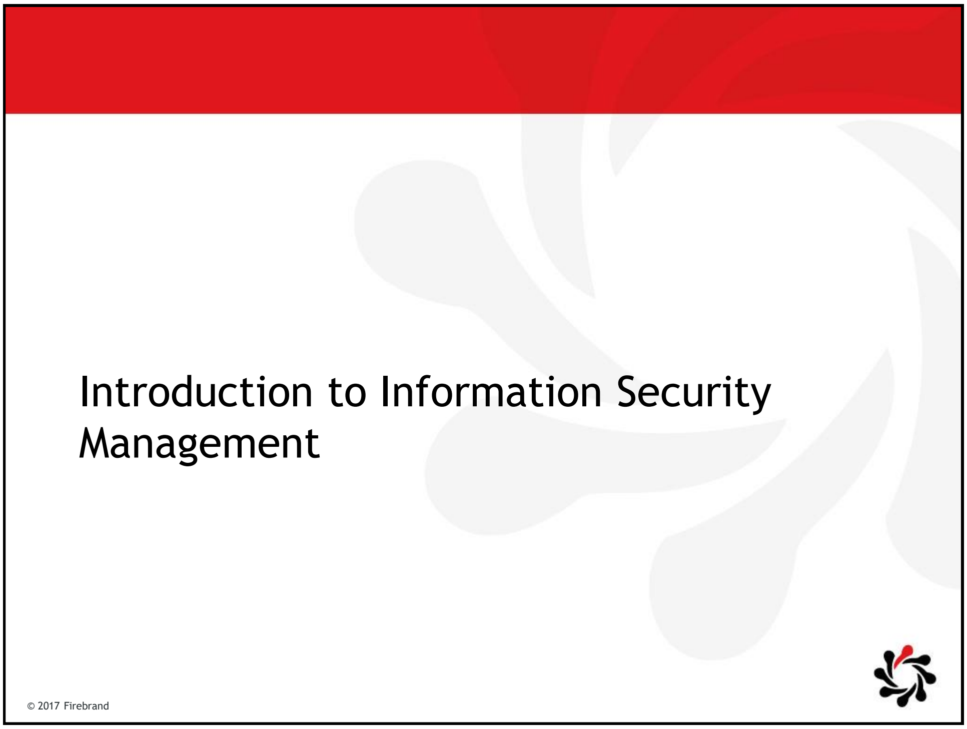
## Certified Information Security Manager

Firebrand Custom Designed Courseware

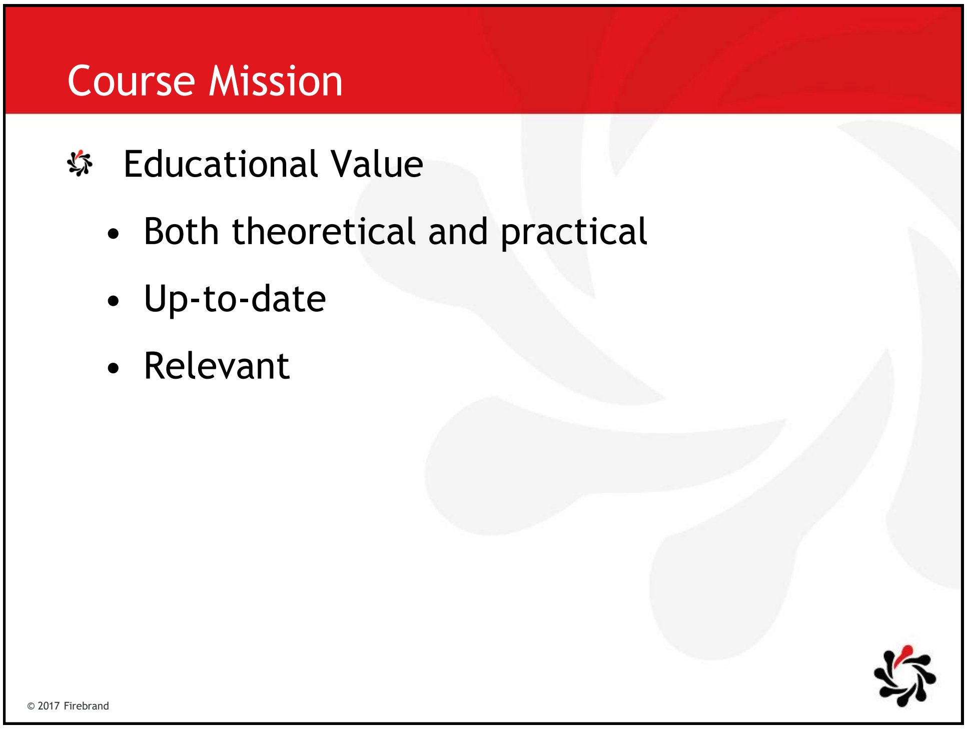


## Logistics

- Start Time
- Breaks
- End Time
- Fire escapes
- Instructor
- Introductions

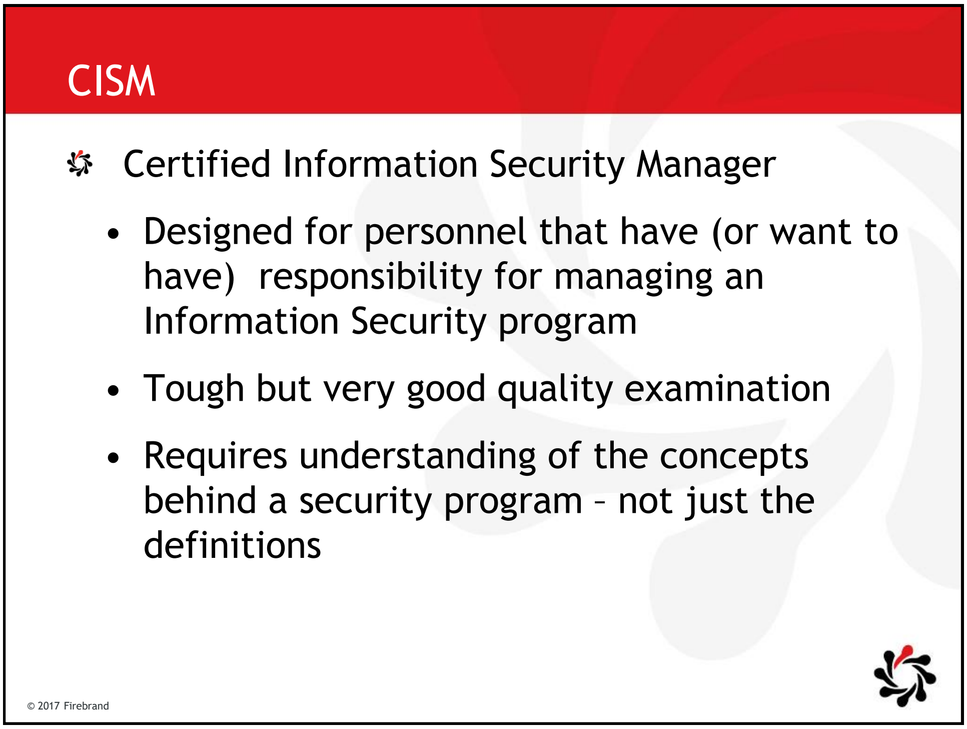


## Introduction to Information Security Management



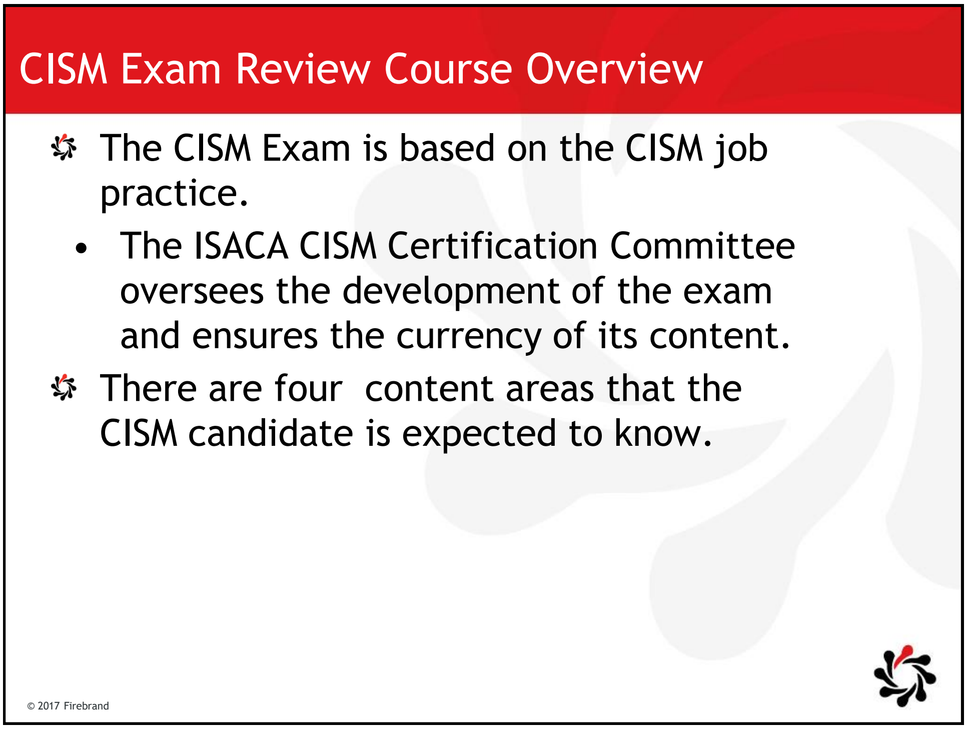
## Course Mission

- Educational Value
  - Both theoretical and practical
  - Up-to-date
  - Relevant



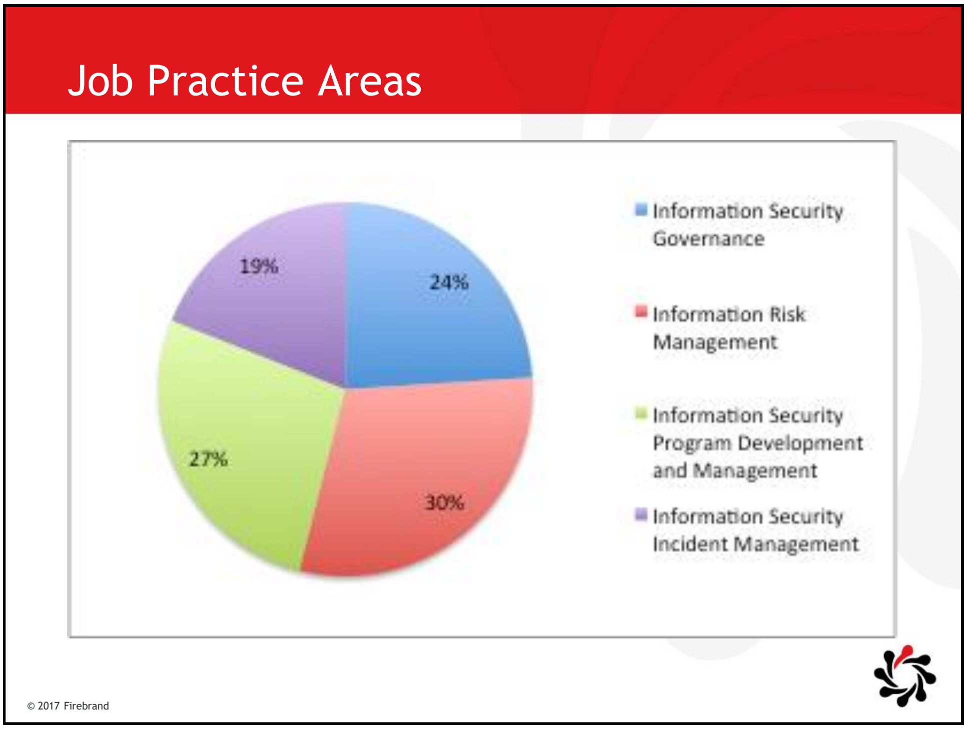
## CISM

- Certified Information Security Manager
  - Designed for personnel that have (or want to have) responsibility for managing an Information Security program
  - Tough but very good quality examination
  - Requires understanding of the concepts behind a security program – not just the definitions

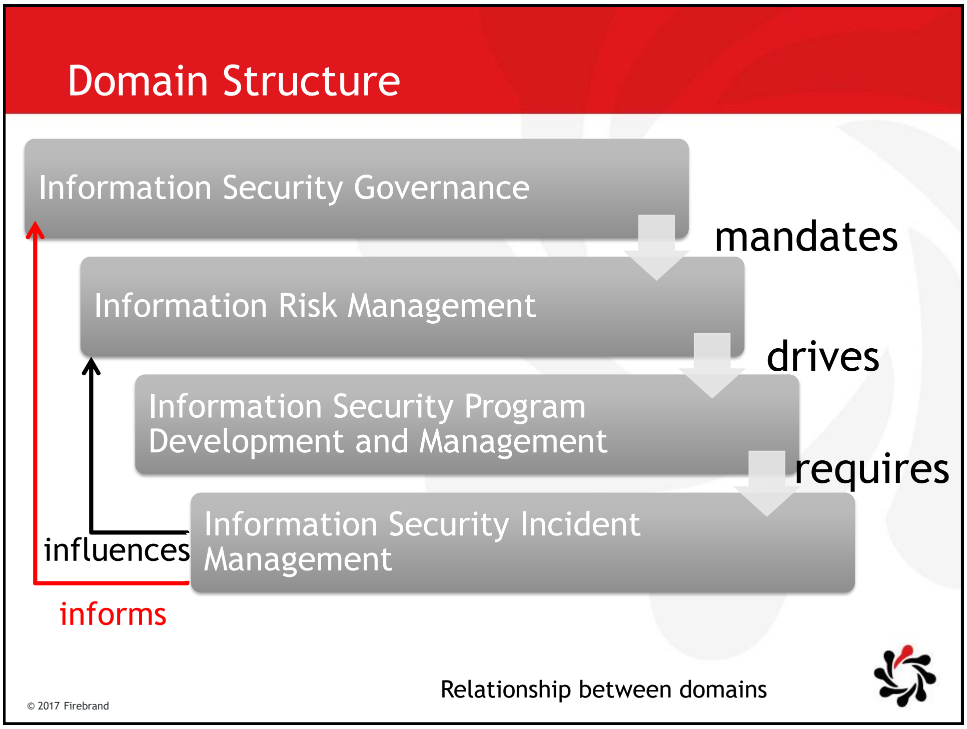


## CISM Exam Review Course Overview

- The CISM Exam is based on the CISM job practice.
  - The ISACA CISM Certification Committee oversees the development of the exam and ensures the currency of its content.
- There are four content areas that the CISM candidate is expected to know.



## Job Practice Areas



## Domain Structure

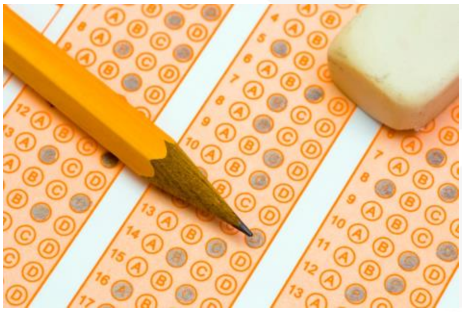
Information Security Governance
mandates
Information Risk Management
drives
Information Security Program Development and Management
requires
Information Security Incident Management
influences
informs

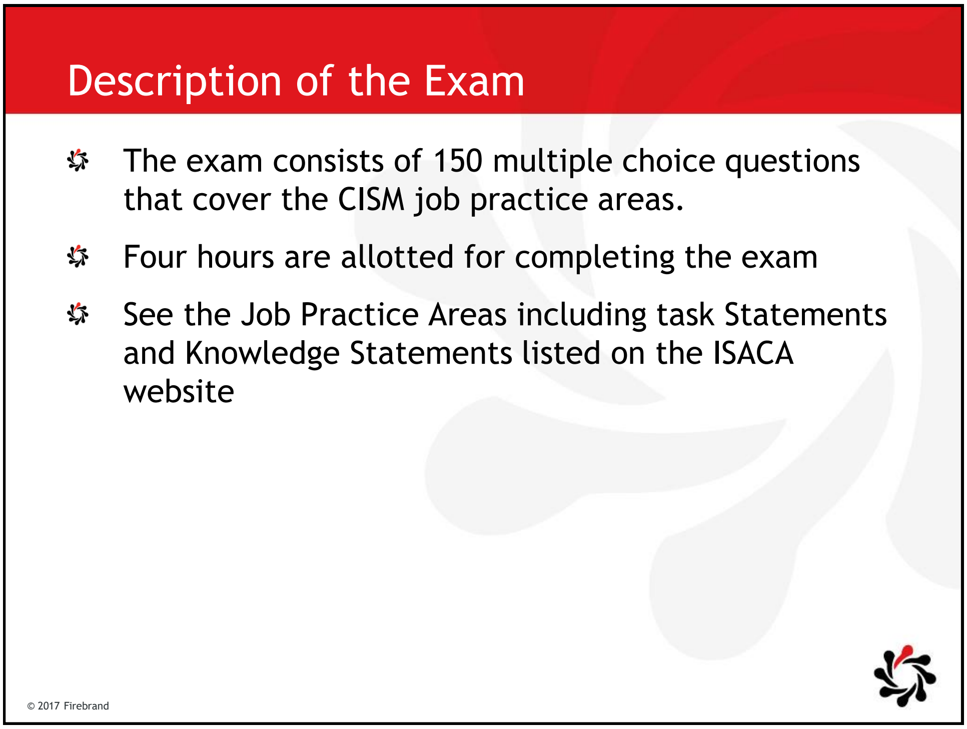
Relationship between domains

## CISM Qualifications

- To earn the CISM designation, information security professionals are required to:
  - Successfully pass the CISM exam
  - Adhere to the ISACA Code of Professional Ethics
  - Agree to comply with the CISM continuing education policy
  - Submit verified evidence of five (5) years of work experience in the field of information security.
    - Waivers are permitted for certifications

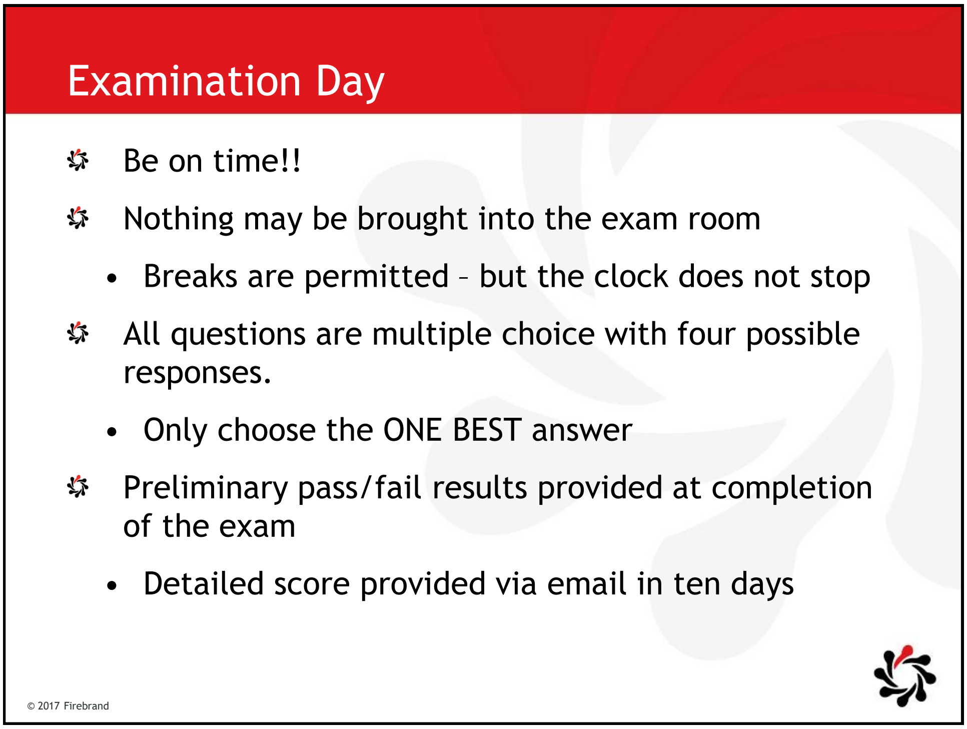
# The Examination





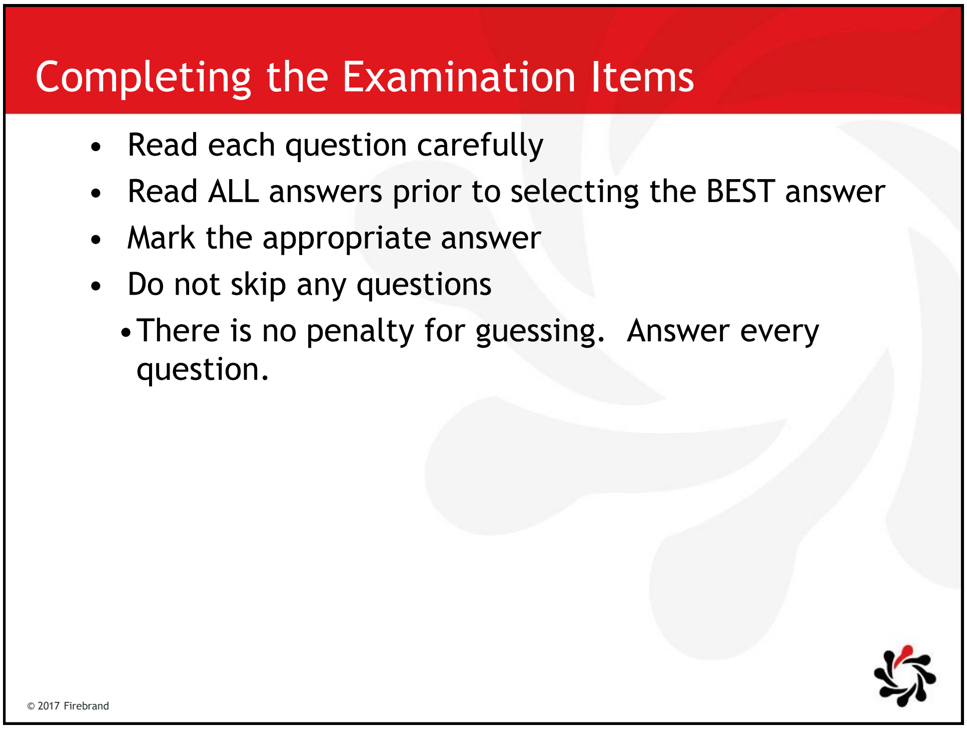
## Description of the Exam

- The exam consists of 150 multiple choice questions that cover the CISM job practice areas.
- Four hours are allotted for completing the exam
- See the Job Practice Areas including task Statements and Knowledge Statements listed on the ISACA website



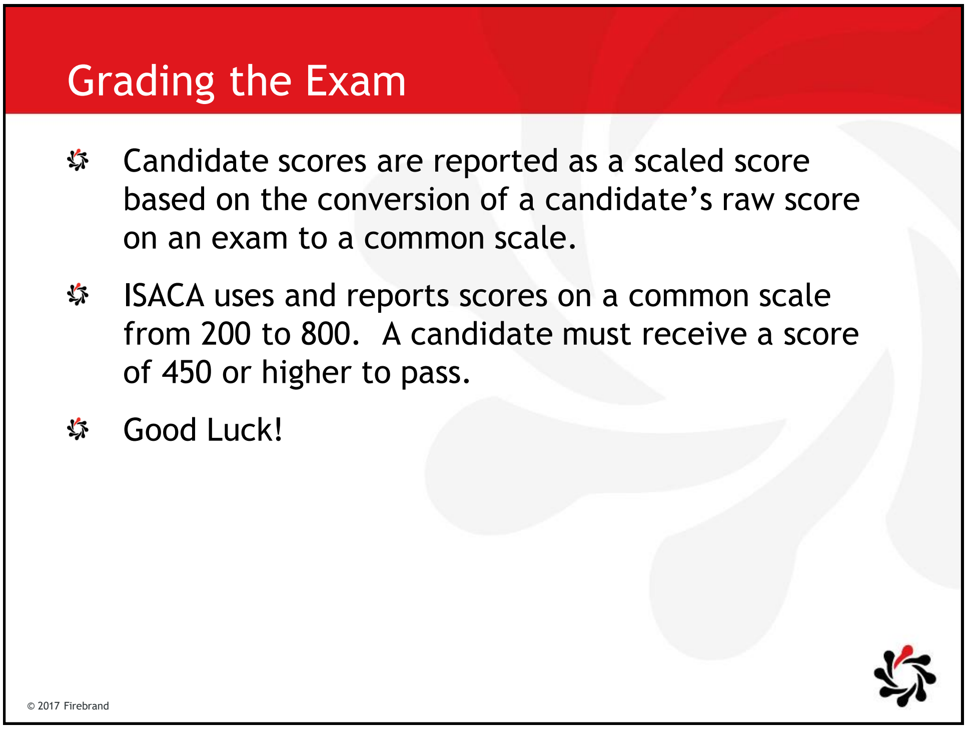
## Examination Day

- Be on time!!
- Nothing may be brought into the exam room
  - Breaks are permitted – but the clock does not stop
- All questions are multiple choice with four possible responses.
  - Only choose the ONE BEST answer
- Preliminary pass/fail results provided at completion of the exam
  - Detailed score provided via email in ten days



## Completing the Examination Items

- Read each question carefully
- Read ALL answers prior to selecting the BEST answer
- Mark the appropriate answer
- Do not skip any questions
  - There is no penalty for guessing.  Answer every question.

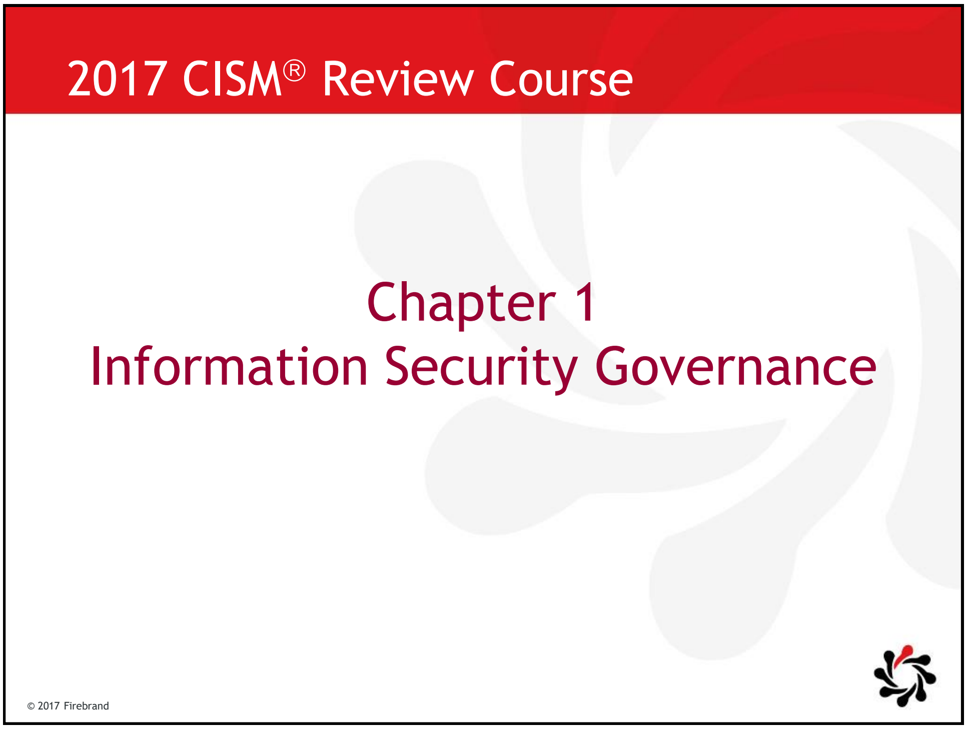


## Grading the Exam

- Candidate scores are reported as a scaled score based on the conversion of a candidate’s raw score on an exam to a common scale.
- ISACA uses and reports scores on a common scale from 200 to 800.  A candidate must receive a score of 450 or higher to pass.
- Good Luck!

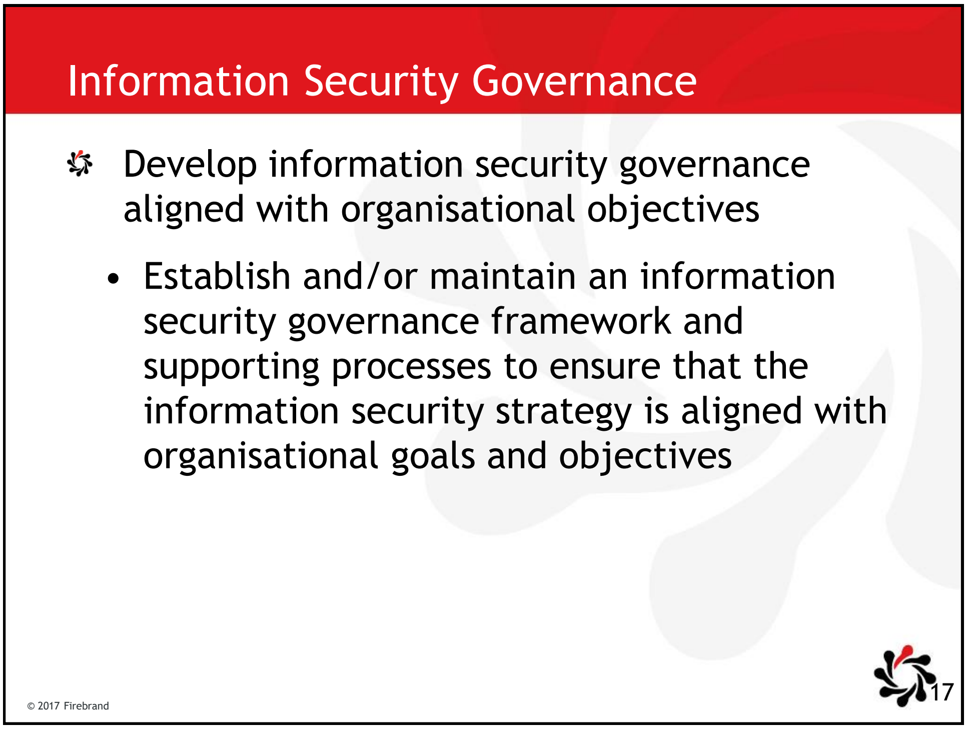
# End of Introduction

- Welcome to the CISM course!!



# 2017 CISM® Review Course

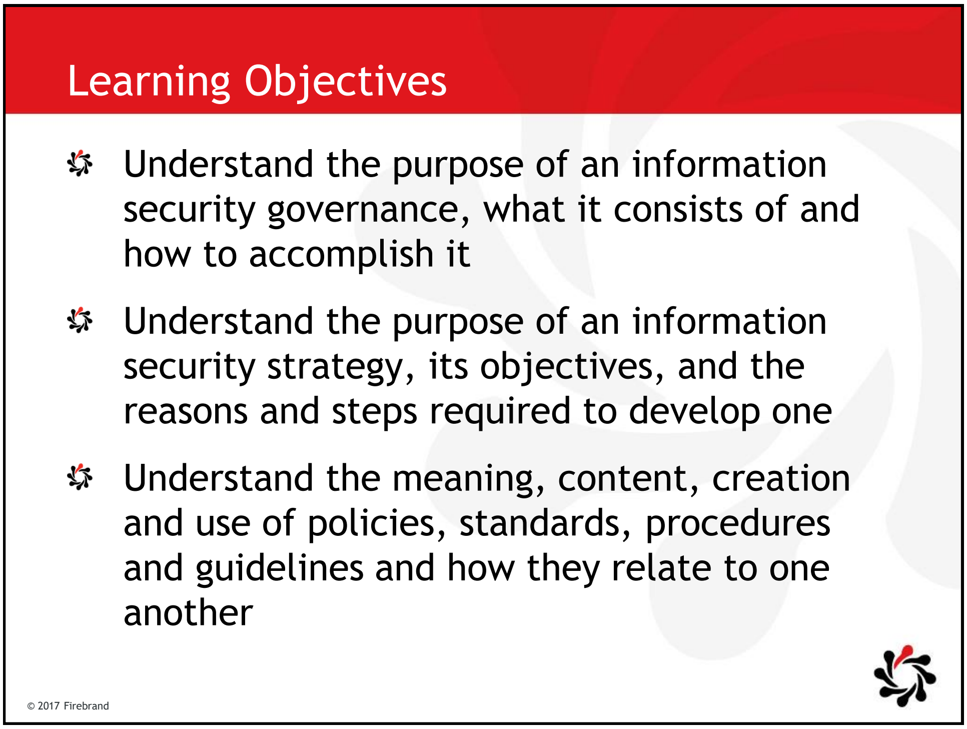
## Chapter 1
## Information Security Governance



## Information Security Governance

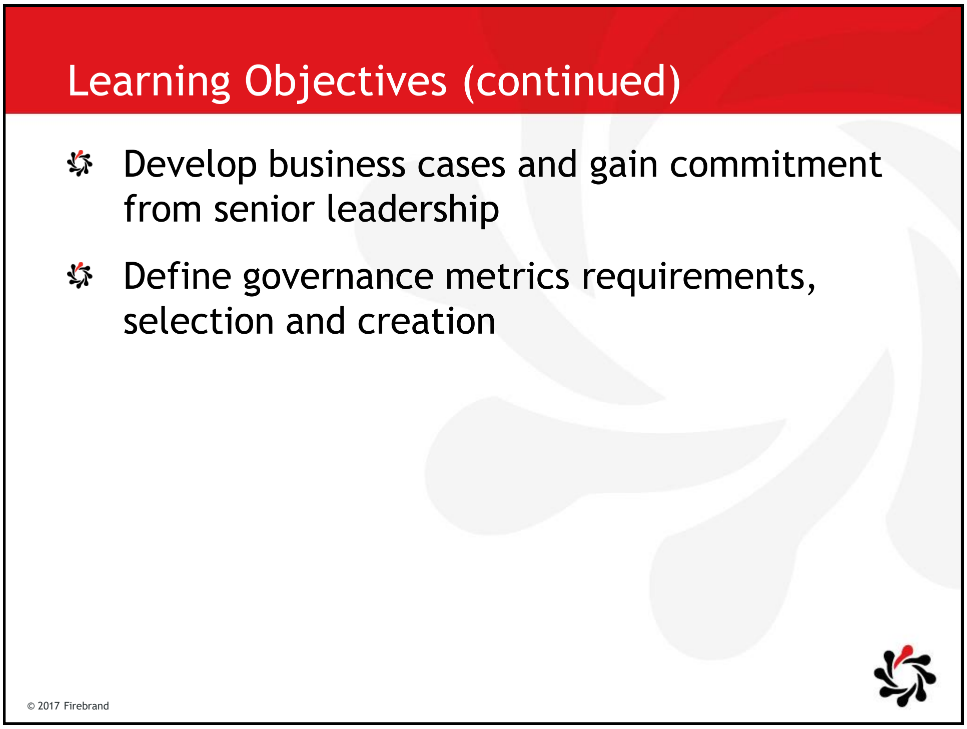
- Develop information security governance aligned with organisational objectives
  - Establish and/or maintain an information security governance framework and supporting processes to ensure that the information security strategy is aligned with organisational goals and objectives

17



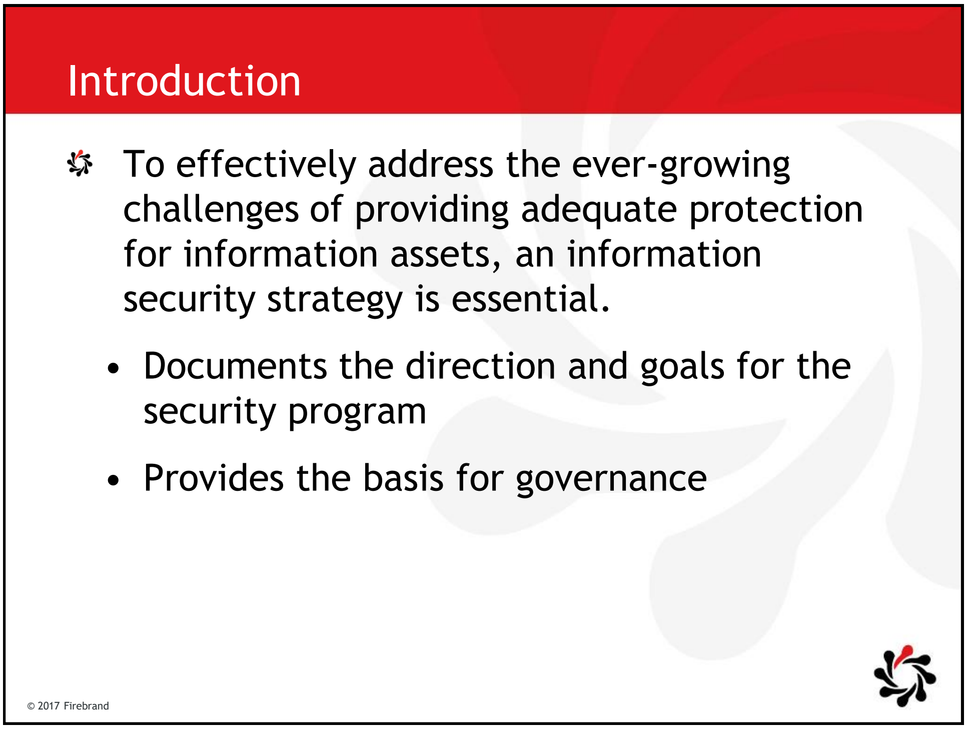
## Learning Objectives

- Understand the purpose of an information security governance, what it consists of and how to accomplish it
- Understand the purpose of an information security strategy, its objectives, and the reasons and steps required to develop one
- Understand the meaning, content, creation and use of policies, standards, procedures and guidelines and how they relate to one another



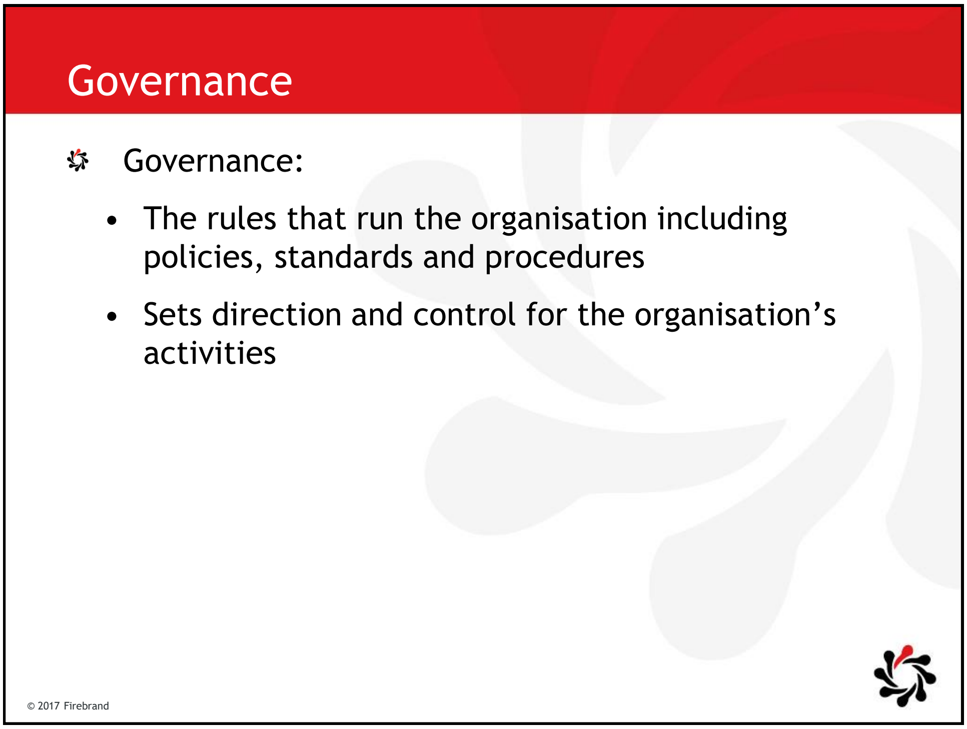
## Learning Objectives (continued)

- Develop business cases and gain commitment from senior leadership
- Define governance metrics requirements, selection and creation



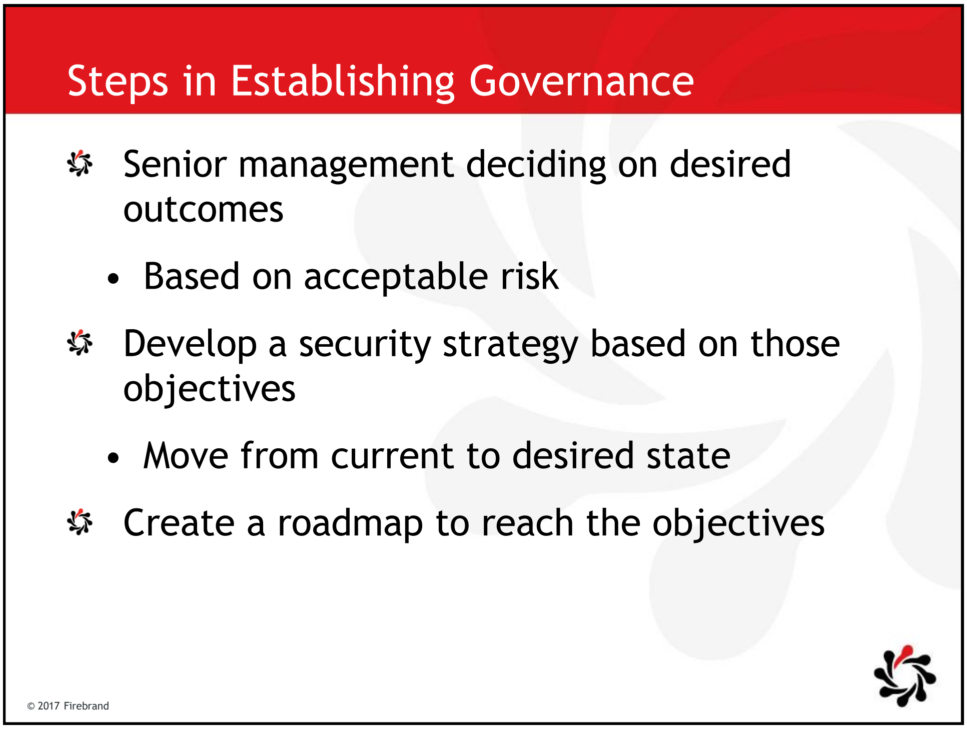
## Introduction

- To effectively address the ever-growing challenges of providing adequate protection for information assets, an information security strategy is essential.
  - Documents the direction and goals for the security program
  - Provides the basis for governance



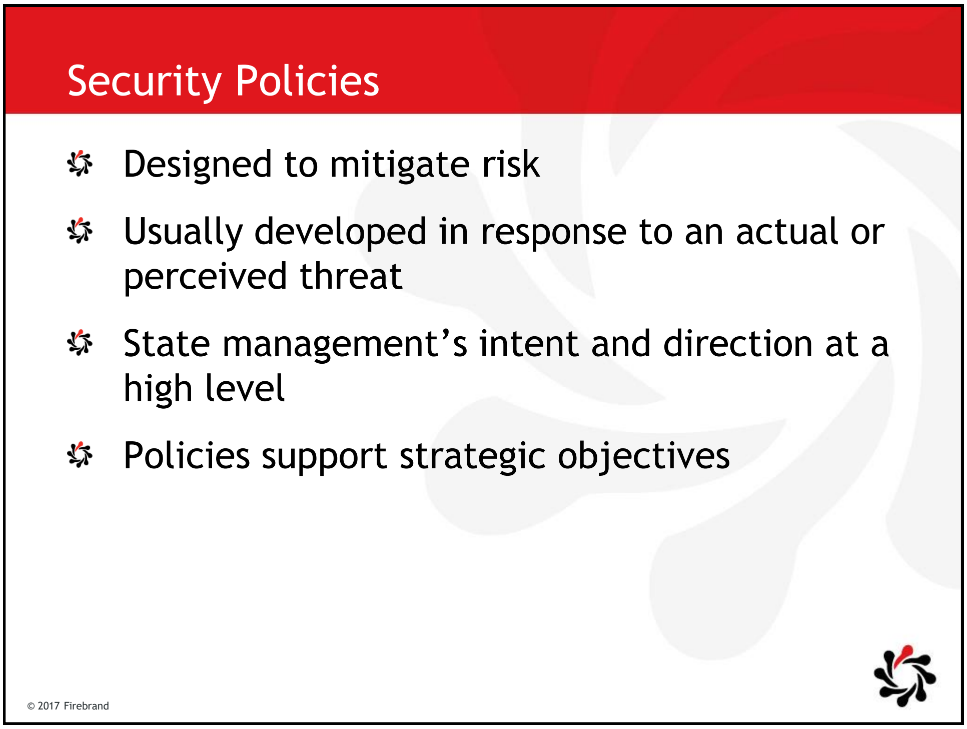
## Governance

- Governance:
  - The rules that run the organisation including policies, standards and procedures
  - Sets direction and control for the organisation’s activities



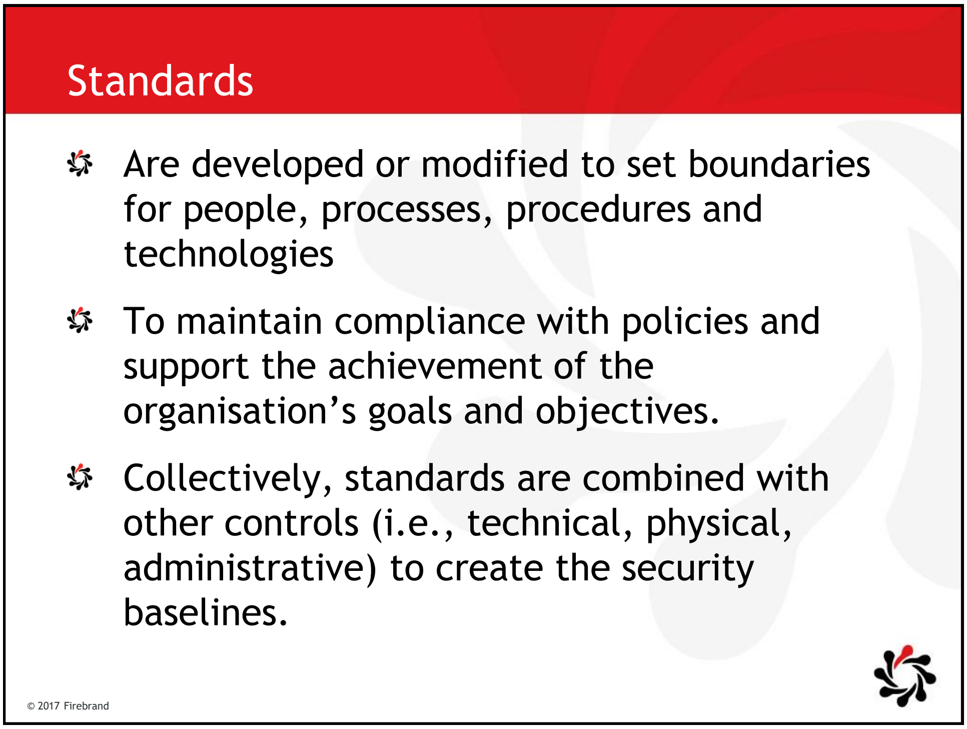
## Steps in Establishing Governance

- Senior management deciding on desired outcomes
  - Based on acceptable risk
- Develop a security strategy based on those objectives
  - Move from current to desired state
- Create a roadmap to reach the objectives



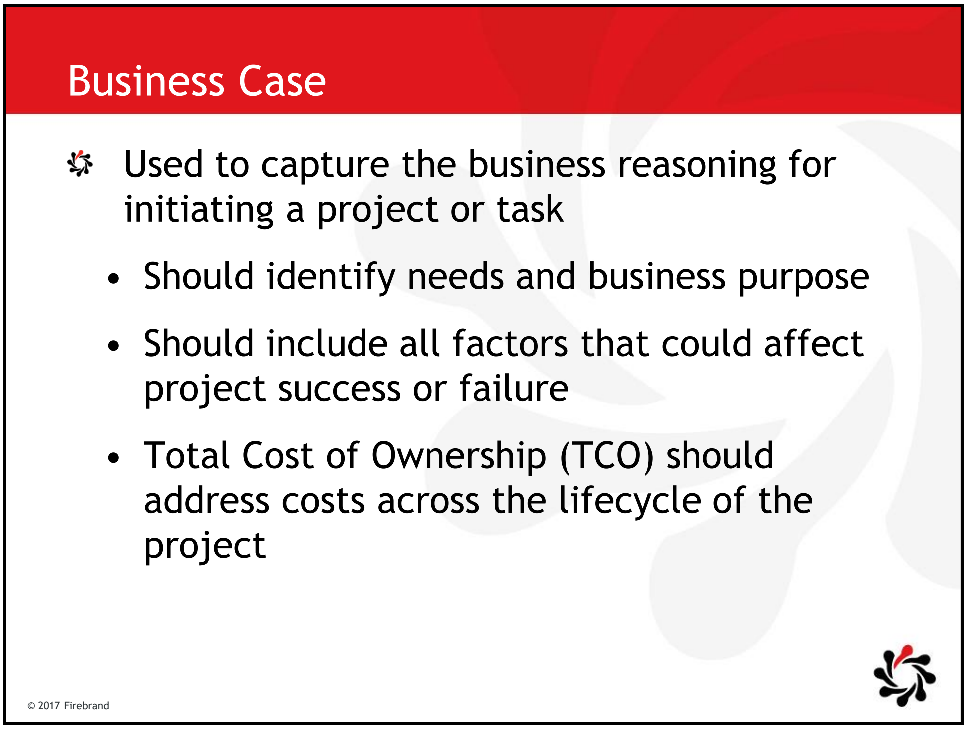
## Security Policies

- Designed to mitigate risk
- Usually developed in response to an actual or perceived threat
- State management’s intent and direction at a high level
- Policies support strategic objectives



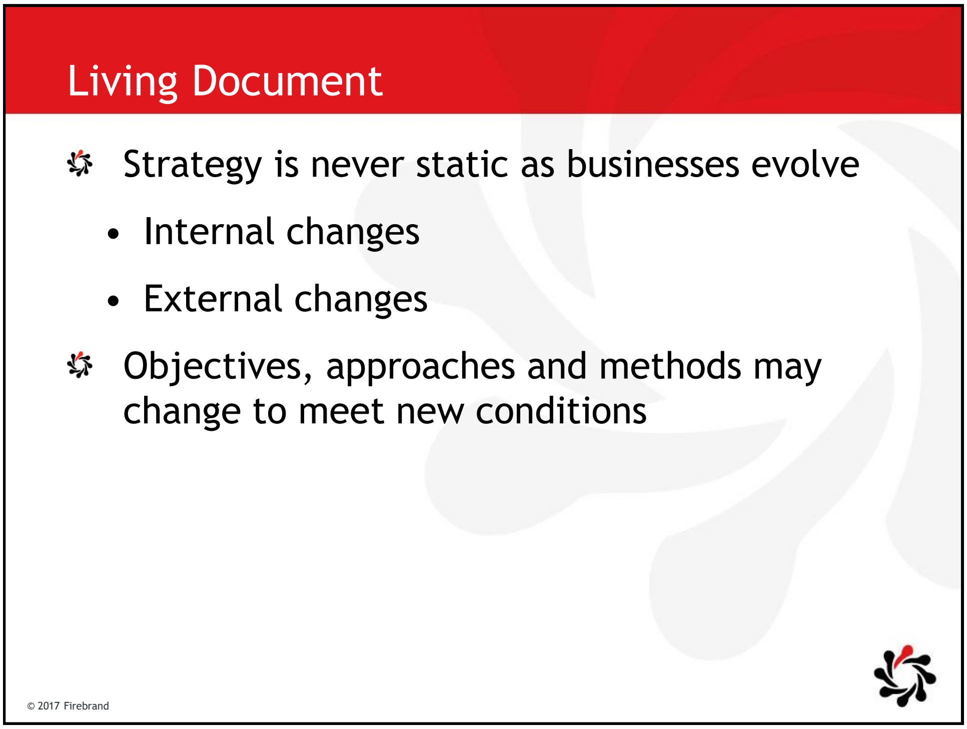
## Standards

- Are developed or modified to set boundaries for people, processes, procedures and technologies
- To maintain compliance with policies and support the achievement of the organisation’s goals and objectives.
- Collectively, standards are combined with other controls (i.e., technical, physical, administrative) to create the security baselines.



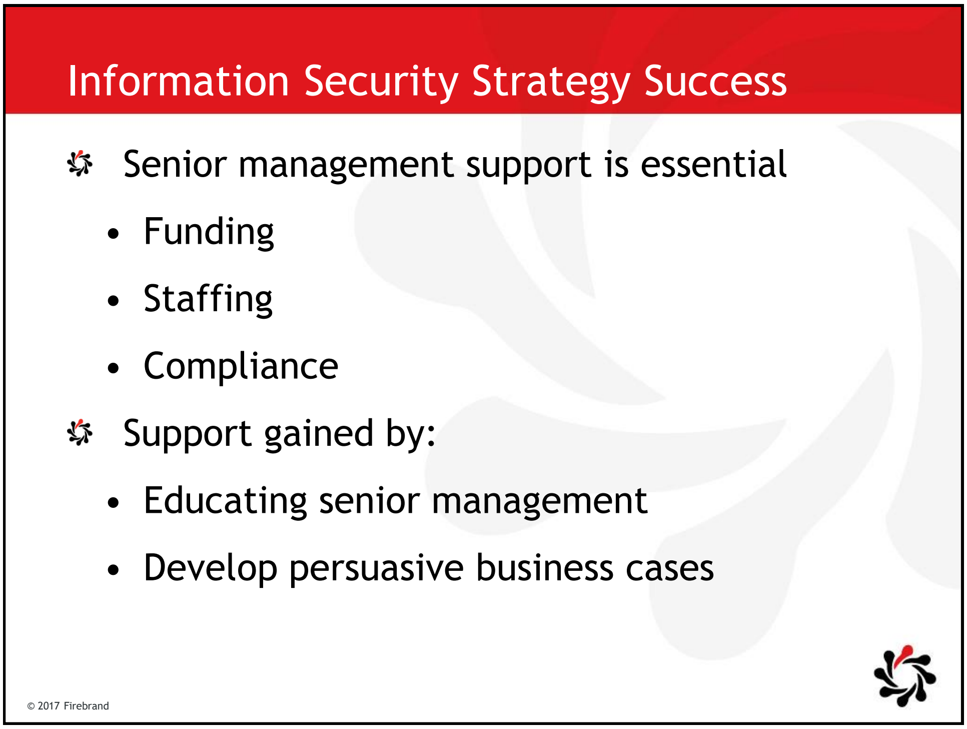
## Business Case

- Used to capture the business reasoning for initiating a project or task
  - Should identify needs and business purpose
  - Should include all factors that could affect project success or failure
  - Total Cost of Ownership (TCO) should address costs across the lifecycle of the project



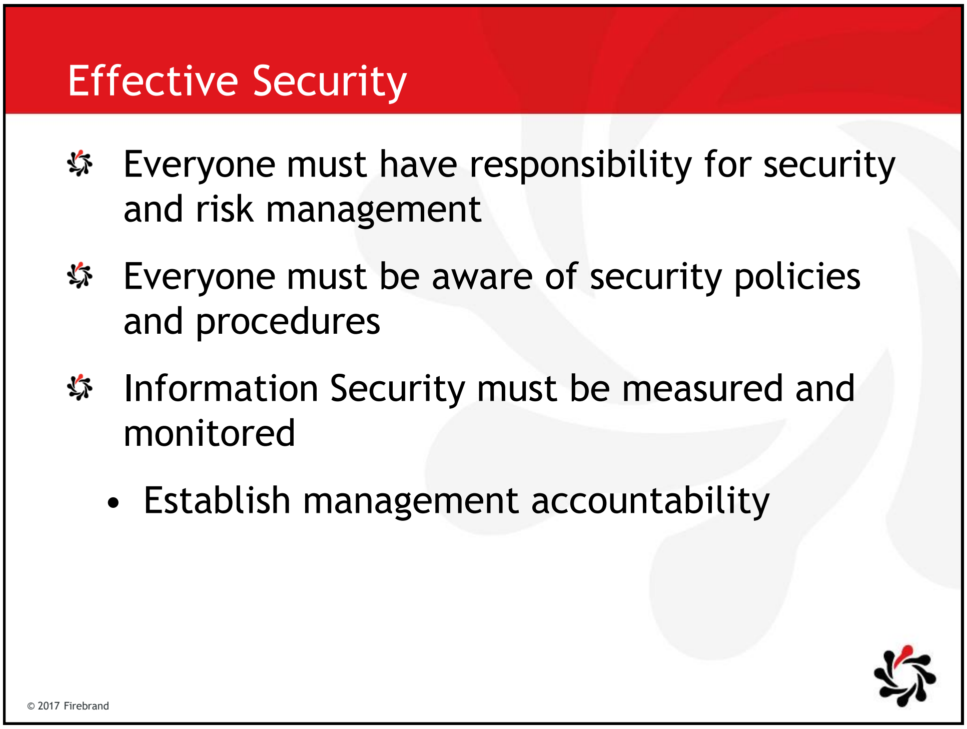
## Living Document

- Strategy is never static as businesses evolve
  - Internal changes
  - External changes
- Objectives, approaches and methods may change to meet new conditions



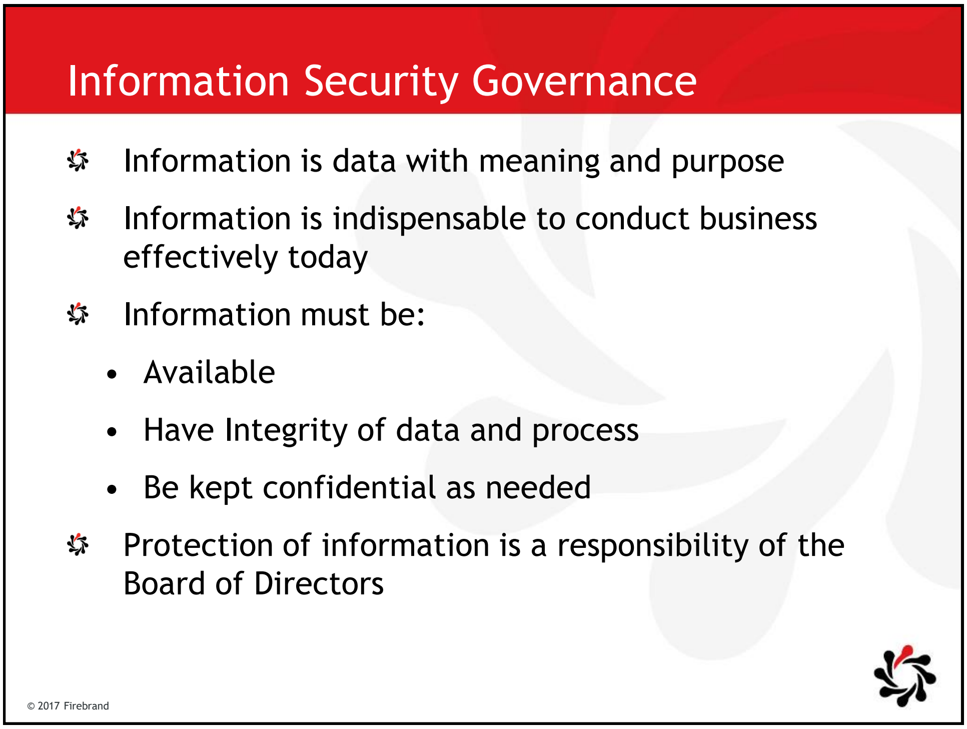
## Information Security Strategy Success

- Senior management support is essential
  - Funding
  - Staffing
  - Compliance
- Support gained by:
  - Educating senior management
  - Develop persuasive business cases



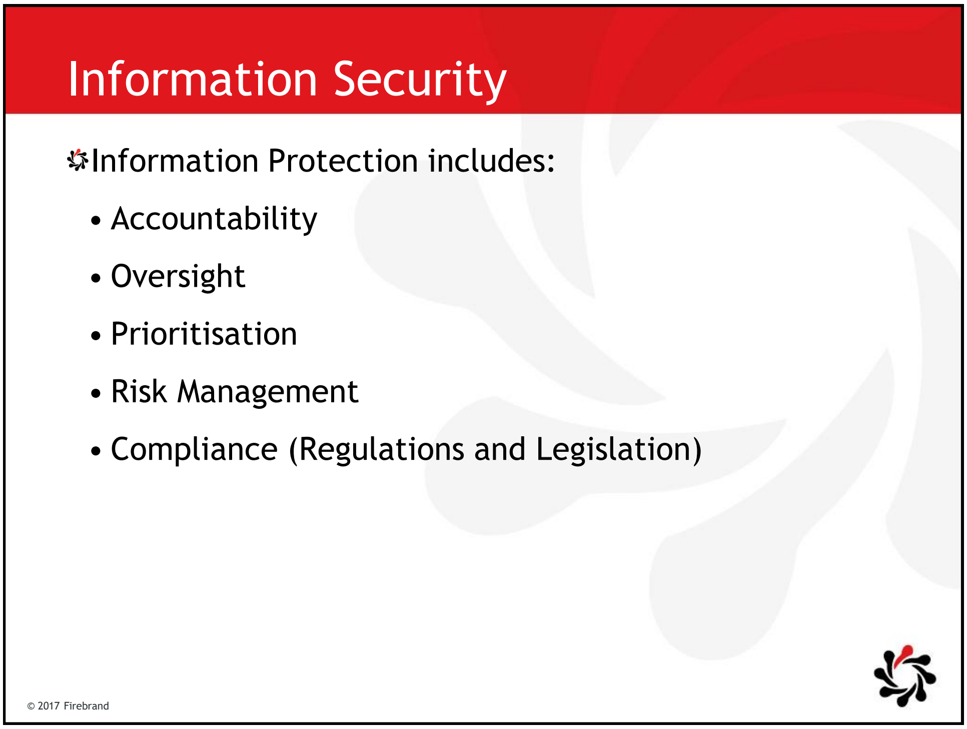
## Effective Security

- Everyone must have responsibility for security and risk management
- Everyone must be aware of security policies and procedures
- Information Security must be measured and monitored
  - Establish management accountability



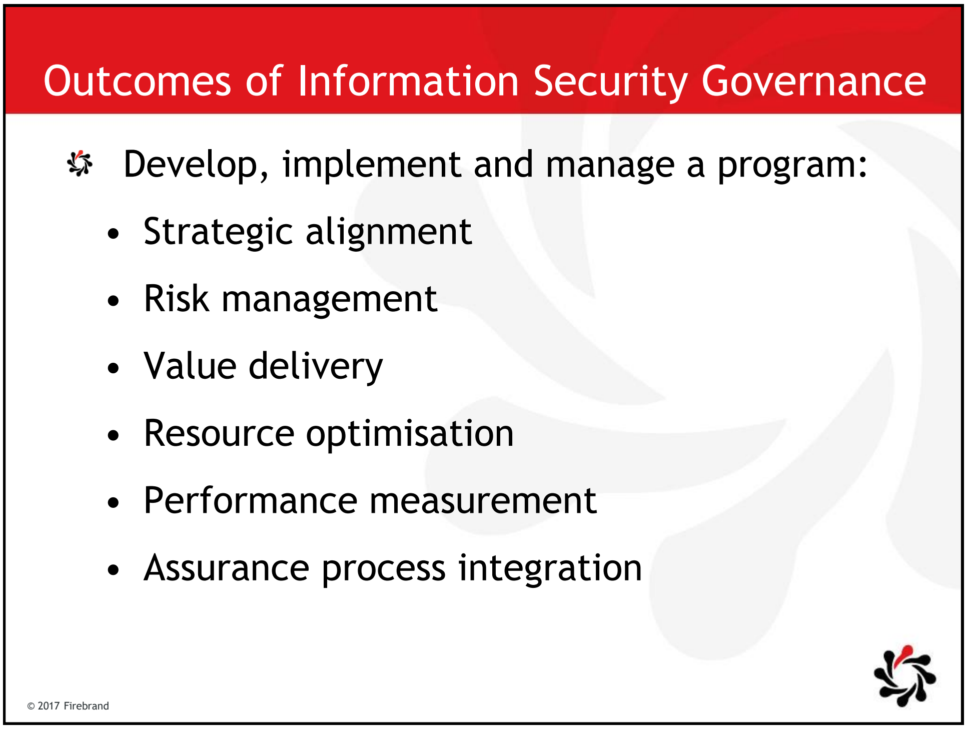
## Information Security Governance

- Information is data with meaning and purpose
- Information is indispensable to conduct business effectively today
- Information must be:
  - Available
  - Have Integrity of data and process
  - Be kept confidential as needed
- Protection of information is a responsibility of the Board of Directors



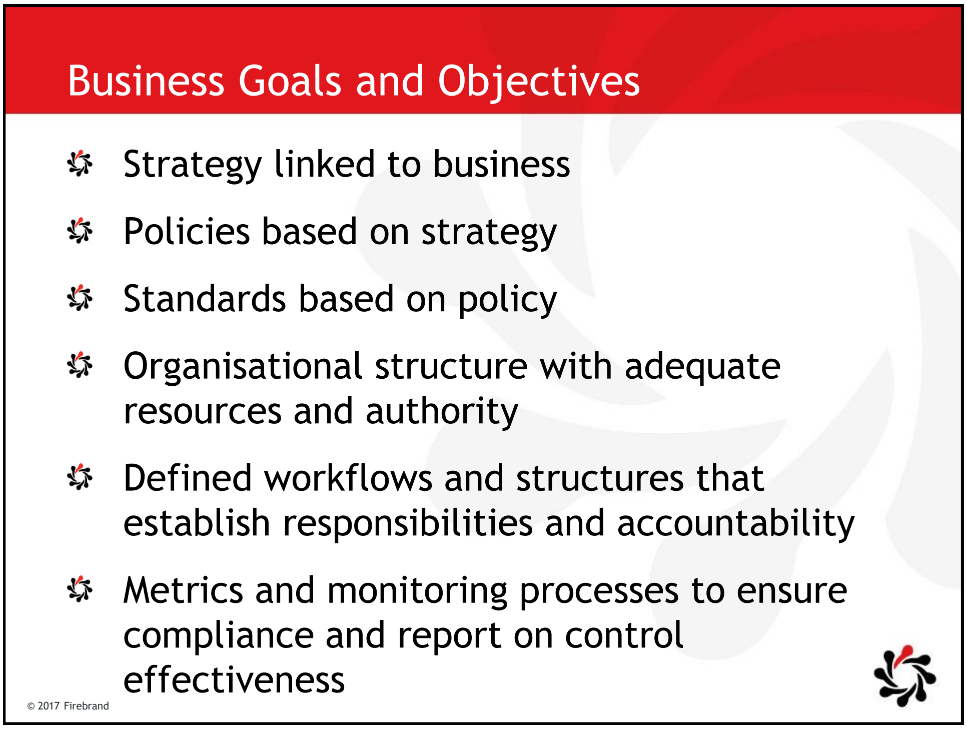
## Information Security

- Information Protection includes:
  - Accountability
  - Oversight
  - Prioritisation
  - Risk Management
  - Compliance (Regulations and Legislation)



## Outcomes of Information Security Governance

- Develop, implement and manage a program:
  - Strategic alignment
  - Risk management
  - Value delivery
  - Resource optimisation
  - Performance measurement
  - Assurance process integration

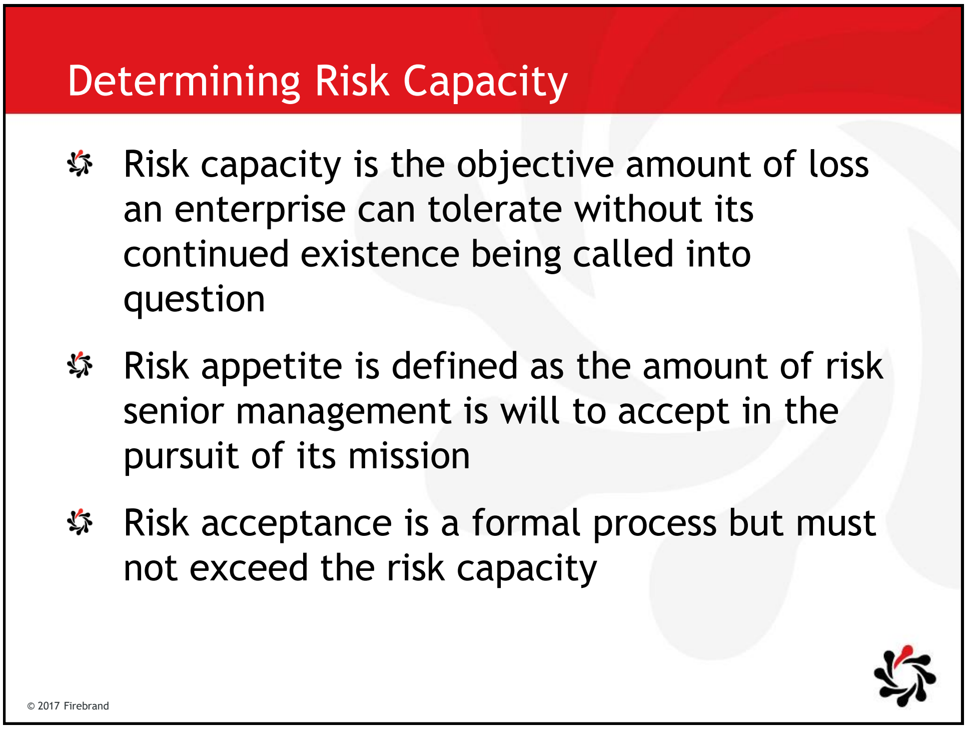


## Business Goals and Objectives

- Strategy linked to business
- Policies based on strategy
- Standards based on policy
- Organisational structure with adequate resources and authority
- Defined workflows and structures that establish responsibilities and accountability
- Metrics and monitoring processes to ensure compliance and report on control effectiveness

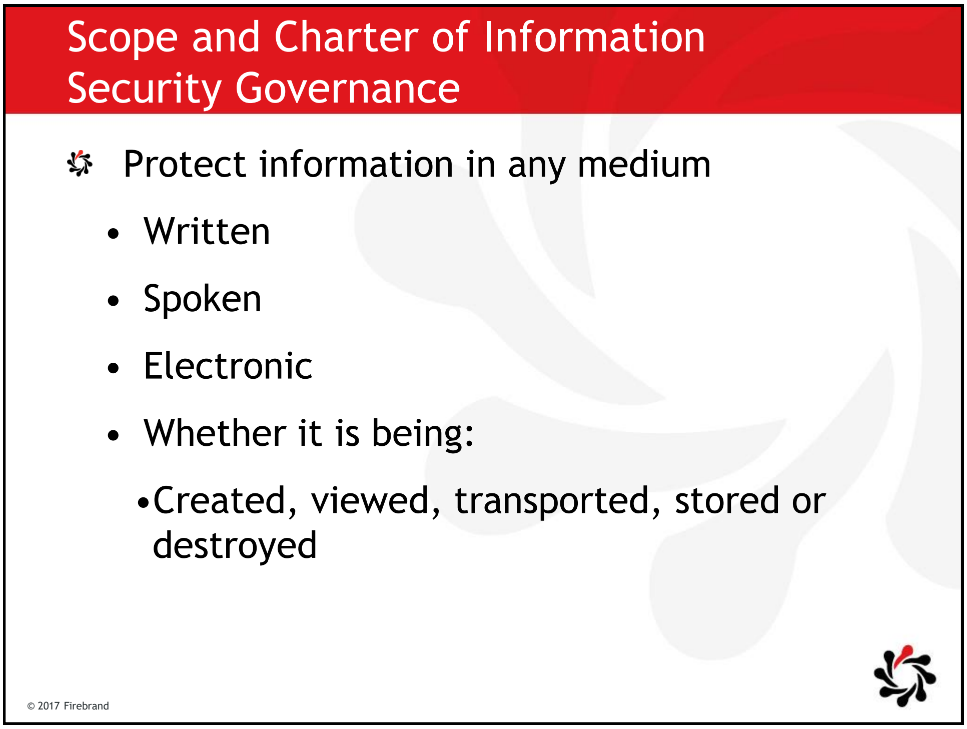
## Security Program Priorities

- Achieve high standards of corporate governance
- Treat information security as a critical business issue
- Create a security positive environment
- Have declared responsibilities



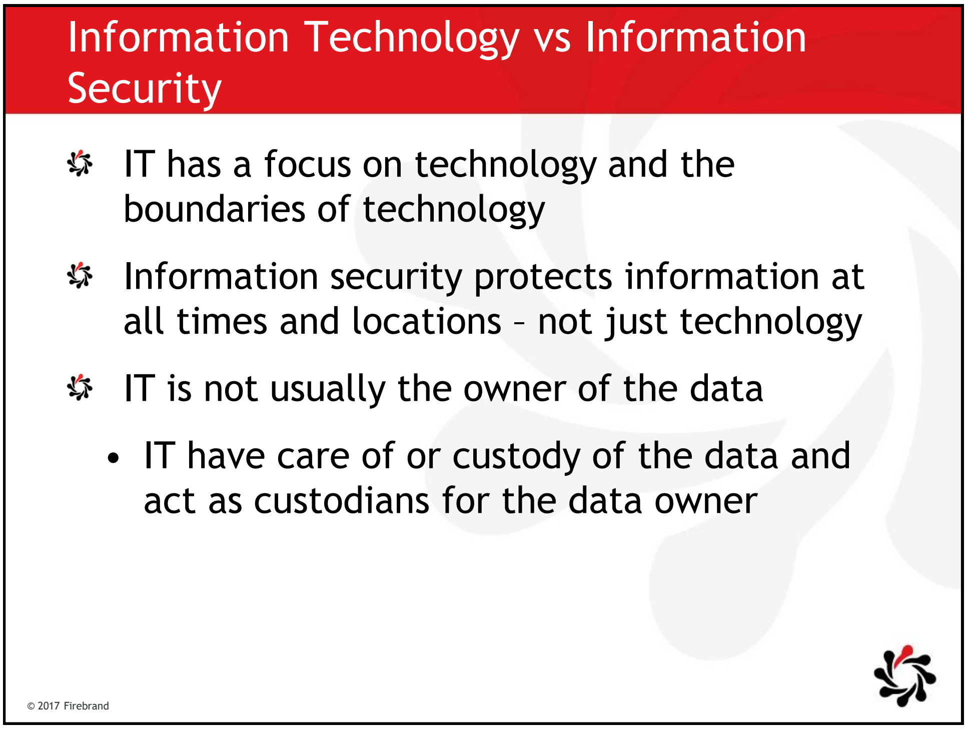
## Determining Risk Capacity

- Risk capacity is the objective amount of loss an enterprise can tolerate without its continued existence being called into question
- Risk appetite is defined as the amount of risk senior management is will to accept in the pursuit of its mission
- Risk acceptance is a formal process but must not exceed the risk capacity



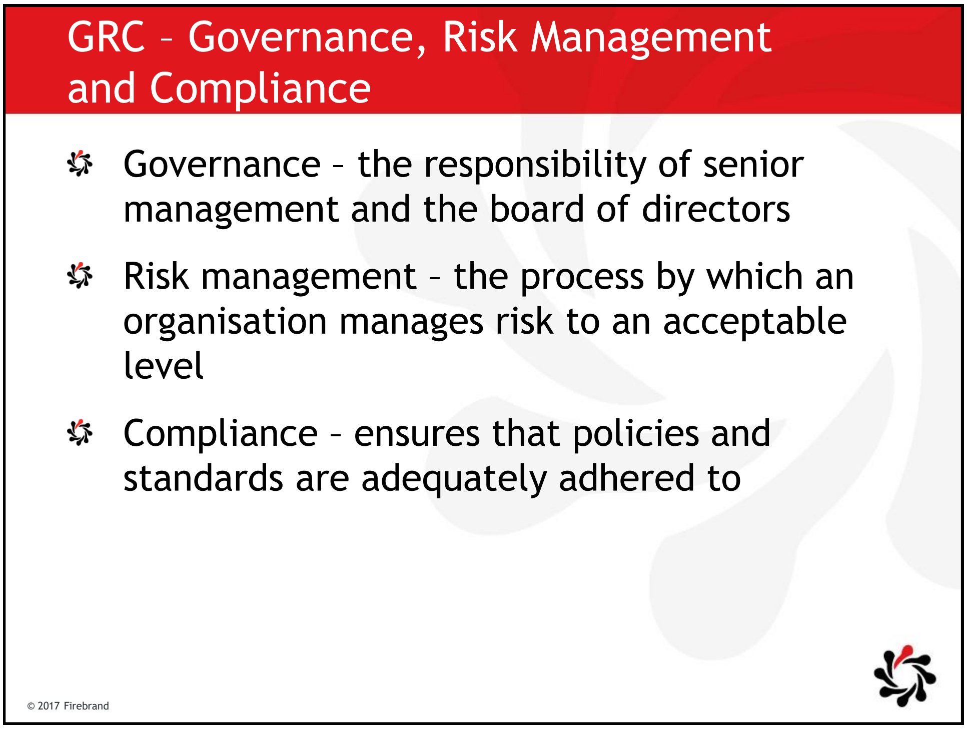
## Scope and Charter of Information Security Governance

- Protect information in any medium
  - Written
  - Spoken
  - Electronic
  - Whether it is being:
    - Created, viewed, transported, stored or destroyed



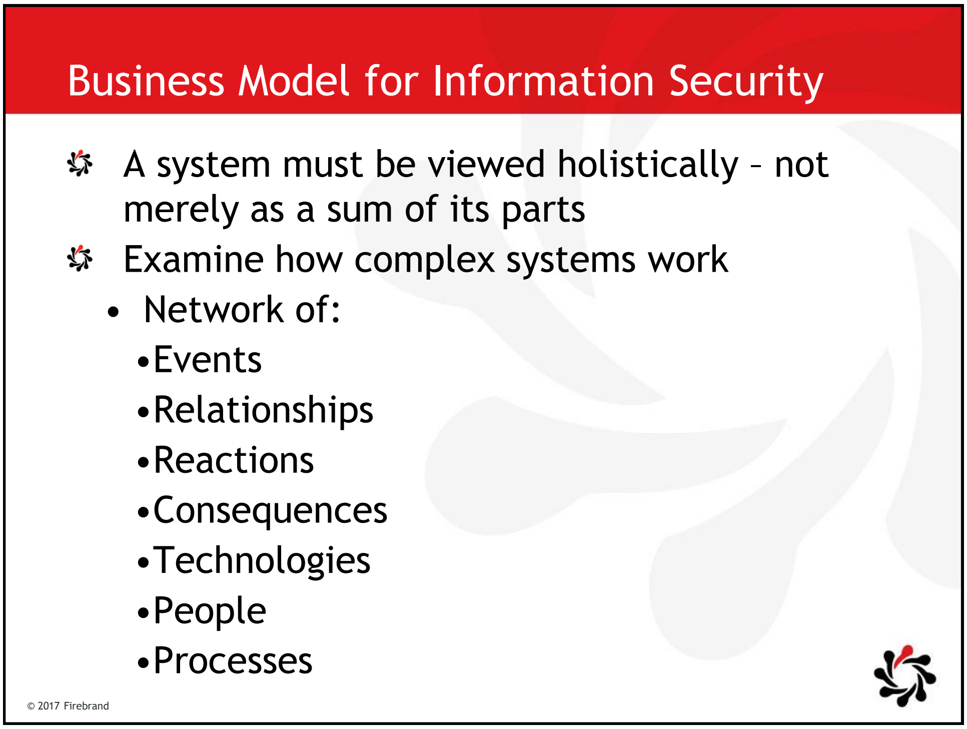
## Information Technology vs Information Security

- IT has a focus on technology and the boundaries of technology
- Information security protects information at all times and locations – not just technology
- IT is not usually the owner of the data
  - IT have care of or custody of the data and act as custodians for the data owner



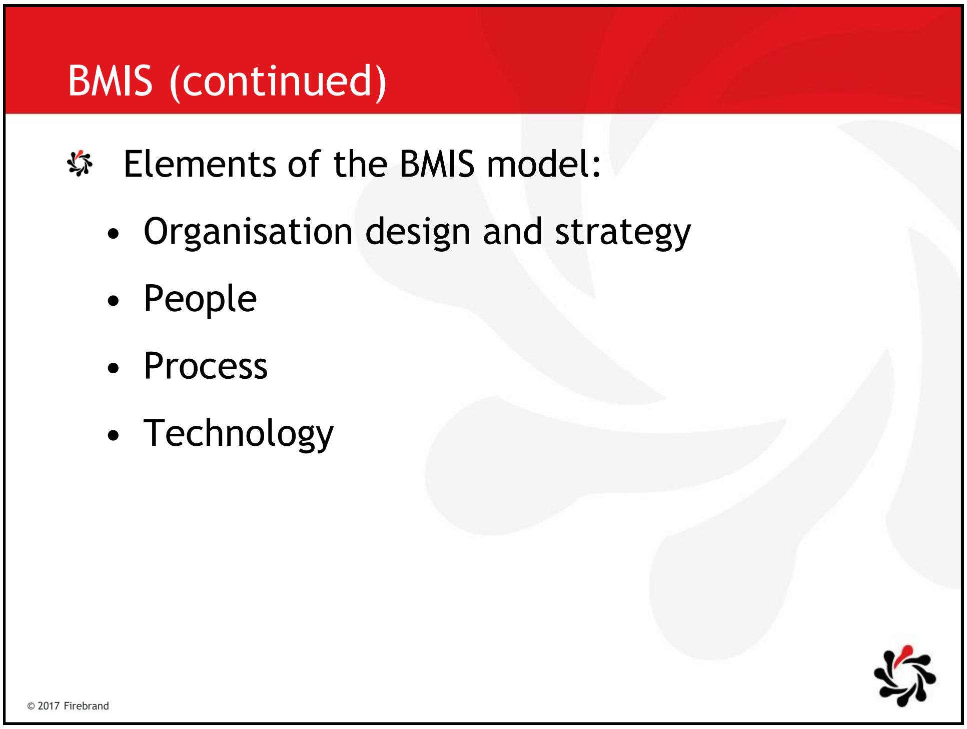
## GRC – Governance, Risk Management and Compliance

- Governance – the responsibility of senior management and the board of directors
- Risk management – the process by which an organisation manages risk to an acceptable level
- Compliance – ensures that policies and standards are adequately adhered to



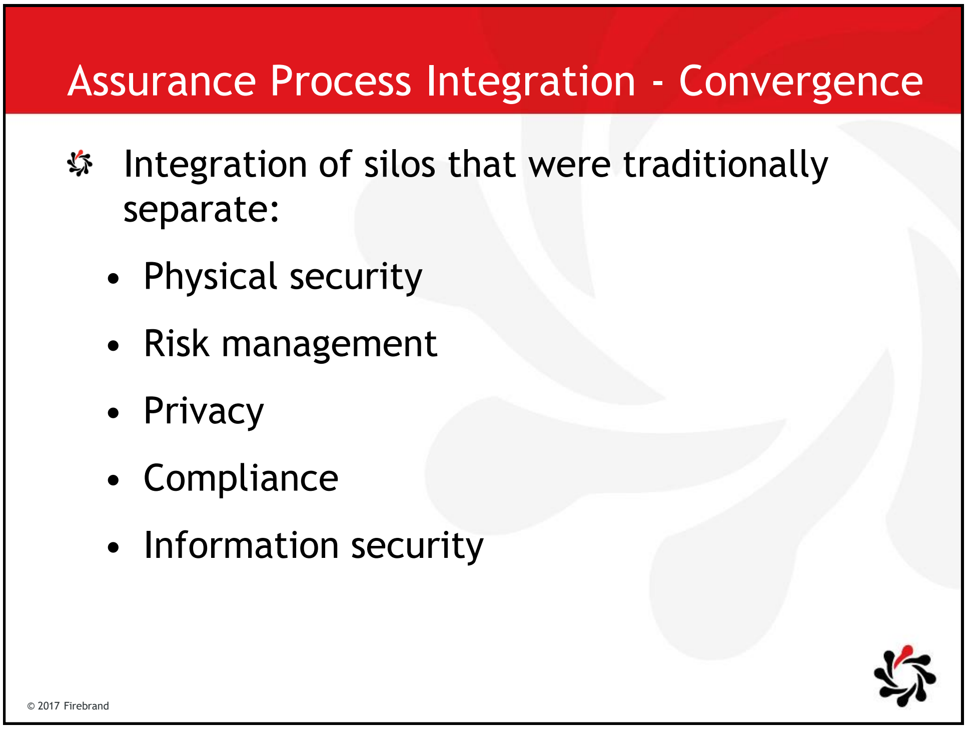
## Business Model for Information Security

- A system must be viewed holistically – not merely as a sum of its parts
- Examine how complex systems work
  - Network of:
    - Events
    - Relationships
    - Reactions
    - Consequences
    - Technologies
    - People
    - Processes



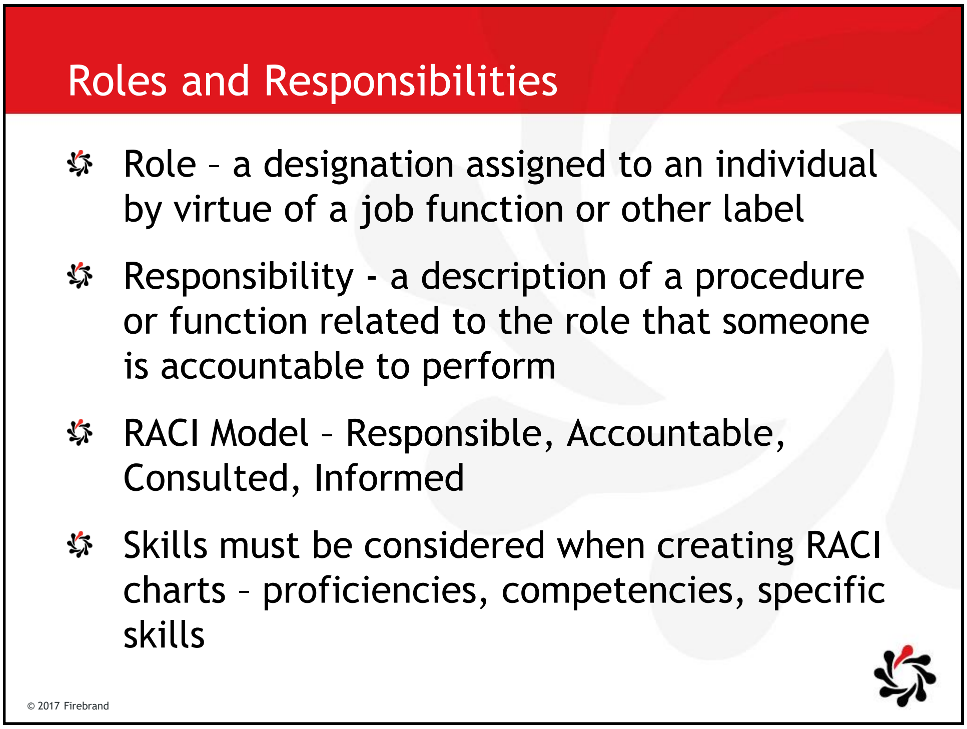
## BMIS (continued)

- Elements of the BMIS model:
  - Organisation design and strategy
  - People
  - Process
  - Technology



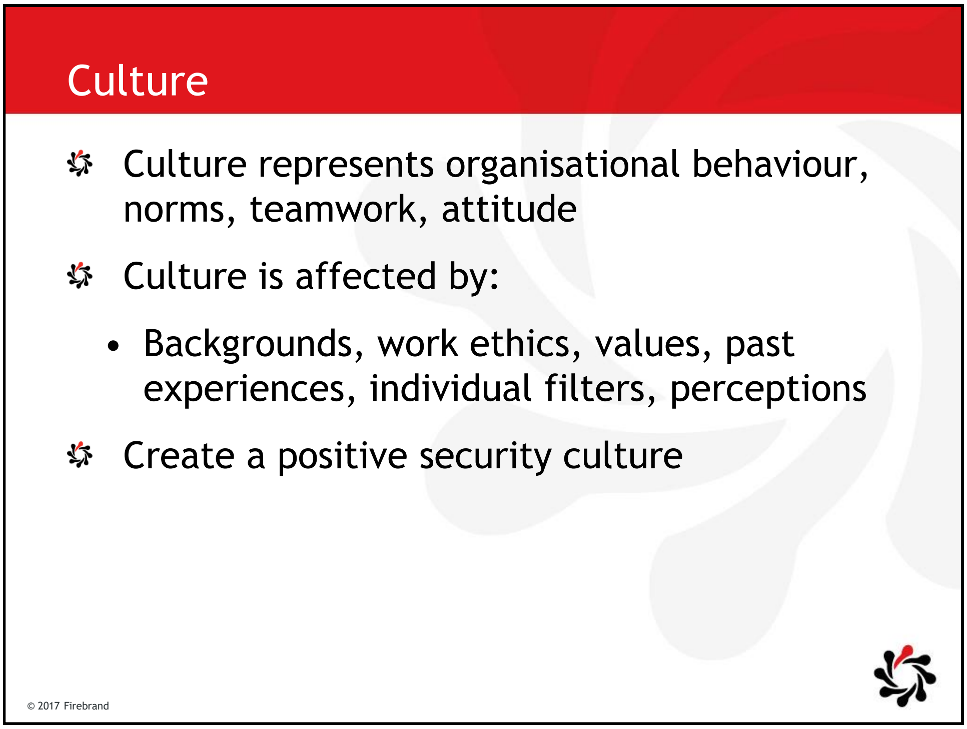
## Assurance Process Integration - Convergence

- Integration of silos that were traditionally separate:
  - Physical security
  - Risk management
  - Privacy
  - Compliance
  - Information security



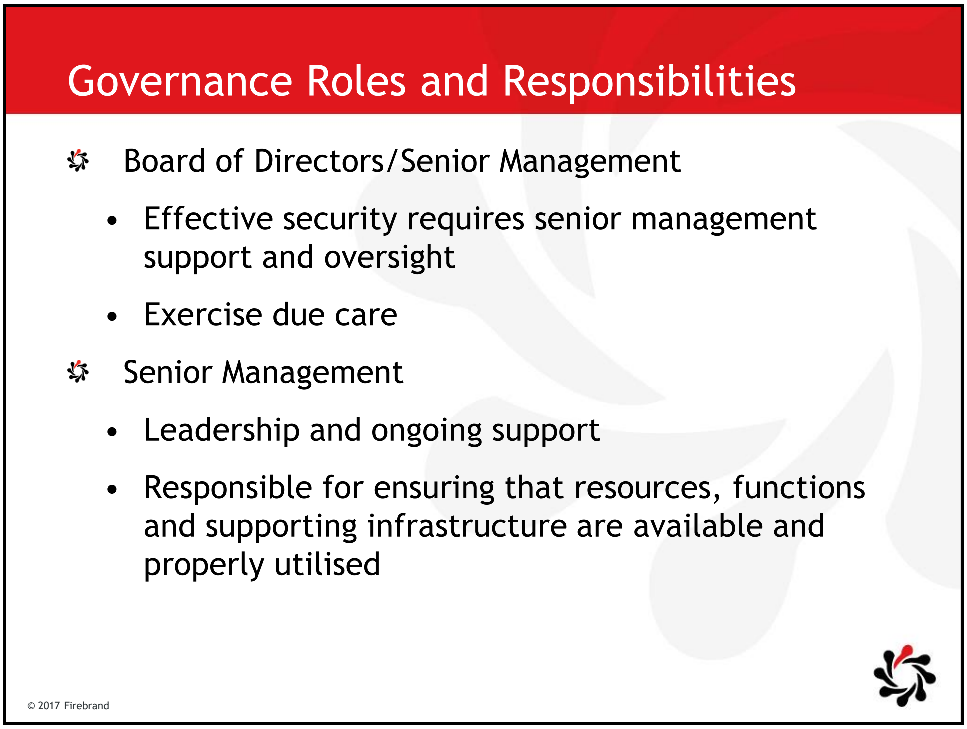
## Roles and Responsibilities

- Role – a designation assigned to an individual by virtue of a job function or other label
- Responsibility - a description of a procedure or function related to the role that someone is accountable to perform
- RACI Model – Responsible, Accountable, Consulted, Informed
- Skills must be considered when creating RACI charts – proficiencies, competencies, specific skills



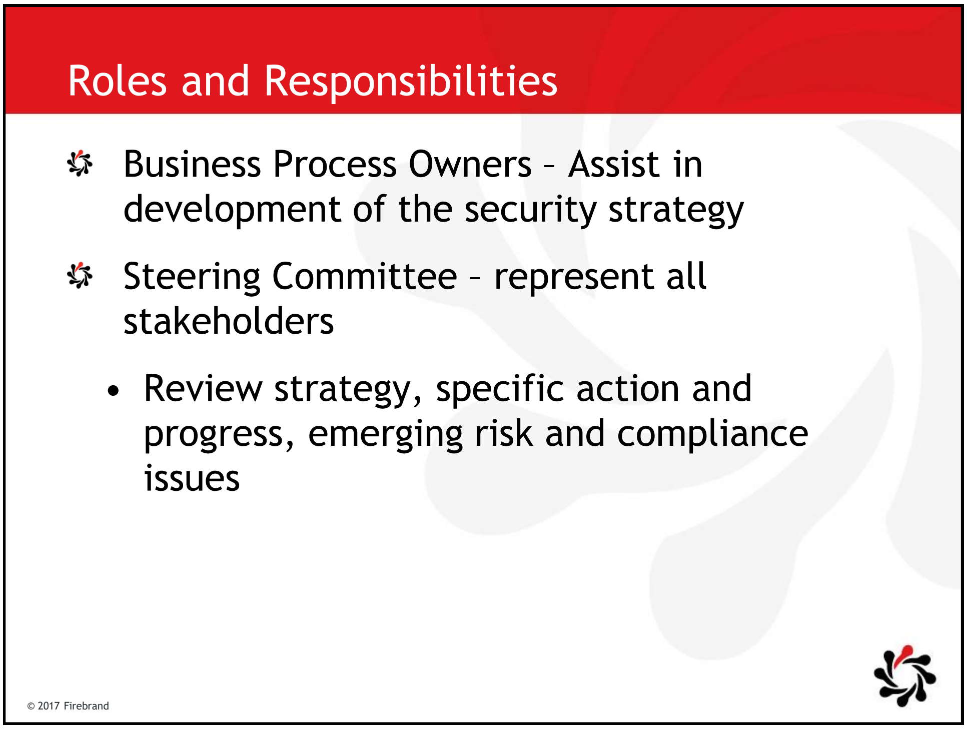
## Culture

- Culture represents organisational behaviour, norms, teamwork, attitude
- Culture is affected by:
  - Backgrounds, work ethics, values, past experiences, individual filters, perceptions
- Create a positive security culture



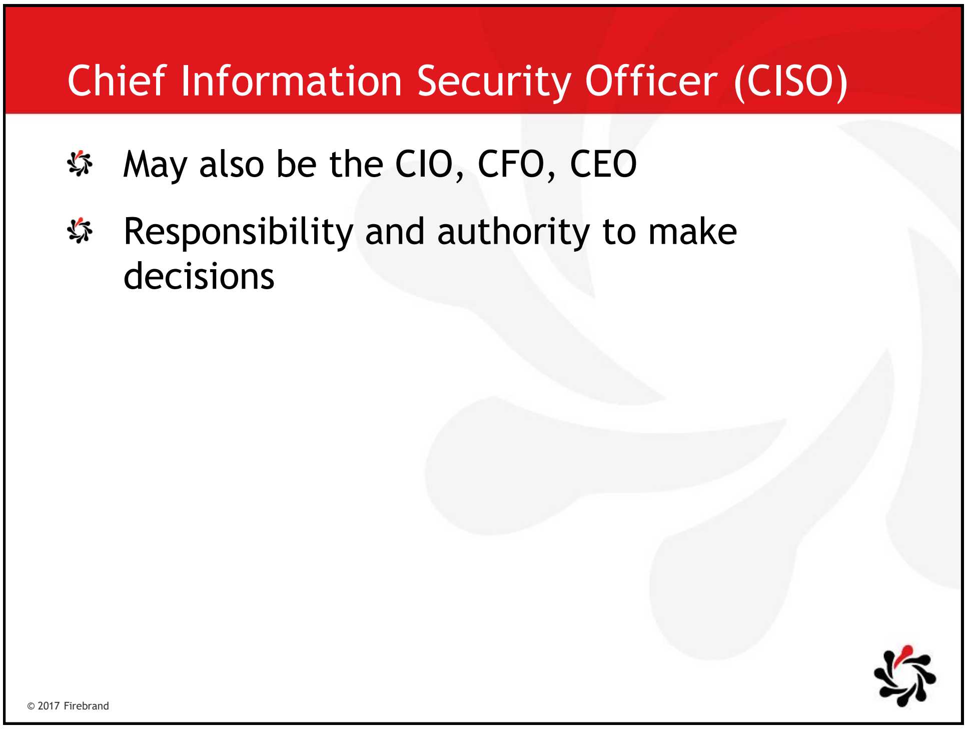
## Governance Roles and Responsibilities

- Board of Directors/Senior Management
  - Effective security requires senior management support and oversight
  - Exercise due care
- Senior Management
  - Leadership and ongoing support
  - Responsible for ensuring that resources, functions and supporting infrastructure are available and properly utilised



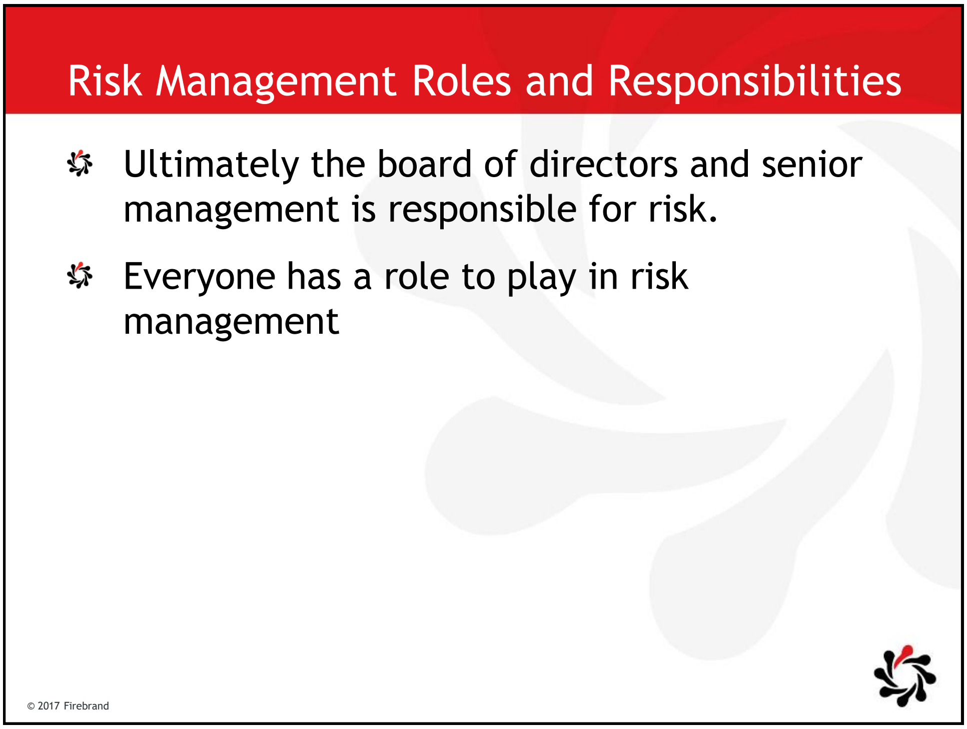
## Roles and Responsibilities

- Business Process Owners – Assist in development of the security strategy
- Steering Committee – represent all stakeholders
  - Review strategy, specific action and progress, emerging risk and compliance issues



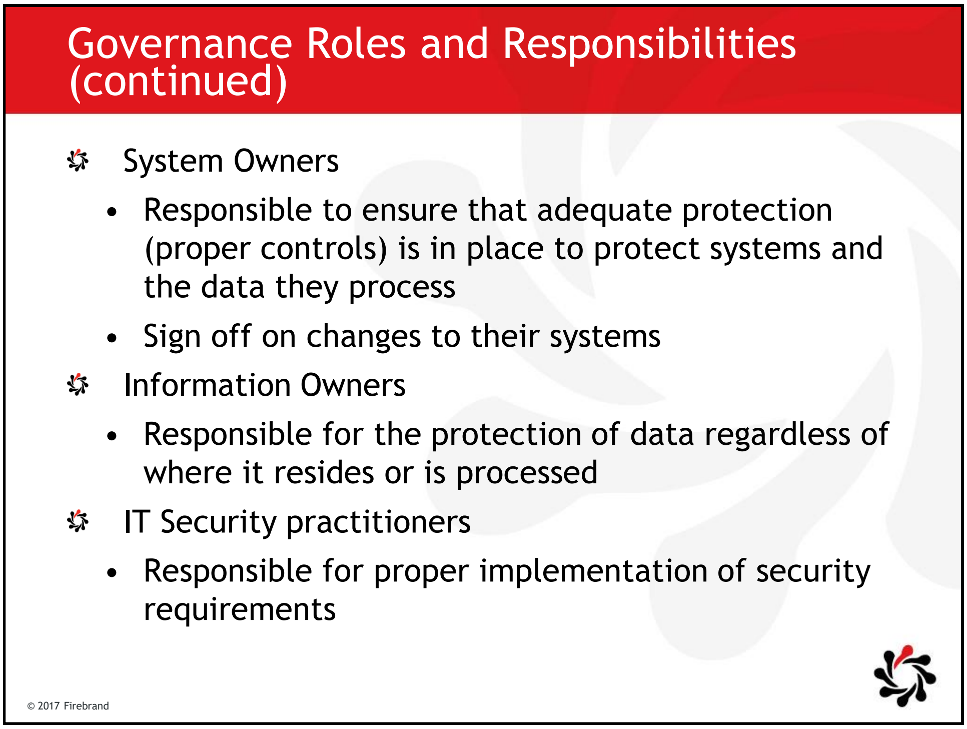
## Chief Information Security Officer (CISO)

- May also be the CIO, CFO, CEO
- Responsibility and authority to make decisions



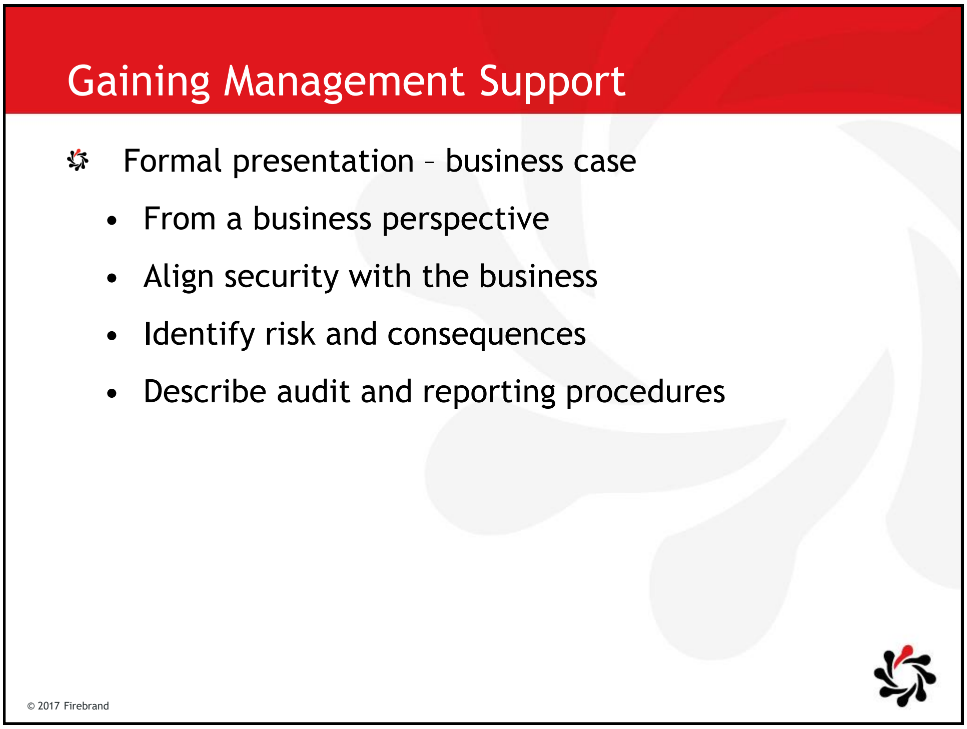
## Risk Management Roles and Responsibilities

- Ultimately the board of directors and senior management is responsible for risk.
- Everyone has a role to play in risk management



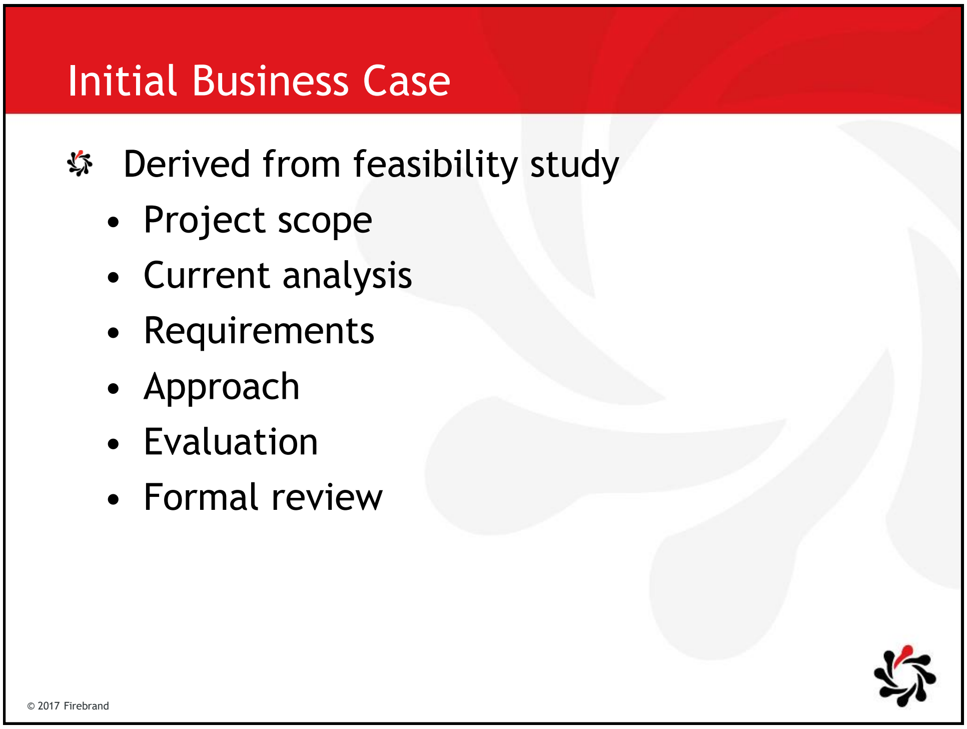
## Governance Roles and Responsibilities (continued)

- System Owners
  - Responsible to ensure that adequate protection (proper controls) is in place to protect systems and the data they process
  - Sign off on changes to their systems
- Information Owners
  - Responsible for the protection of data regardless of where it resides or is processed
- IT Security practitioners
  - Responsible for proper implementation of security requirements



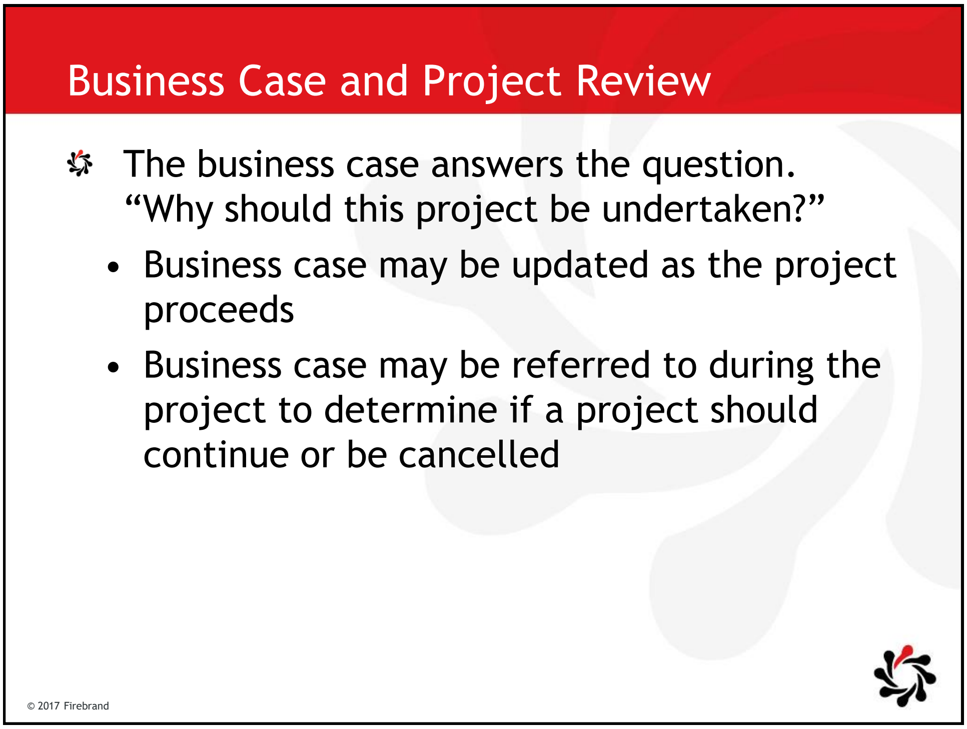
## Gaining Management Support

- Formal presentation – business case
  - From a business perspective
  - Align security with the business
  - Identify risk and consequences
  - Describe audit and reporting procedures



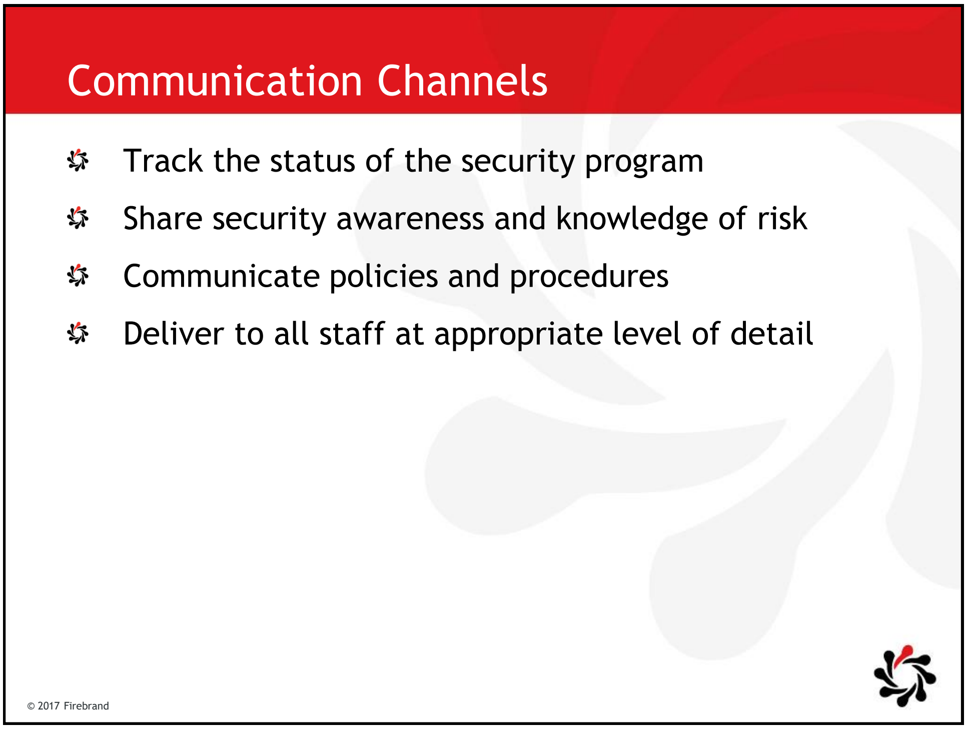
## Initial Business Case

- Derived from feasibility study
  - Project scope
  - Current analysis
  - Requirements
  - Approach
  - Evaluation
  - Formal review



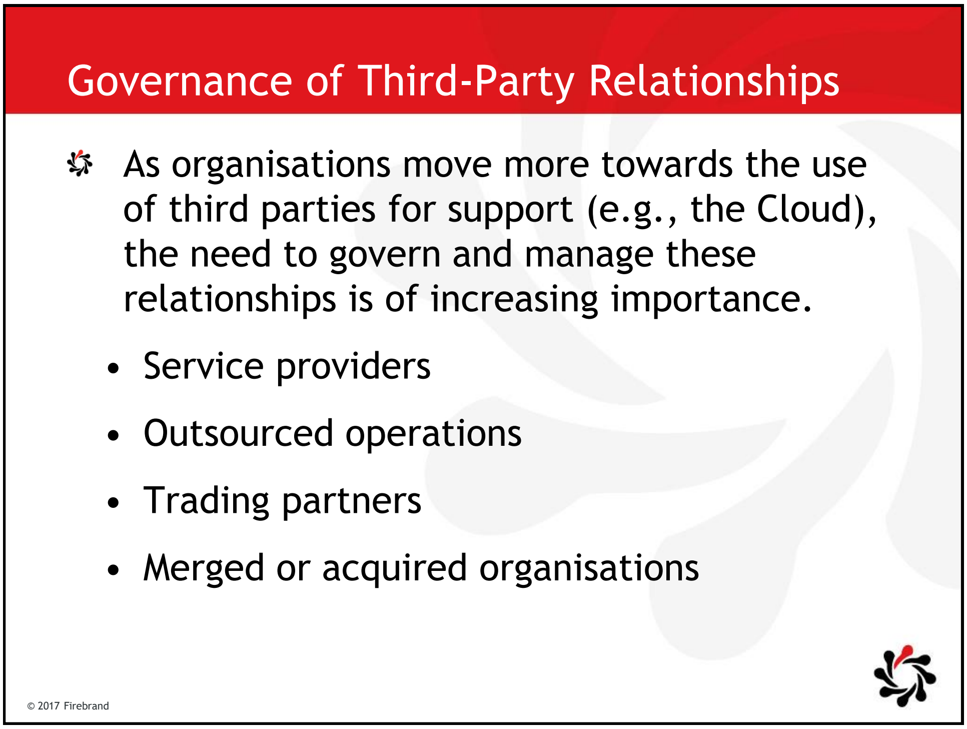
## Business Case and Project Review

- The business case answers the question. "Why should this project be undertaken?"
  - Business case may be updated as the project proceeds
  - Business case may be referred to during the project to determine if a project should continue or be cancelled



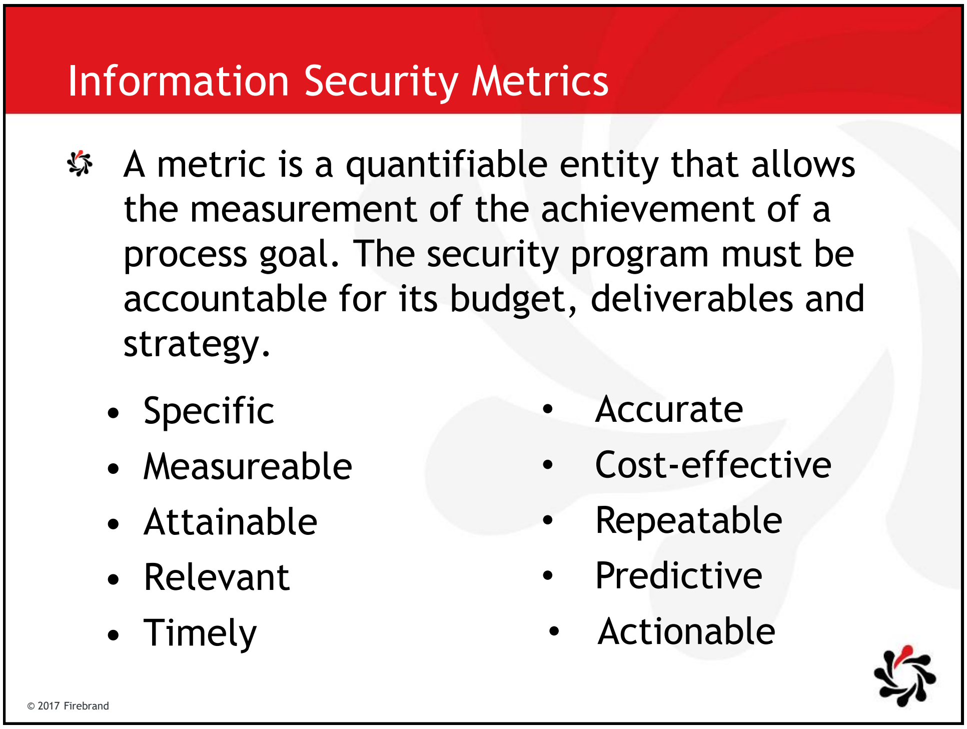
## Communication Channels

- Track the status of the security program
- Share security awareness and knowledge of risk
- Communicate policies and procedures
- Deliver to all staff at appropriate level of detail



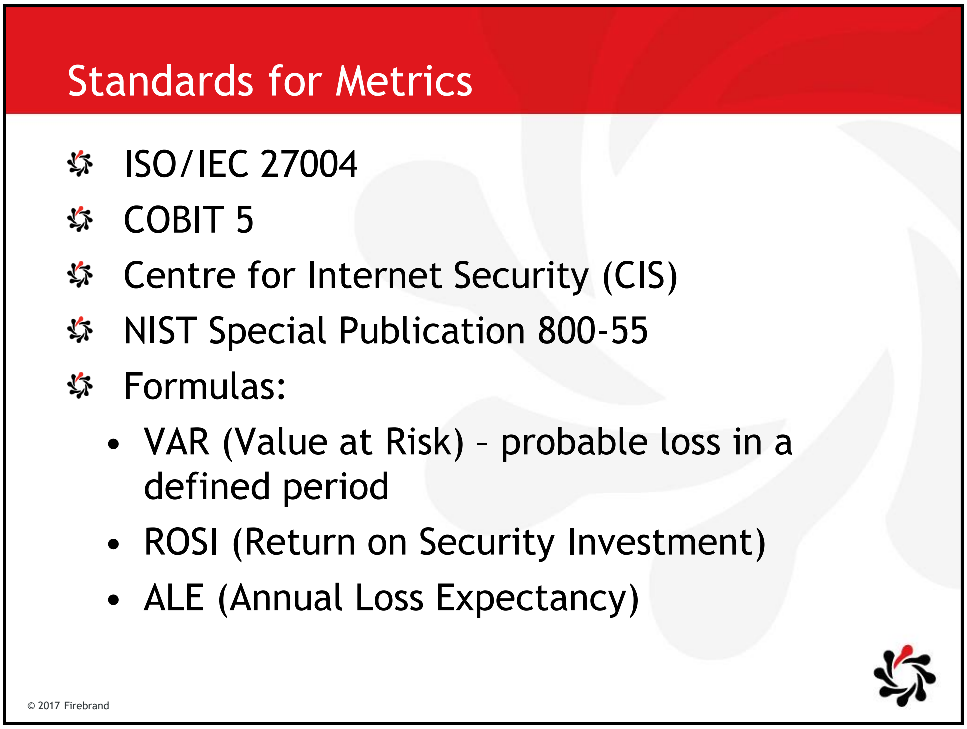
## Governance of Third-Party Relationships

- As organisations move more towards the use of third parties for support (e.g., the Cloud), the need to govern and manage these relationships is of increasing importance.
  - Service providers
  - Outsourced operations
  - Trading partners
  - Merged or acquired organisations



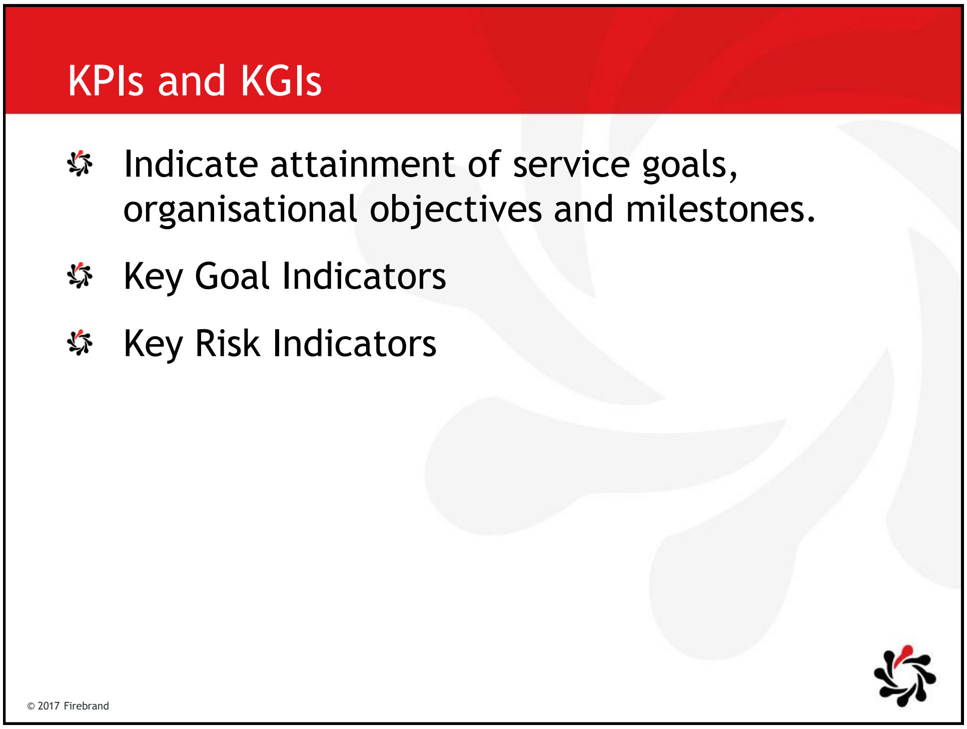
## Information Security Metrics

- A metric is a quantifiable entity that allows the measurement of the achievement of a process goal. The security program must be accountable for its budget, deliverables and strategy.
  - Specific
  - Measureable
  - Attainable
  - Relevant
  - Timely
  - Accurate
  - Cost-effective
  - Repeatable
  - Predictive
  - Actionable



## Standards for Metrics

- ISO/IEC 27004
- COBIT 5
- Centre for Internet Security (CIS)
- NIST Special Publication 800-55
- Formulas:
  - VAR (Value at Risk) – probable loss in a defined period
  - ROSI (Return on Security Investment)
  - ALE (Annual Loss Expectancy)

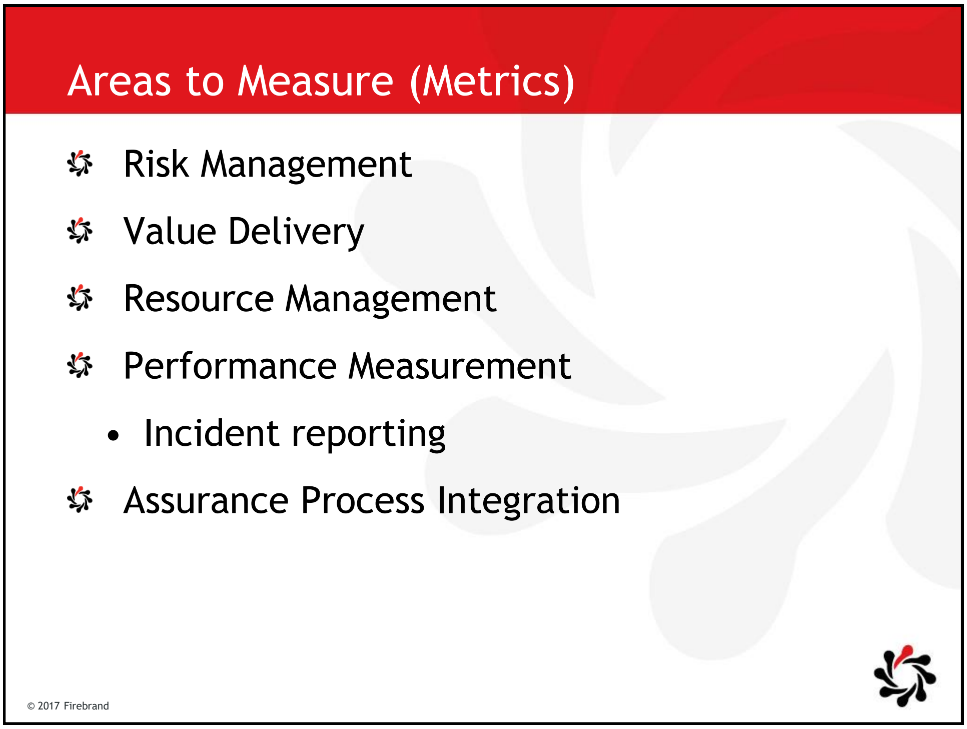


## KPIs and KGIs

- Indicate attainment of service goals, organisational objectives and milestones.
- Key Goal Indicators
- Key Risk Indicators

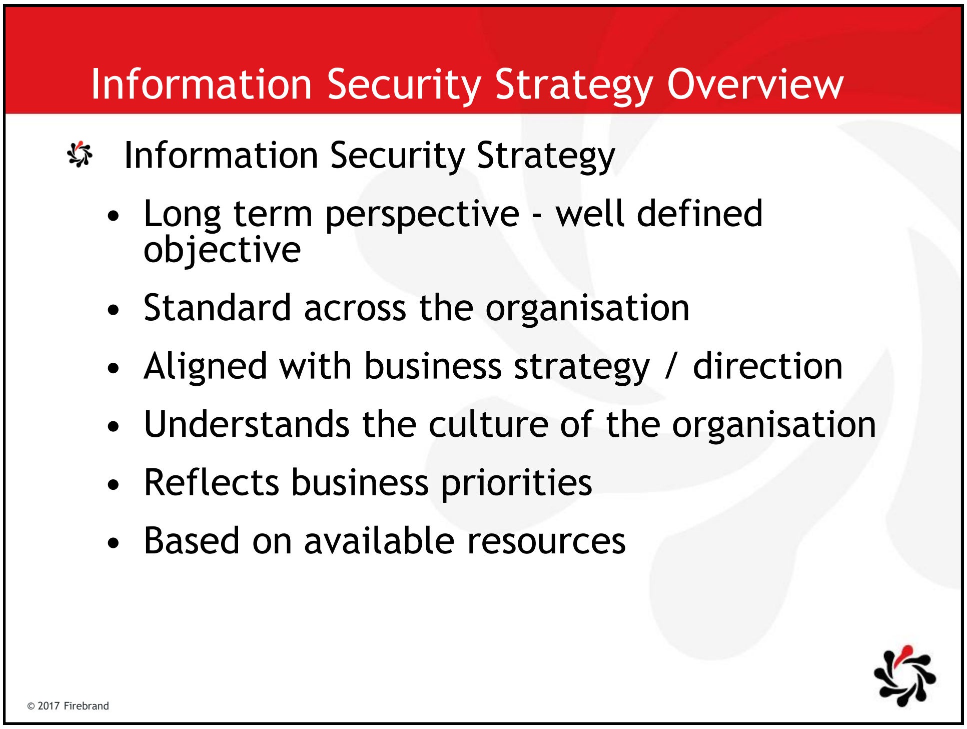
## Security Integration

- Security needs to be integrated INTO the business processes
- The goal is to reduce security gaps through organisational-wide security programs
- Indicators of alignment:
  - Security enables business activities
  - Delay to business when risk cannot be managed
  - Defined security objectives and activities mapped to organisational objectives
  - Security steering committee



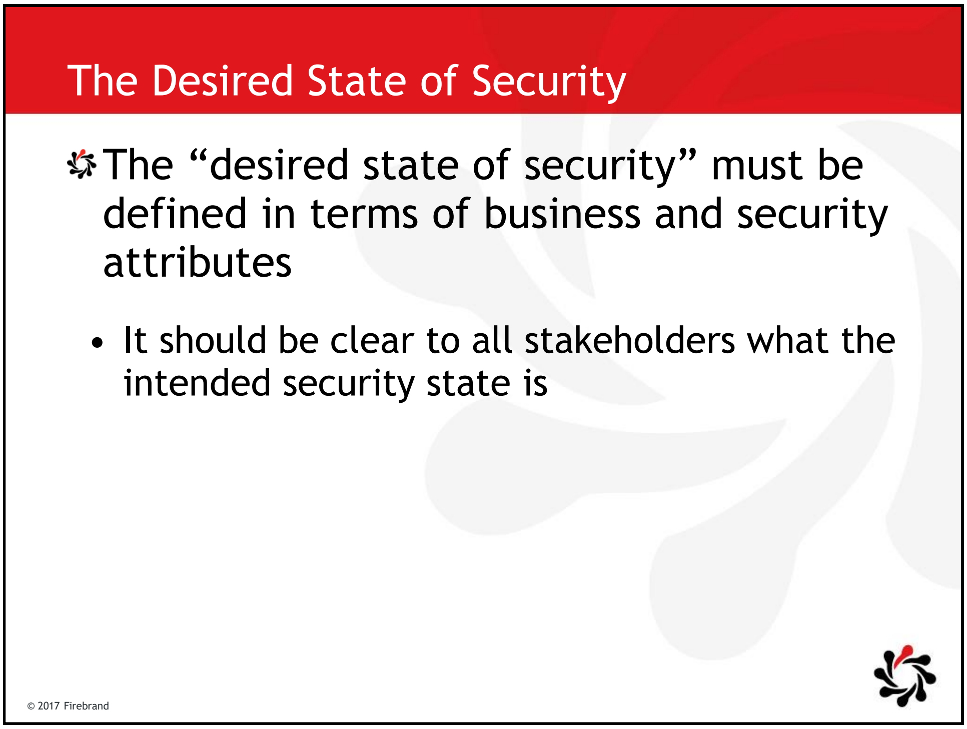
## Areas to Measure (Metrics)

- Risk Management
- Value Delivery
- Resource Management
- Performance Measurement
  - Incident reporting
- Assurance Process Integration



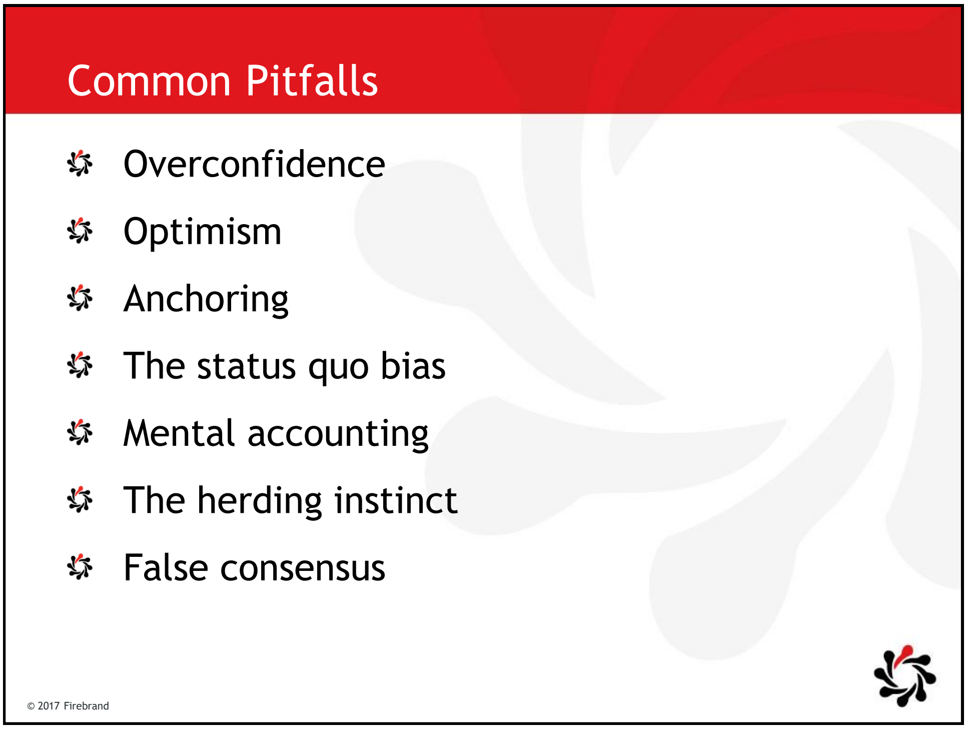
## Information Security Strategy Overview

- Information Security Strategy
  - Long term perspective - well defined objective
  - Standard across the organisation
  - Aligned with business strategy / direction
  - Understands the culture of the organisation
  - Reflects business priorities
  - Based on available resources



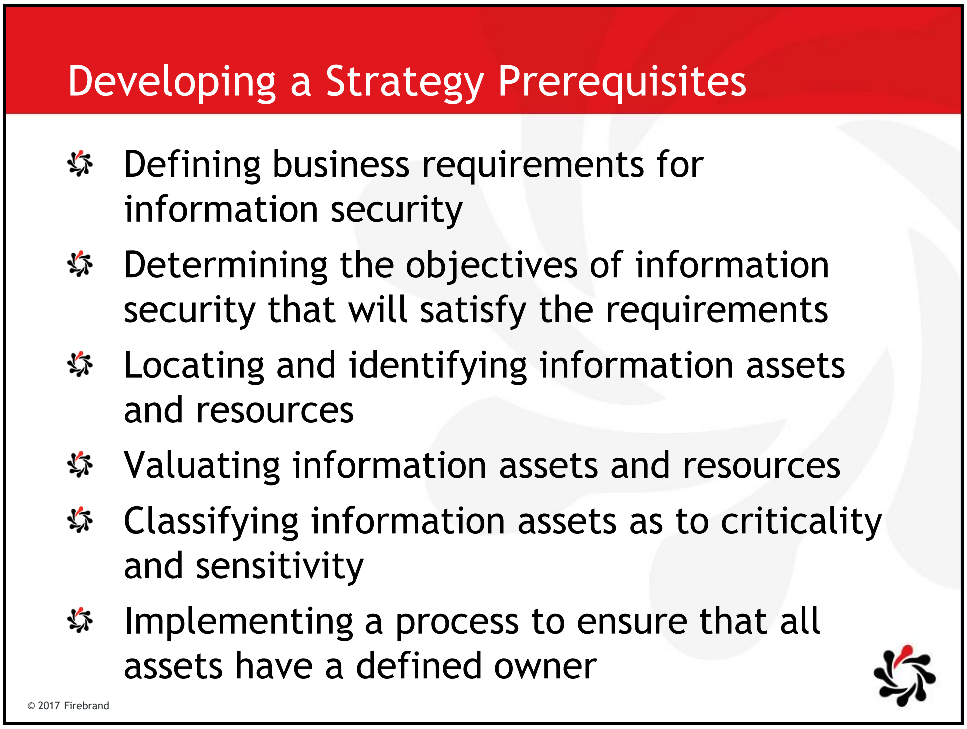
## The Desired State of Security

- The “desired state of security” must be defined in terms of business and security attributes
  - It should be clear to all stakeholders what the intended security state is



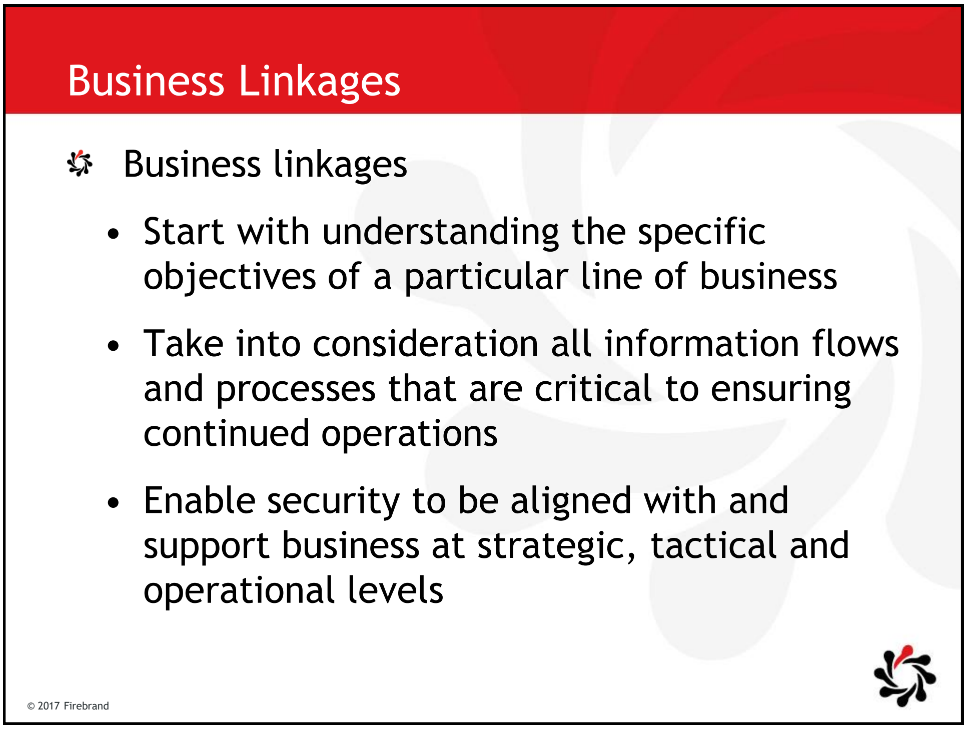
## Common Pitfalls

- Overconfidence
- Optimism
- Anchoring
- The status quo bias
- Mental accounting
- The herding instinct
- False consensus



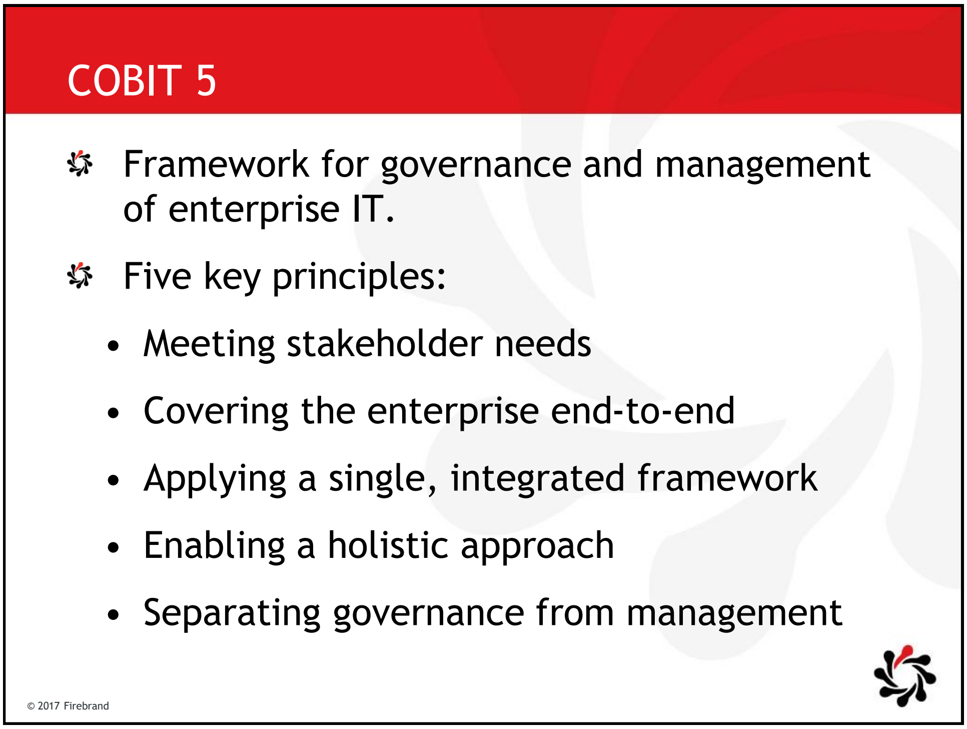
## Developing a Strategy Prerequisites

- Defining business requirements for information security
- Determining the objectives of information security that will satisfy the requirements
- Locating and identifying information assets and resources
- Valuating information assets and resources
- Classifying information assets as to criticality and sensitivity
- Implementing a process to ensure that all assets have a defined owner



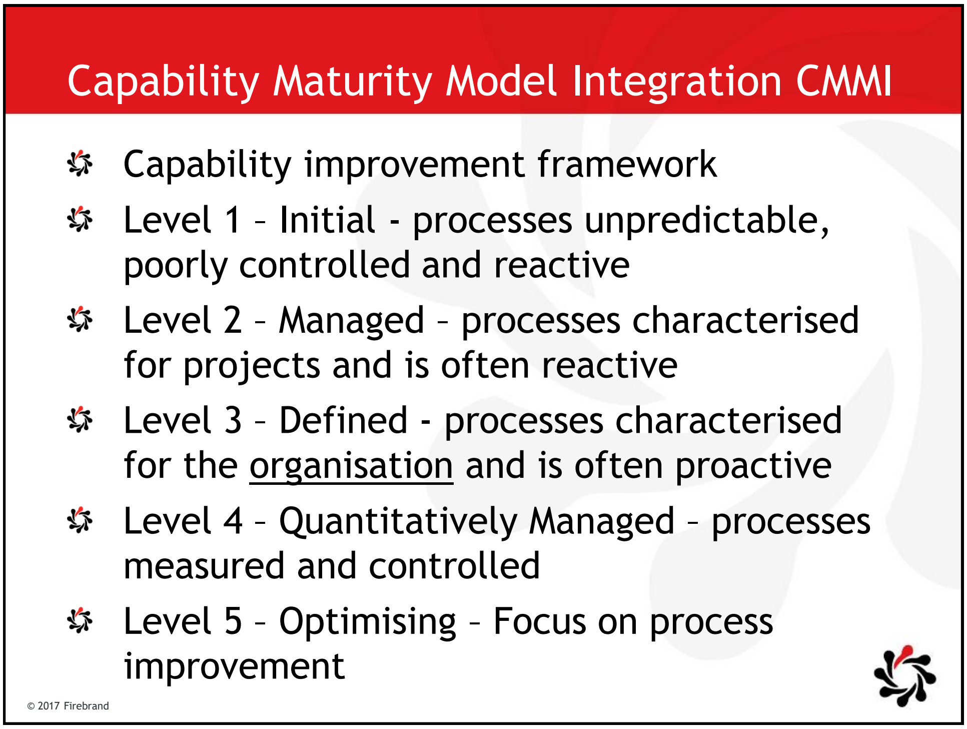
## Business Linkages

- Business linkages
  - Start with understanding the specific objectives of a particular line of business
  - Take into consideration all information flows and processes that are critical to ensuring continued operations
  - Enable security to be aligned with and support business at strategic, tactical and operational levels



## COBIT 5

- Framework for governance and management of enterprise IT.
- Five key principles:
  - Meeting stakeholder needs
  - Covering the enterprise end-to-end
  - Applying a single, integrated framework
  - Enabling a holistic approach
  - Separating governance from management



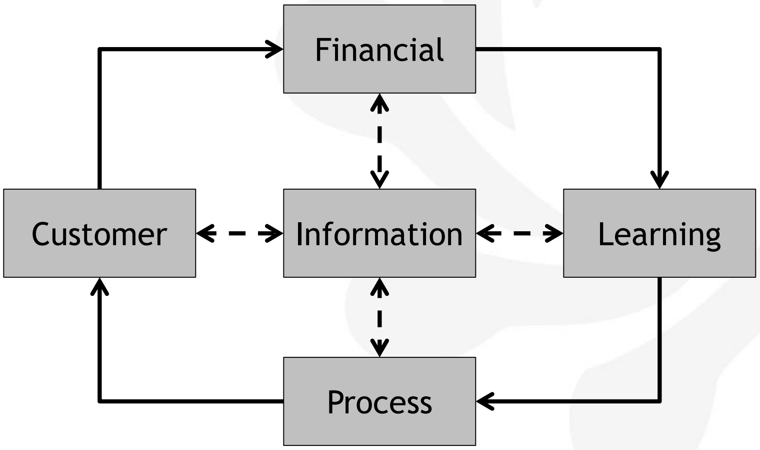
## Capability Maturity Model Integration CMMI

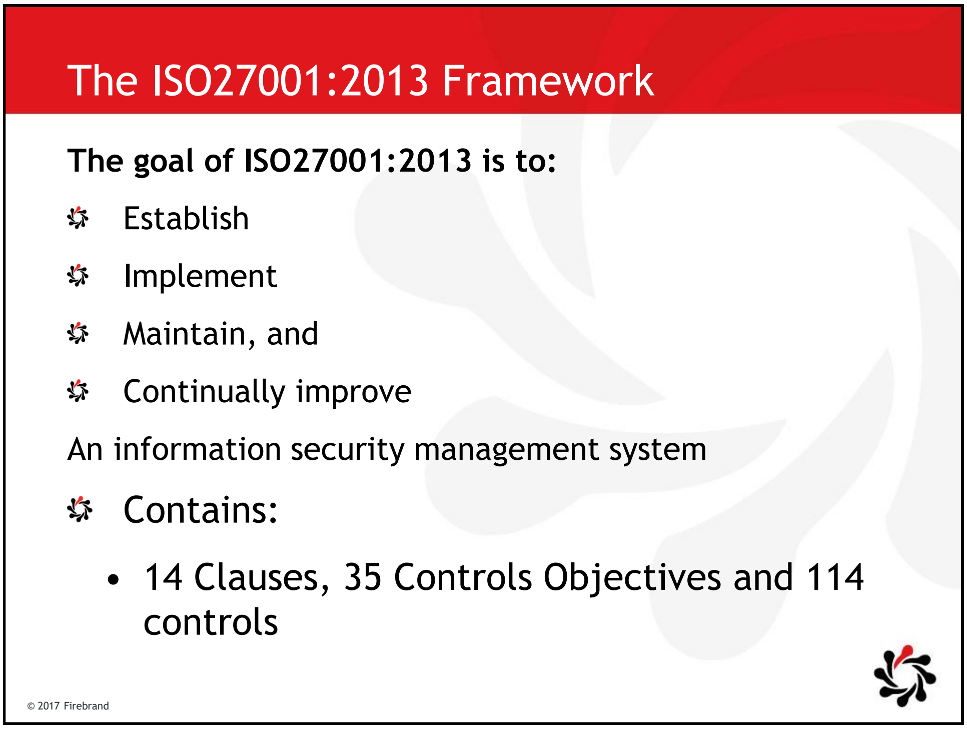
- Capability improvement framework
- Level 1 – Initial - processes unpredictable, poorly controlled and reactive
- Level 2 – Managed – processes characterised for projects and is often reactive
- Level 3 – Defined - processes characterised for the organisation and is often proactive
- Level 4 – Quantitatively Managed – processes measured and controlled
- Level 5 – Optimising – Focus on process improvement

## Balanced Scorecard (BSC)

- See next slide for diagram
- Enables organisations to clarify their vision and strategy and translate them into action

## Balanced Scorecard (BSC)





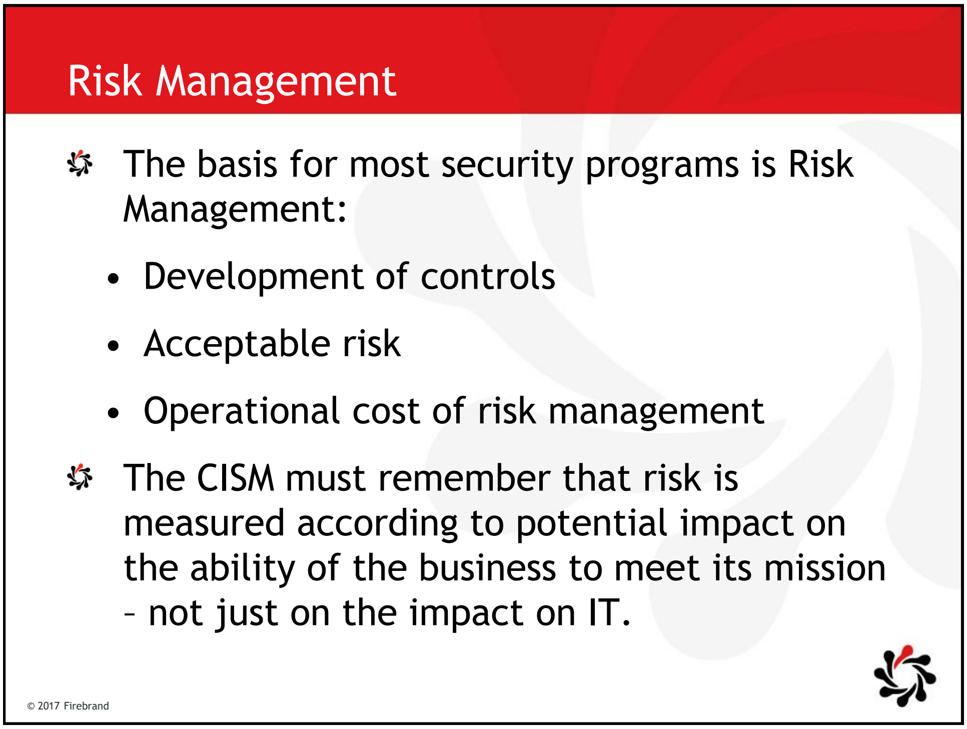
## The ISO27001:2013 Framework

**The goal of ISO27001:2013 is to:**

- Establish
- Implement
- Maintain, and
- Continually improve

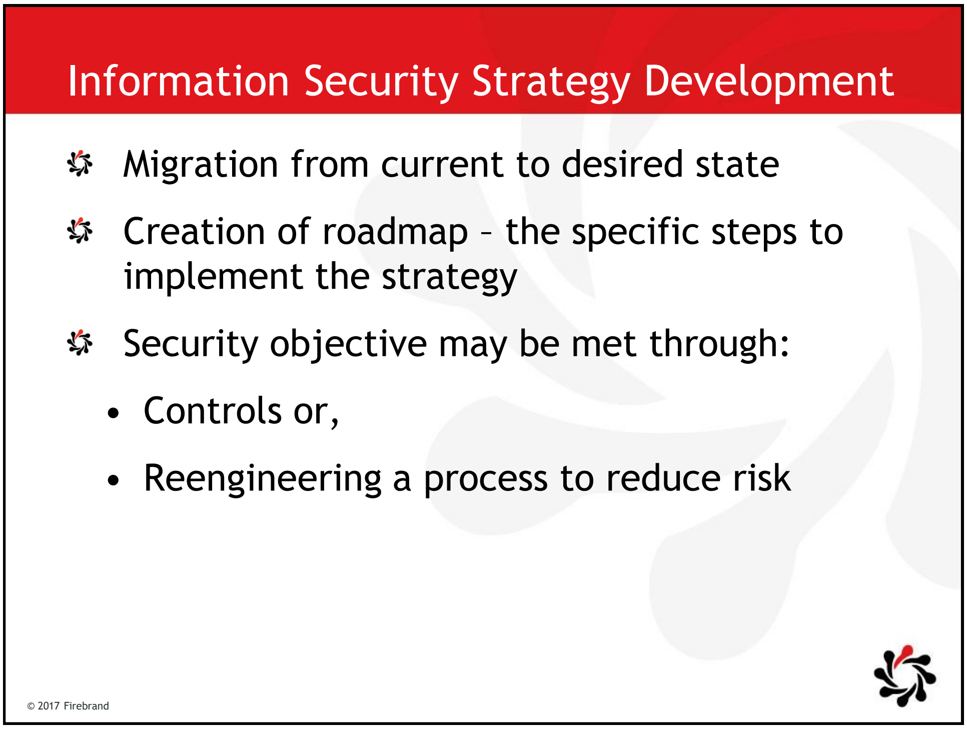
An information security management system

- Contains:
  - 14 Clauses, 35 Controls Objectives and 114 controls



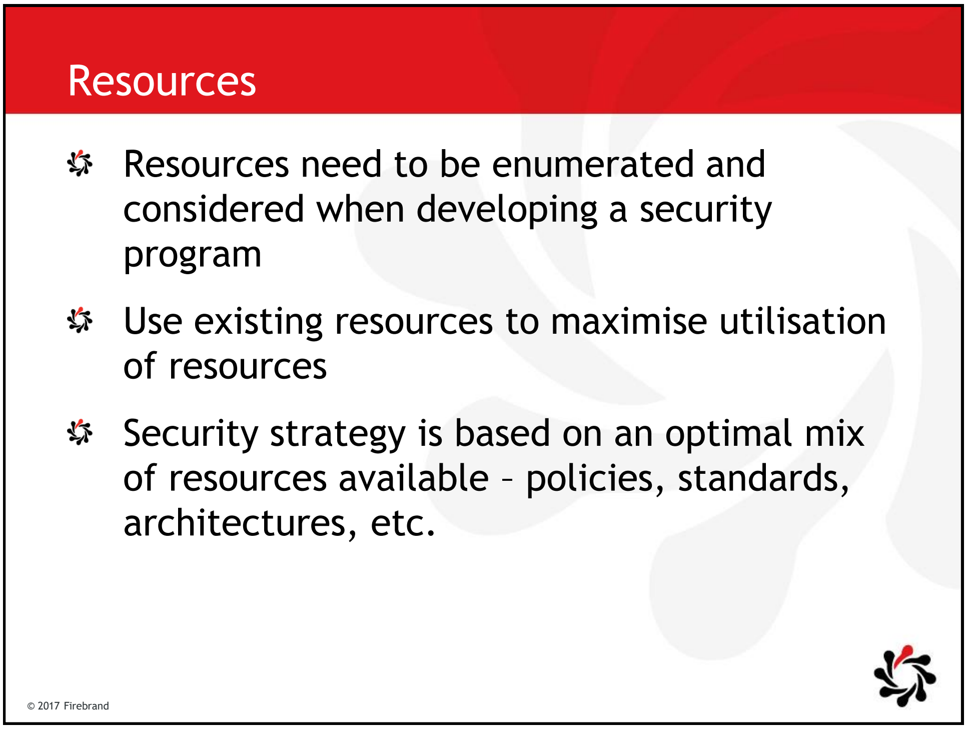
## Risk Management

- The basis for most security programs is Risk Management:
  - Development of controls
  - Acceptable risk
  - Operational cost of risk management
- The CISM must remember that risk is measured according to potential impact on the ability of the business to meet its mission – not just on the impact on IT.



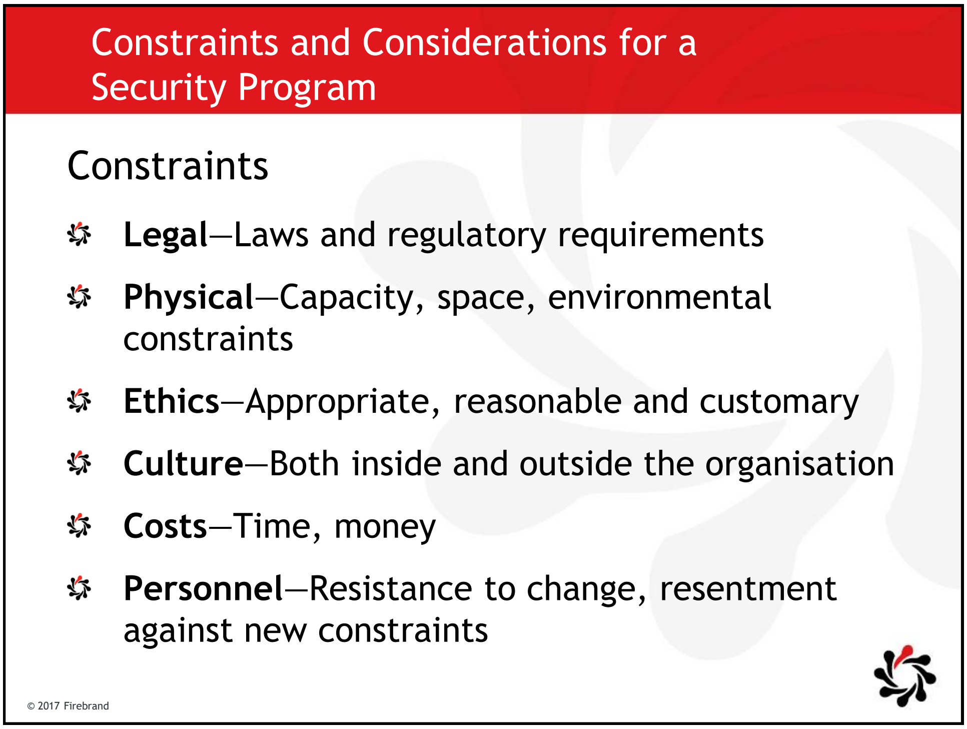
## Information Security Strategy Development

- Migration from current to desired state
- Creation of roadmap – the specific steps to implement the strategy
- Security objective may be met through:
  - Controls or,
  - Reengineering a process to reduce risk



## Resources

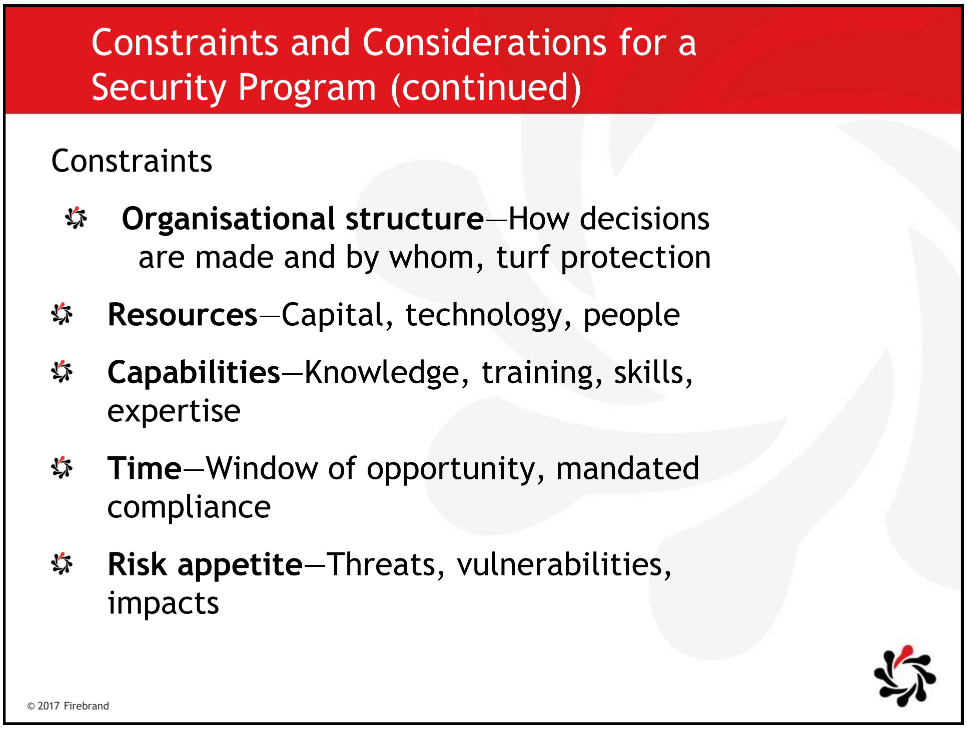
- Resources need to be enumerated and considered when developing a security program
- Use existing resources to maximise utilisation of resources
- Security strategy is based on an optimal mix of resources available – policies, standards, architectures, etc.



## Constraints and Considerations for a Security Program

Constraints

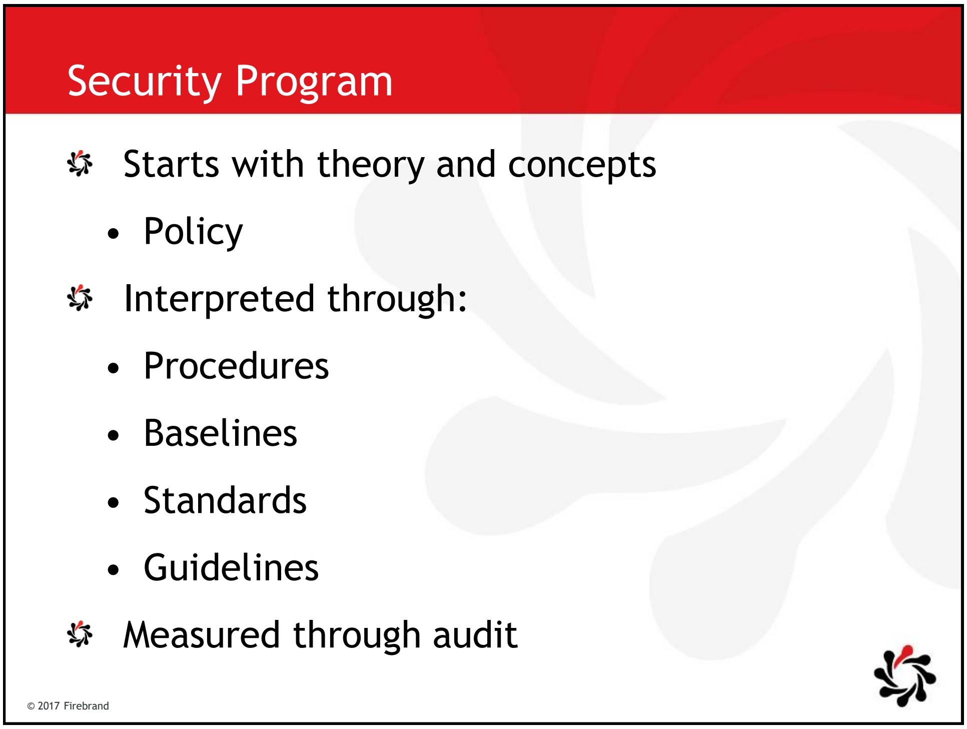
- **Legal**—Laws and regulatory requirements
- **Physical**—Capacity, space, environmental constraints
- **Ethics**—Appropriate, reasonable and customary
- **Culture**—Both inside and outside the organisation
- **Costs**—Time, money
- **Personnel**—Resistance to change, resentment against new constraints



## Constraints and Considerations for a Security Program (continued)

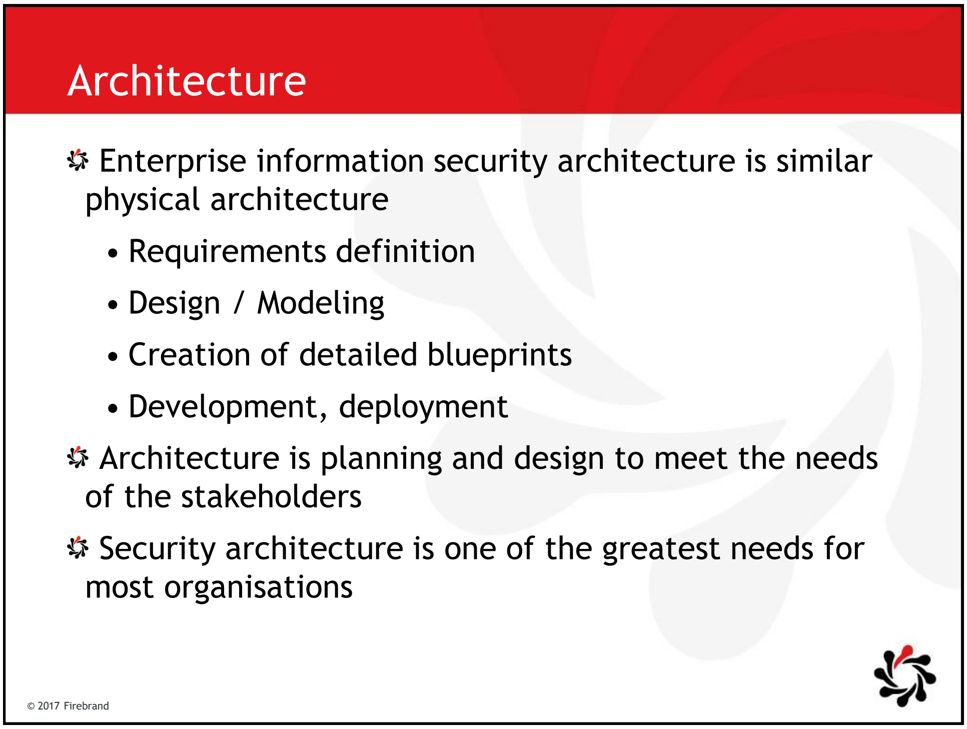
Constraints

- **Organisational structure**—How decisions are made and by whom, turf protection
- **Resources**—Capital, technology, people
- **Capabilities**—Knowledge, training, skills, expertise
- **Time**—Window of opportunity, mandated compliance
- **Risk appetite**—Threats, vulnerabilities, impacts



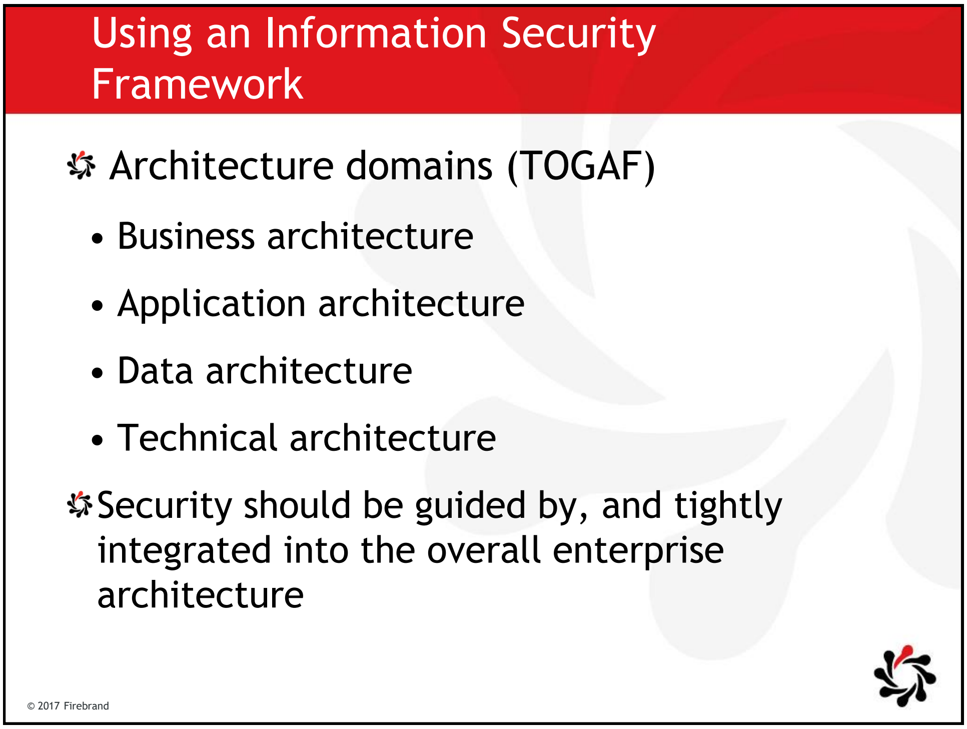
## Security Program

- Starts with theory and concepts
  - Policy
- Interpreted through:
  - Procedures
  - Baselines
  - Standards
  - Guidelines
- Measured through audit



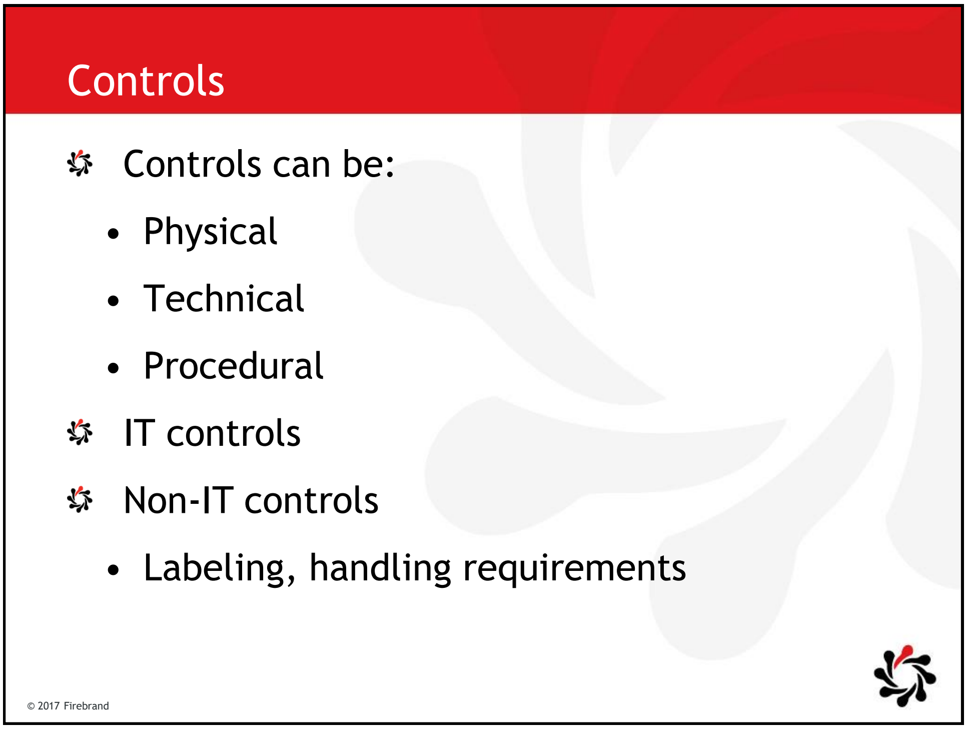
## Architecture

- Enterprise information security architecture is similar physical architecture
  - Requirements definition
  - Design / Modeling
  - Creation of detailed blueprints
  - Development, deployment
- Architecture is planning and design to meet the needs of the stakeholders
- Security architecture is one of the greatest needs for most organisations



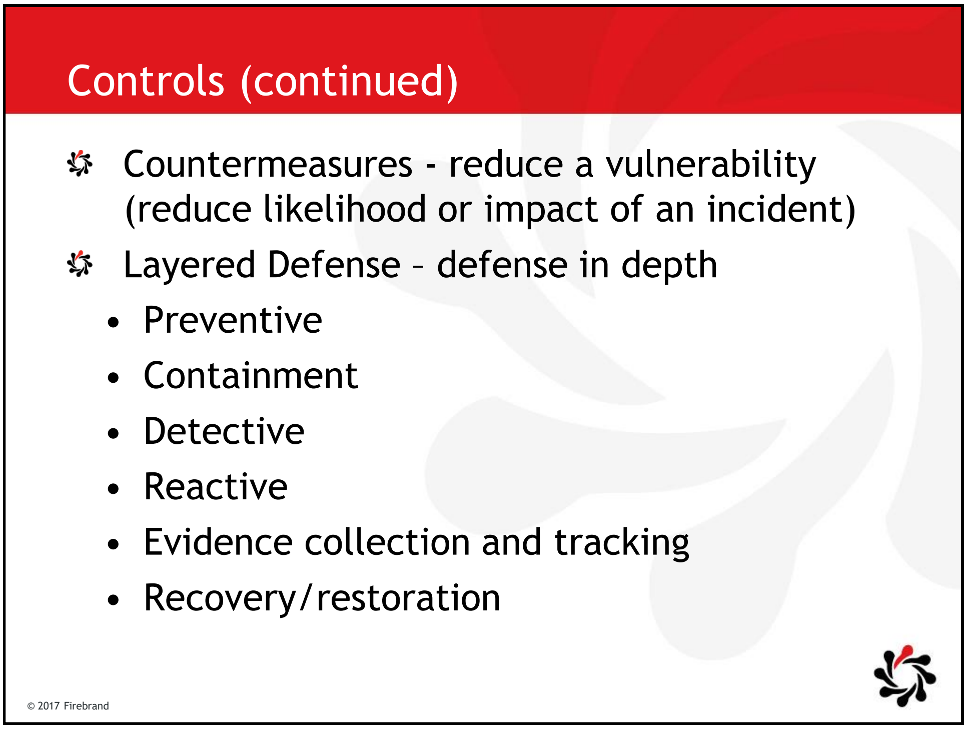
## Using an Information Security Framework

- Architecture domains (TOGAF)
  - Business architecture
  - Application architecture
  - Data architecture
  - Technical architecture
- Security should be guided by, and tightly integrated into the overall enterprise architecture



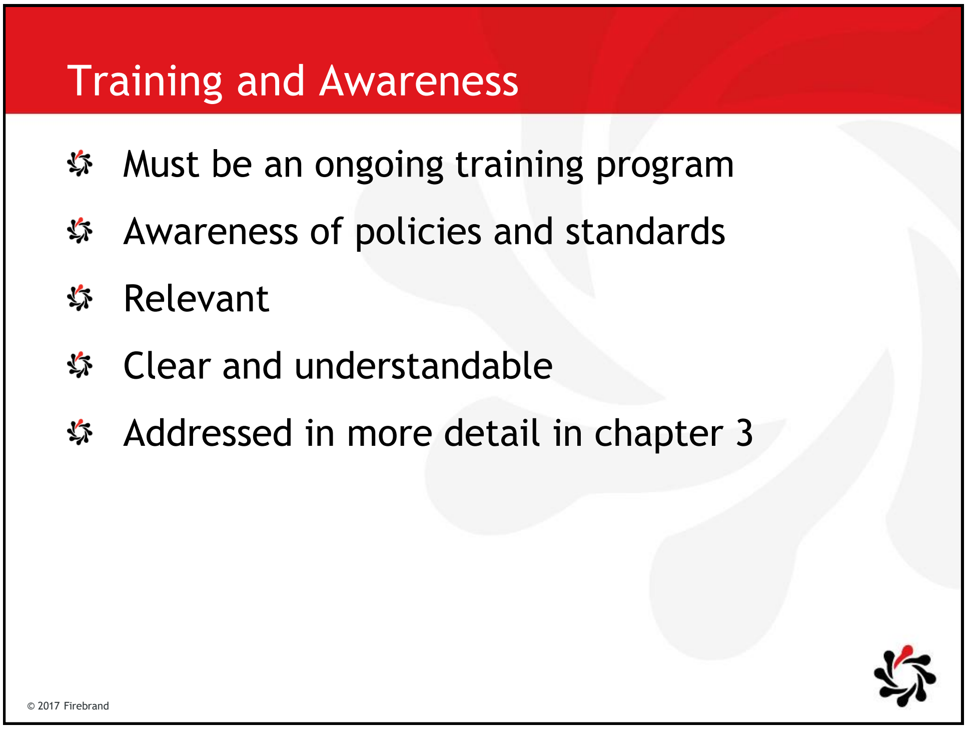
## Controls

- Controls can be:
  - Physical
  - Technical
  - Procedural
- IT controls
- Non-IT controls
  - Labeling, handling requirements



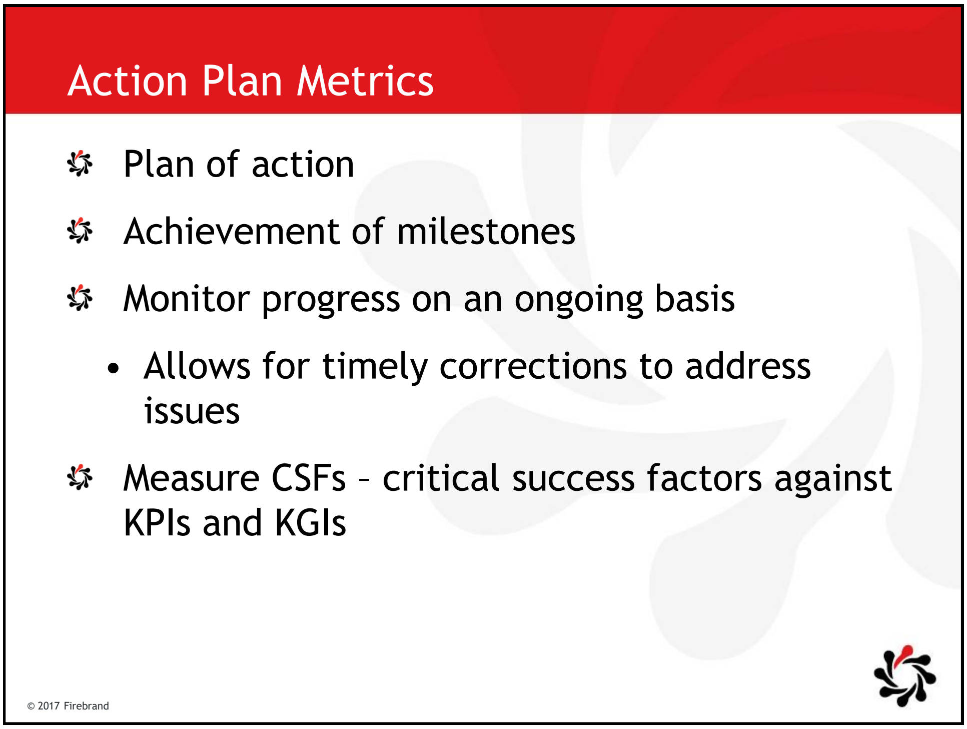
## Controls (continued)

- Countermeasures - reduce a vulnerability (reduce likelihood or impact of an incident)
- Layered Defense – defense in depth
  - Preventive
  - Containment
  - Detective
  - Reactive
  - Evidence collection and tracking
  - Recovery/restoration



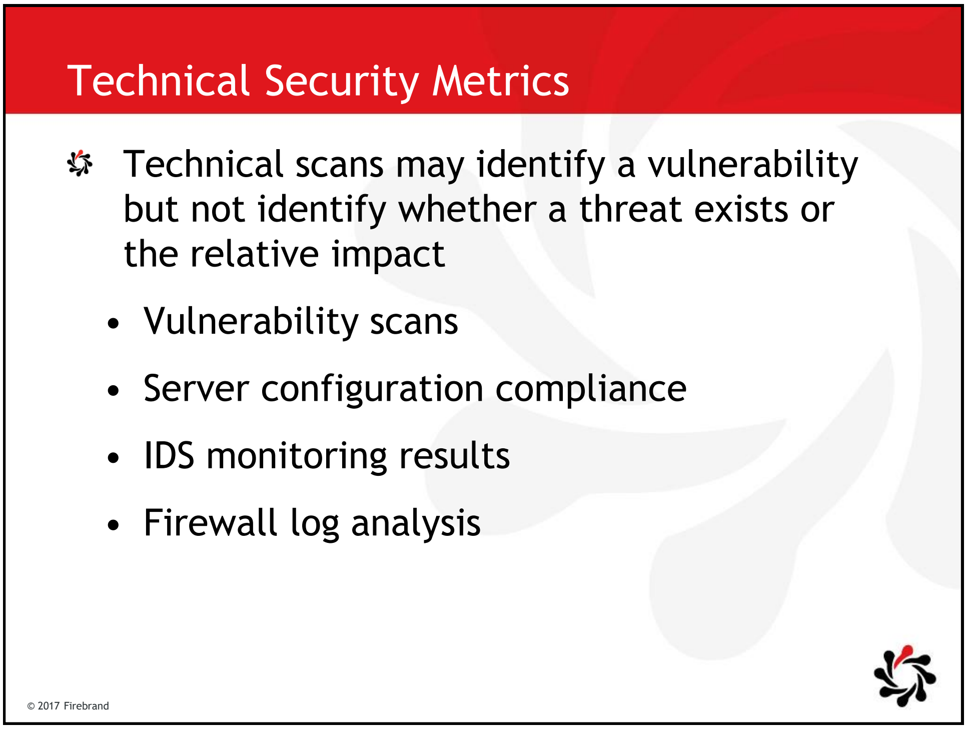
## Training and Awareness

- Must be an ongoing training program
- Awareness of policies and standards
- Relevant
- Clear and understandable
- Addressed in more detail in chapter 3



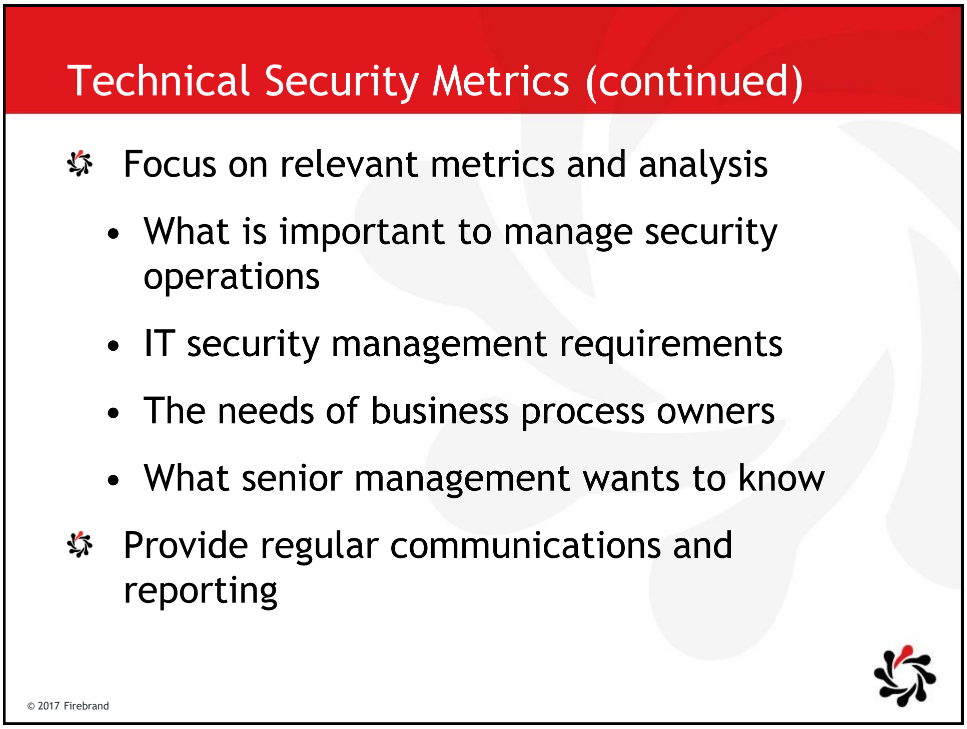
## Action Plan Metrics

- Plan of action
- Achievement of milestones
- Monitor progress on an ongoing basis
  - Allows for timely corrections to address issues
- Measure CSFs – critical success factors against KPIs and KGIs



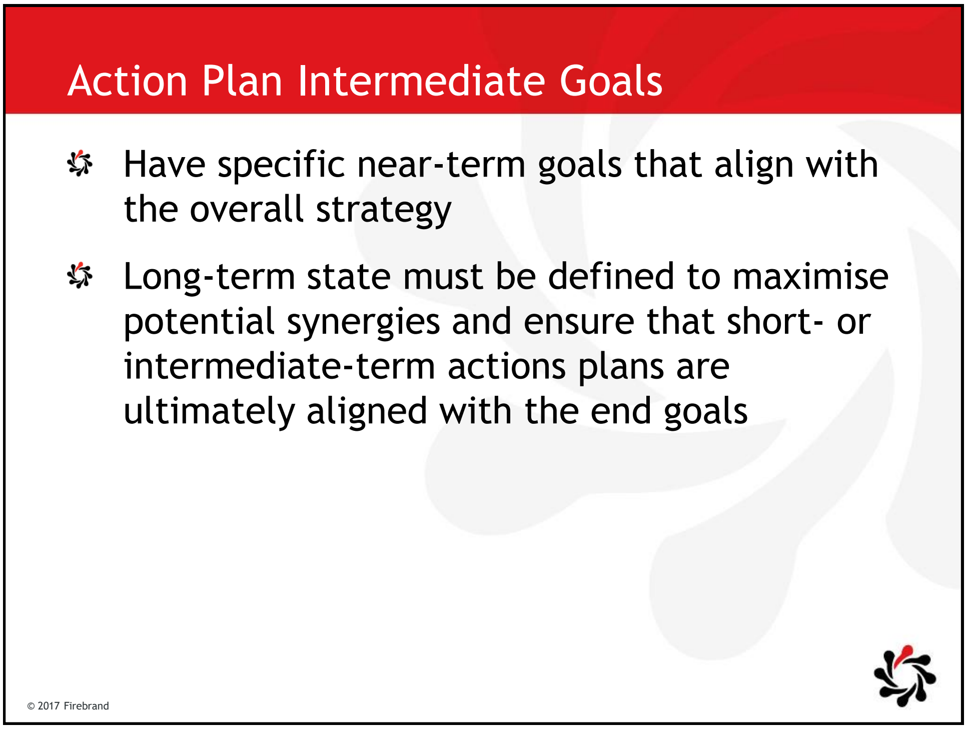
## Technical Security Metrics

- Technical scans may identify a vulnerability but not identify whether a threat exists or the relative impact
  - Vulnerability scans
  - Server configuration compliance
  - IDS monitoring results
  - Firewall log analysis



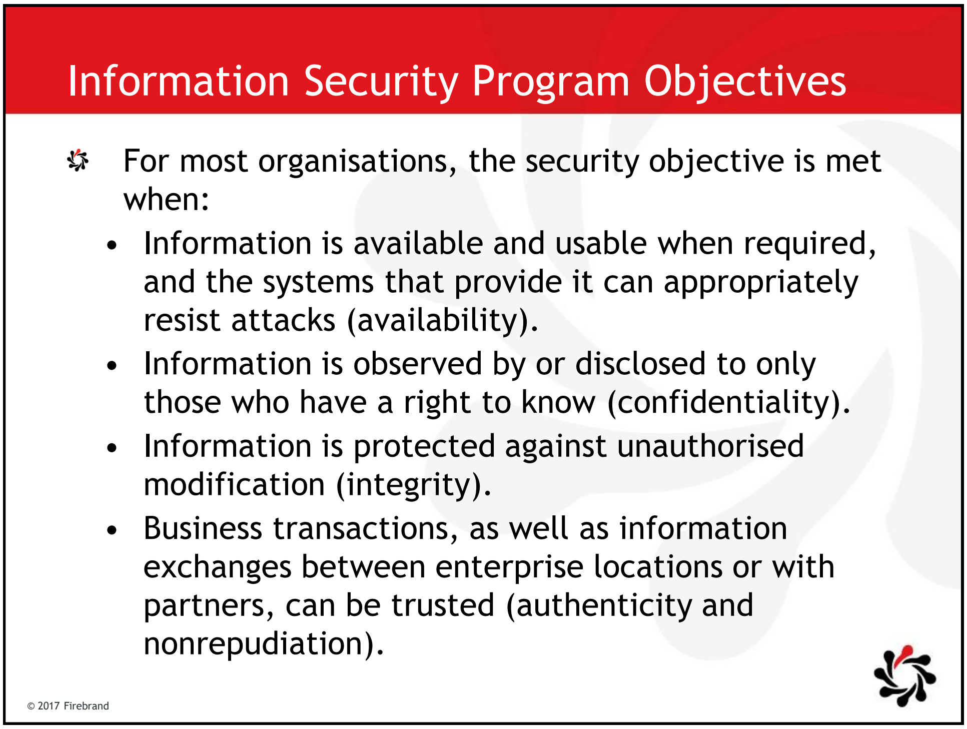
## Technical Security Metrics (continued)

- Focus on relevant metrics and analysis
  - What is important to manage security operations
  - IT security management requirements
  - The needs of business process owners
  - What senior management wants to know
- Provide regular communications and reporting



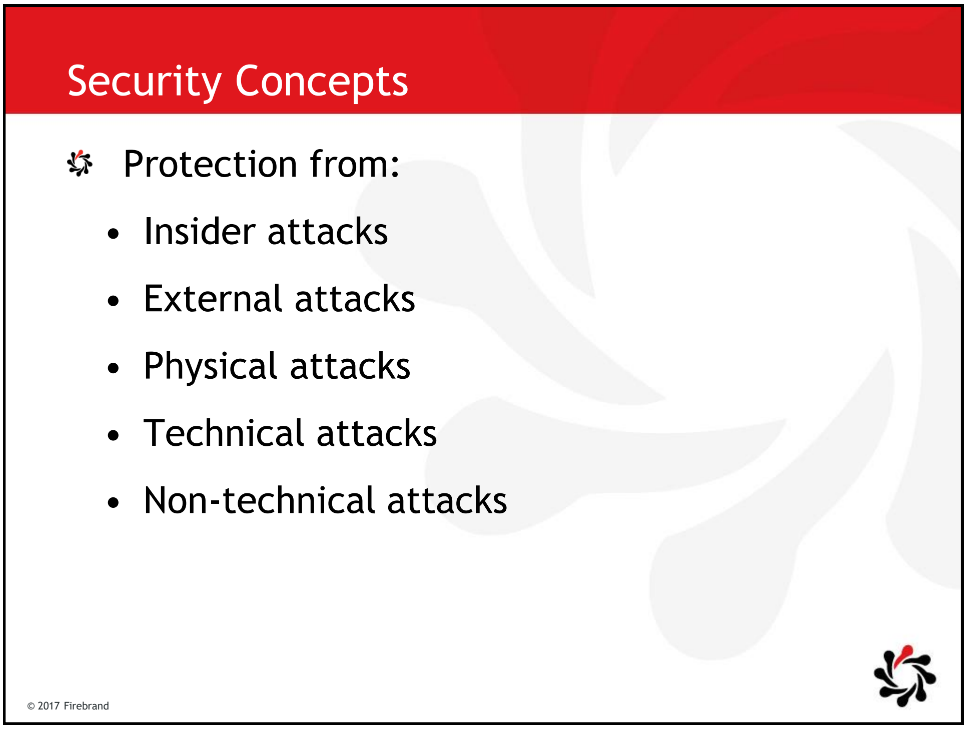
## Action Plan Intermediate Goals

- Have specific near-term goals that align with the overall strategy
- Long-term state must be defined to maximise potential synergies and ensure that short- or intermediate-term actions plans are ultimately aligned with the end goals



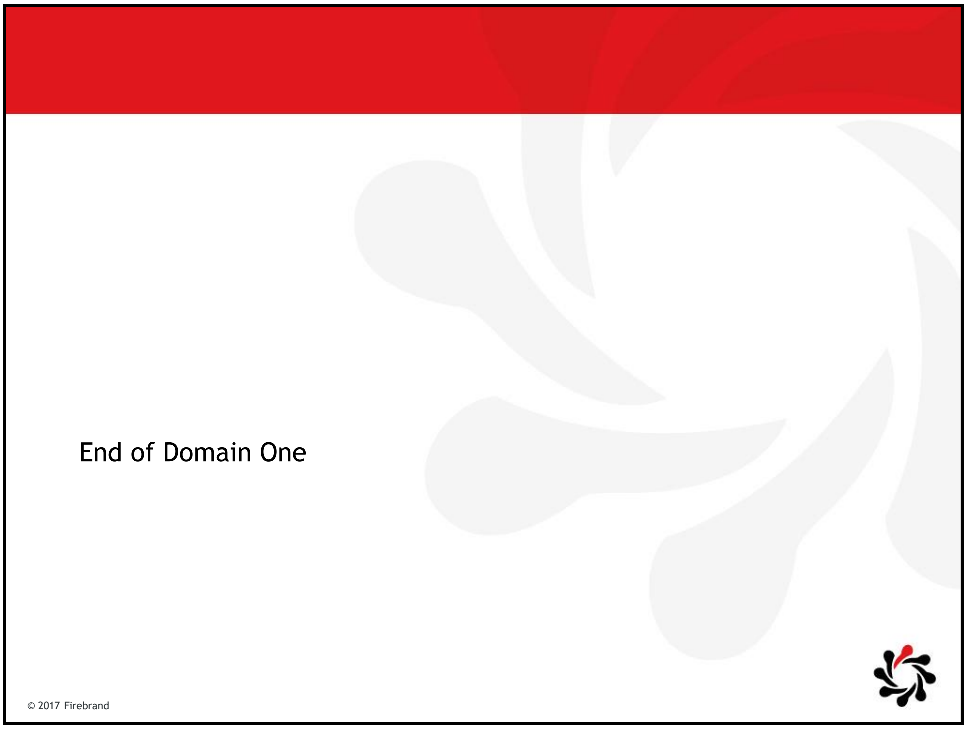
## Information Security Program Objectives

- For most organisations, the security objective is met when:
  - Information is available and usable when required, and the systems that provide it can appropriately resist attacks (availability).
  - Information is observed by or disclosed to only those who have a right to know (confidentiality).
  - Information is protected against unauthorised modification (integrity).
  - Business transactions, as well as information exchanges between enterprise locations or with partners, can be trusted (authenticity and nonrepudiation).

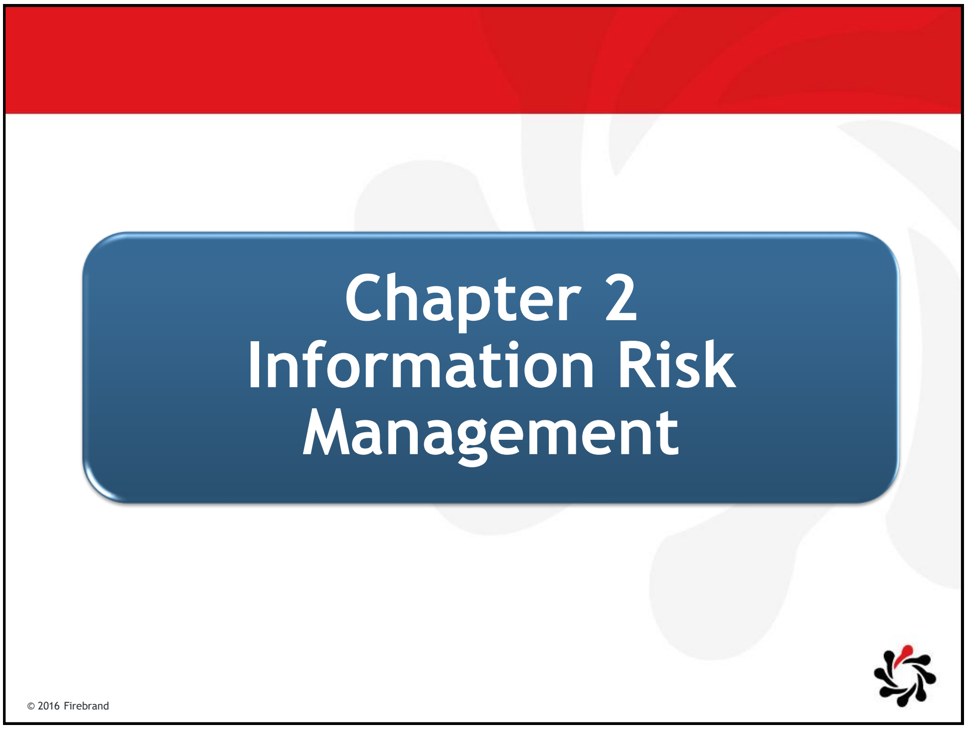


## Security Concepts

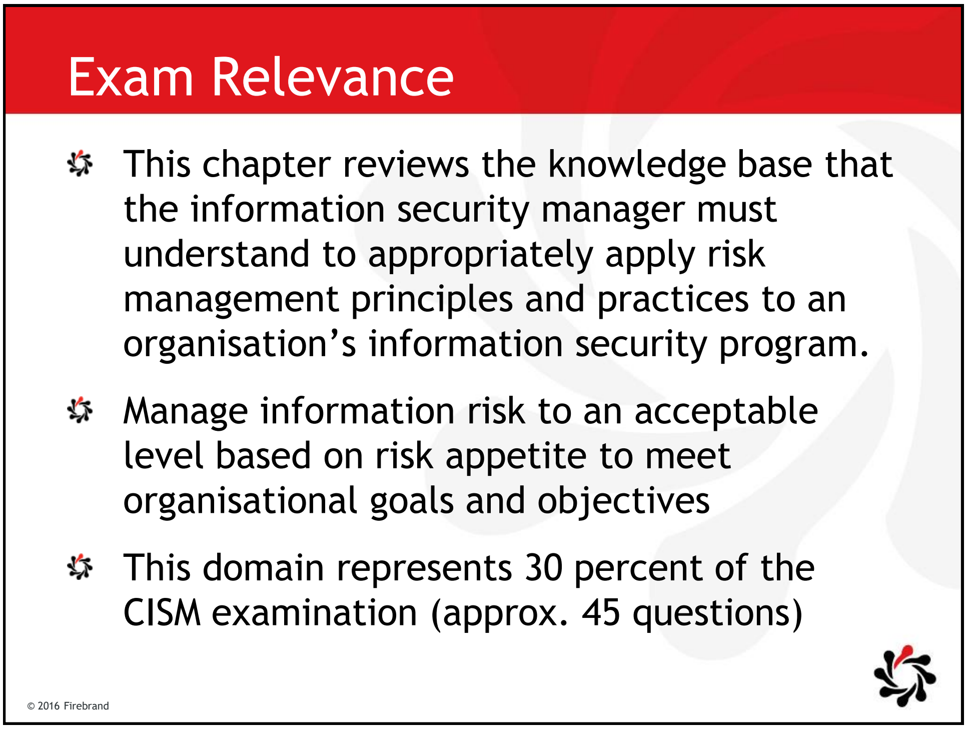
- Protection from:
  - Insider attacks
  - External attacks
  - Physical attacks
  - Technical attacks
  - Non-technical attacks



End of Domain One

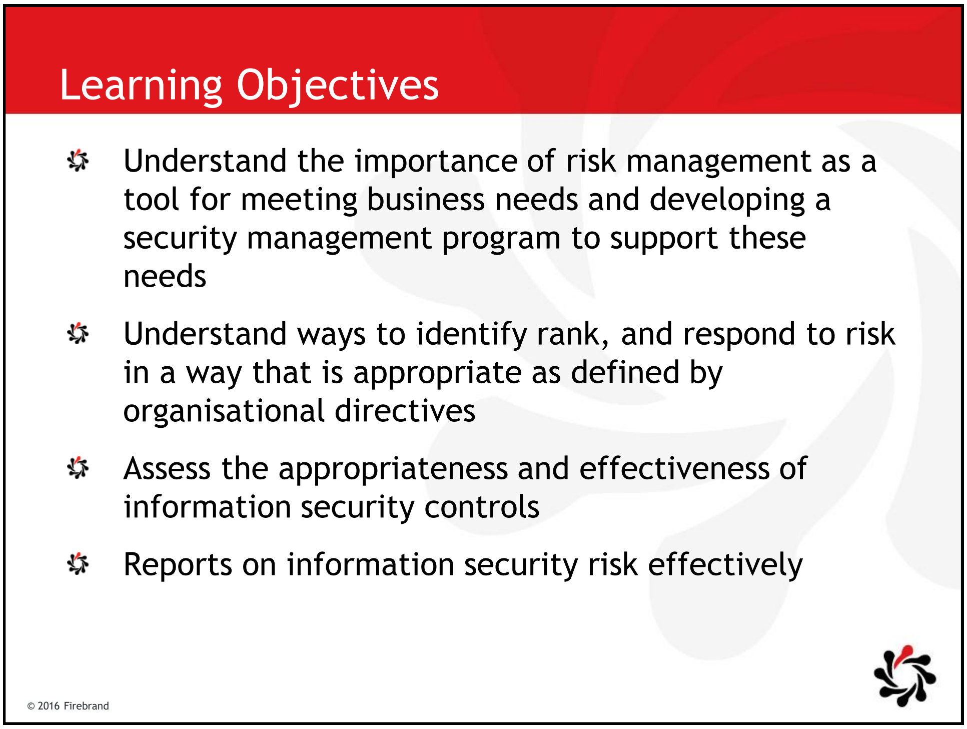


# Chapter 2 Information Risk Management



## Exam Relevance

- This chapter reviews the knowledge base that the information security manager must understand to appropriately apply risk management principles and practices to an organisation's information security program.
- Manage information risk to an acceptable level based on risk appetite to meet organisational goals and objectives
- This domain represents 30 percent of the CISM examination (approx. 45 questions)



## Learning Objectives

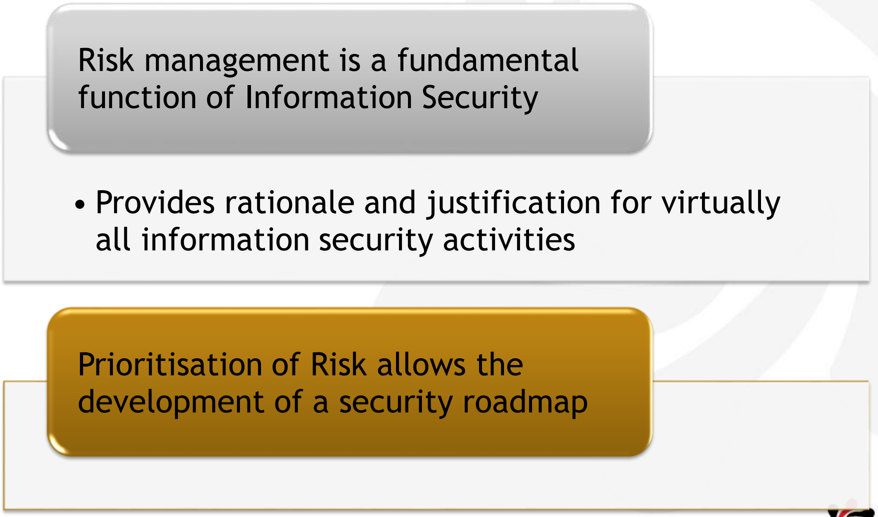
- Understand the importance of risk management as a tool for meeting business needs and developing a security management program to support these needs
- Understand ways to identify rank, and respond to risk in a way that is appropriate as defined by organisational directives
- Assess the appropriateness and effectiveness of information security controls
- Reports on information security risk effectively

# Risk Management

## Definition of Risk

- Rick can be defined as the combination of the probability (or likelihood) of an event and its consequences
- Risk is present when a threat can exploit a vulnerability and cause damage to an asset.
- Exposure (attack surface) represents the probability and impact of compromise

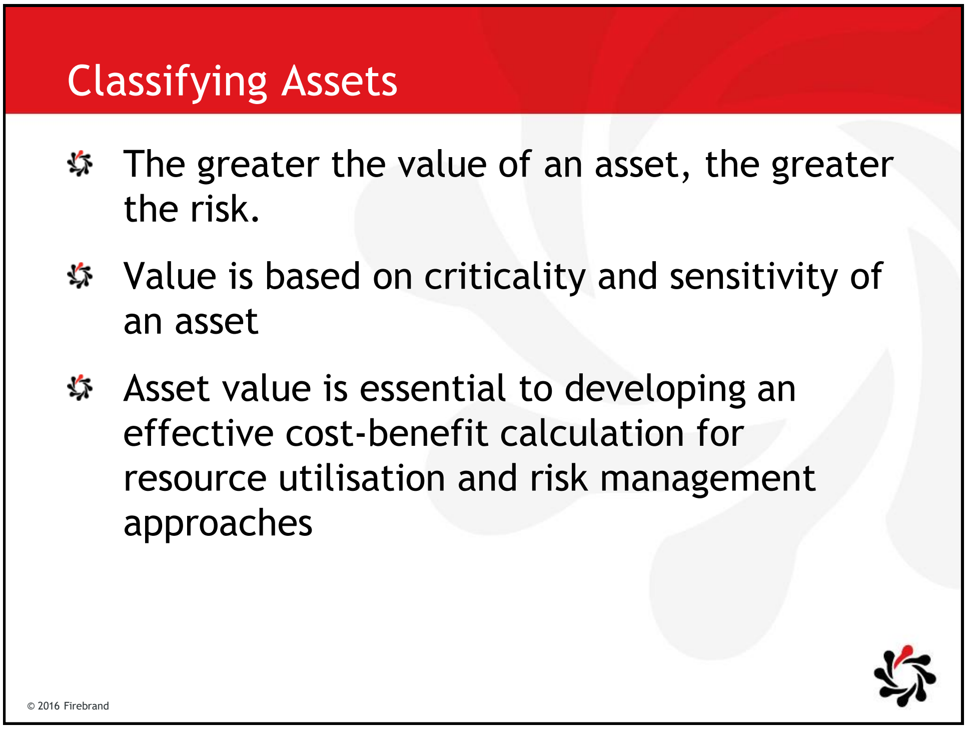
## Why is Risk Important?



Risk management is a fundamental function of Information Security

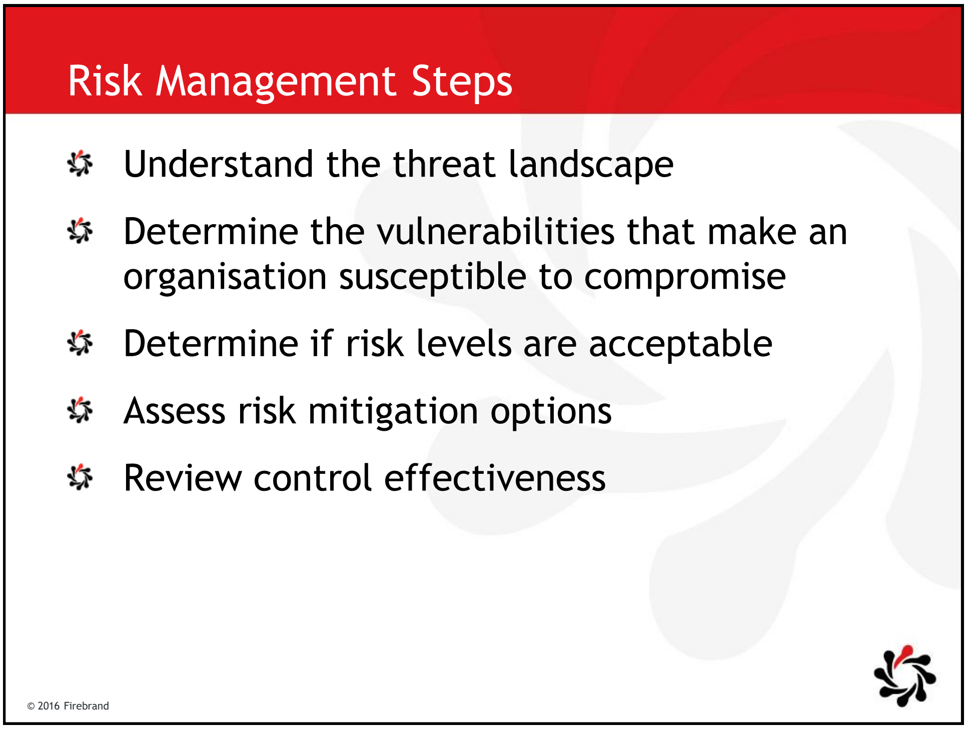
- Provides rationale and justification for virtually all information security activities

Prioritisation of Risk allows the development of a security roadmap



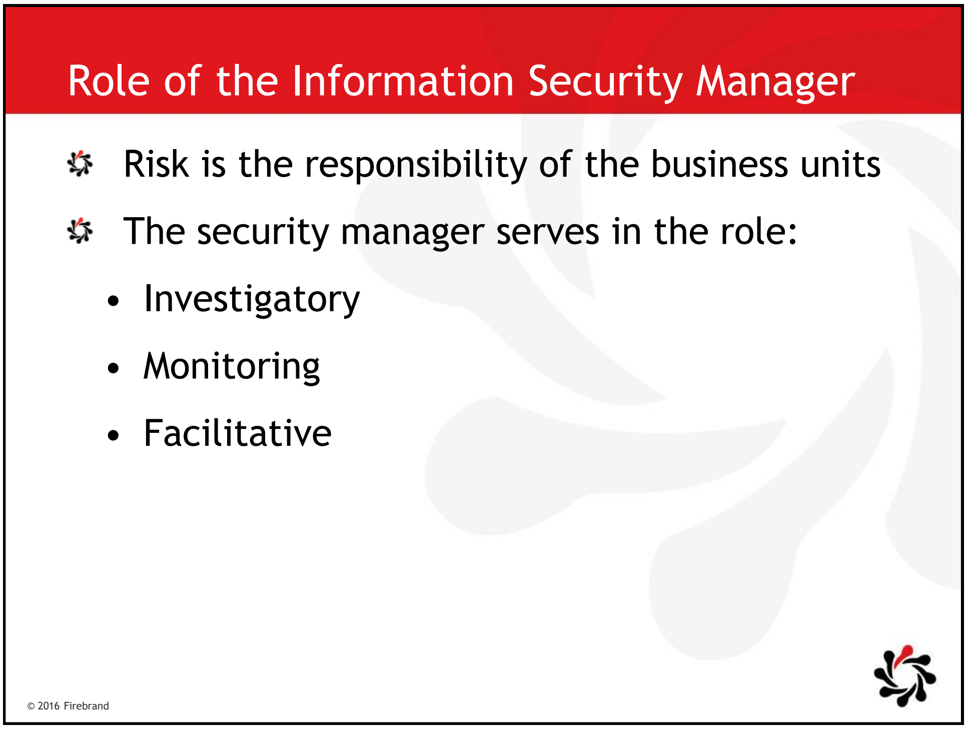
## Classifying Assets

- The greater the value of an asset, the greater the risk.
- Value is based on criticality and sensitivity of an asset
- Asset value is essential to developing an effective cost-benefit calculation for resource utilisation and risk management approaches



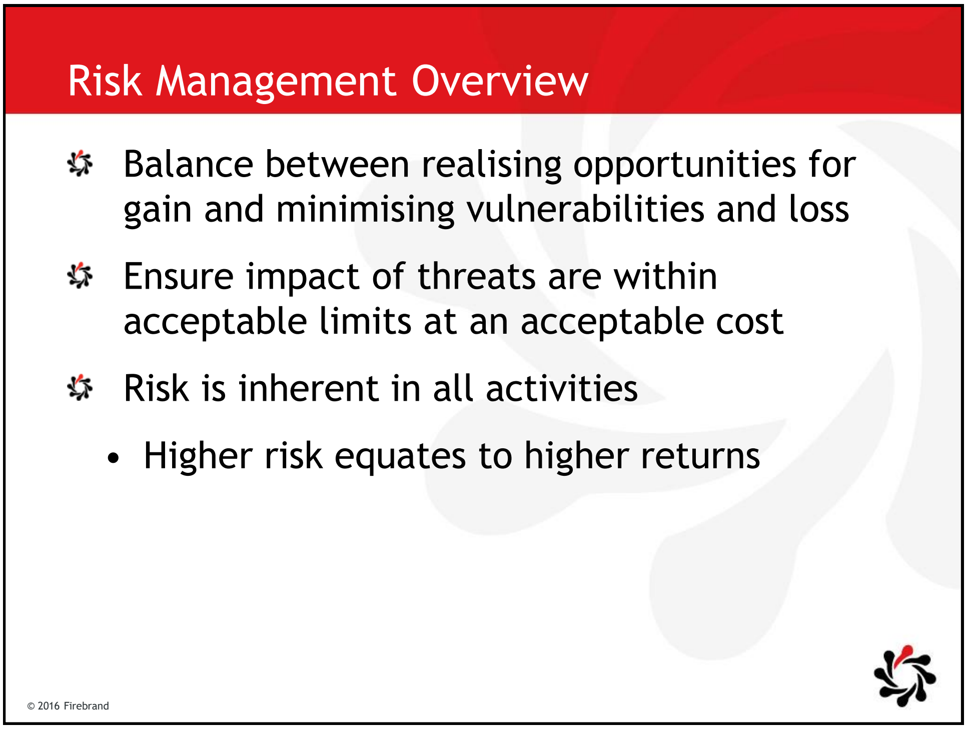
## Risk Management Steps

- Understand the threat landscape
- Determine the vulnerabilities that make an organisation susceptible to compromise
- Determine if risk levels are acceptable
- Assess risk mitigation options
- Review control effectiveness



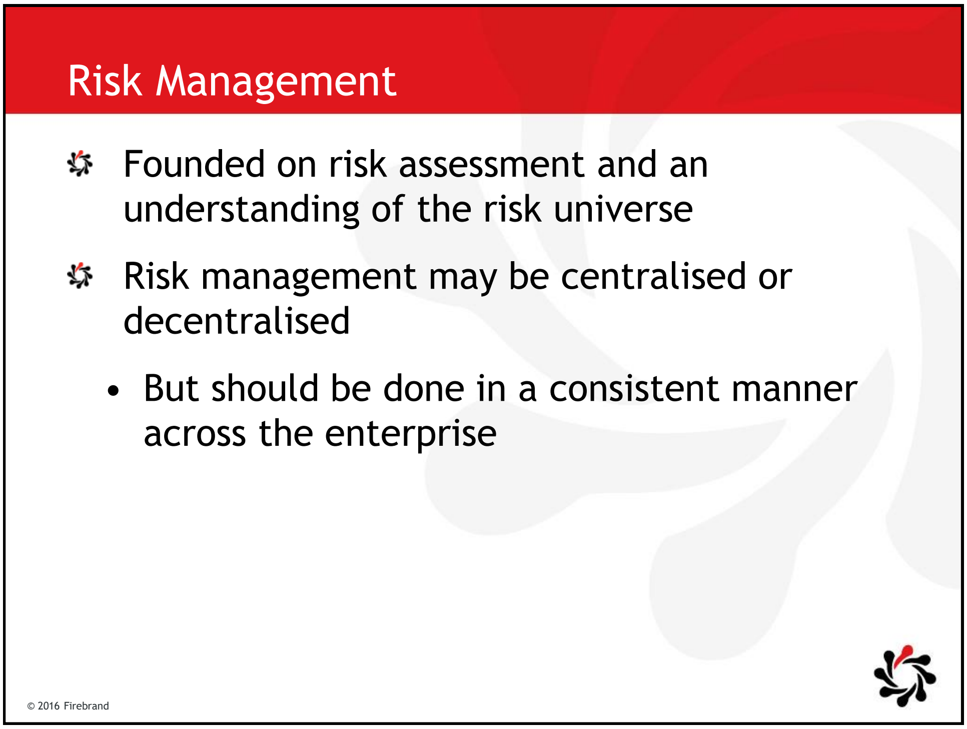
## Role of the Information Security Manager

- Risk is the responsibility of the business units
- The security manager serves in the role:
  - Investigatory
  - Monitoring
  - Facilitative



## Risk Management Overview

- Balance between realising opportunities for gain and minimising vulnerabilities and loss
- Ensure impact of threats are within acceptable limits at an acceptable cost
- Risk is inherent in all activities
  - Higher risk equates to higher returns

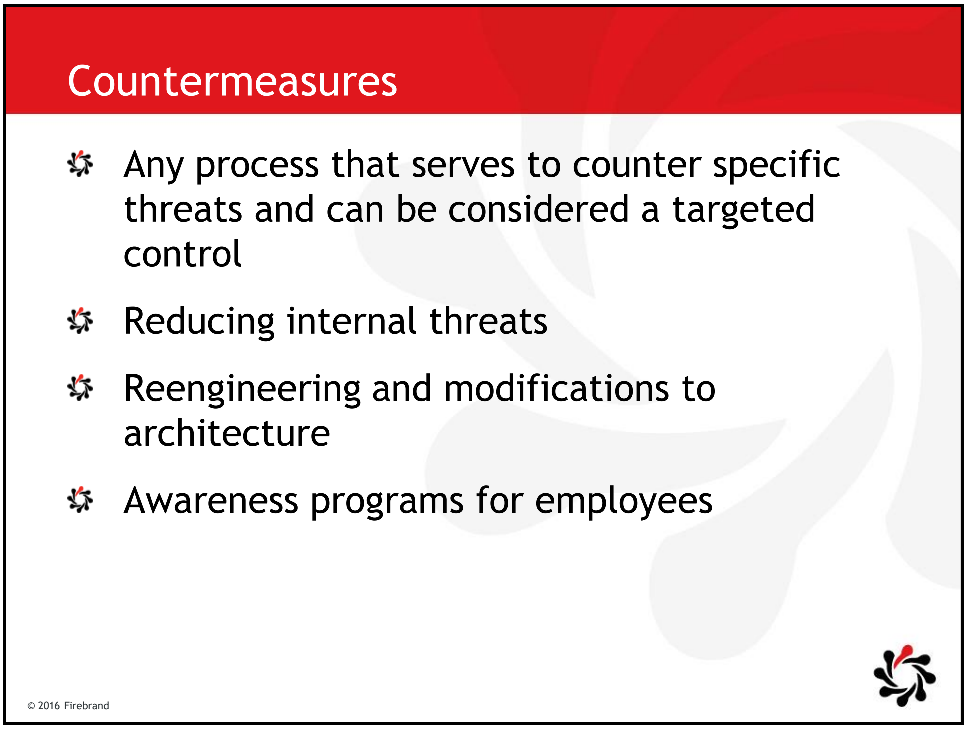


## Risk Management

- Founded on risk assessment and an understanding of the risk universe
- Risk management may be centralised or decentralised
  - But should be done in a consistent manner across the enterprise

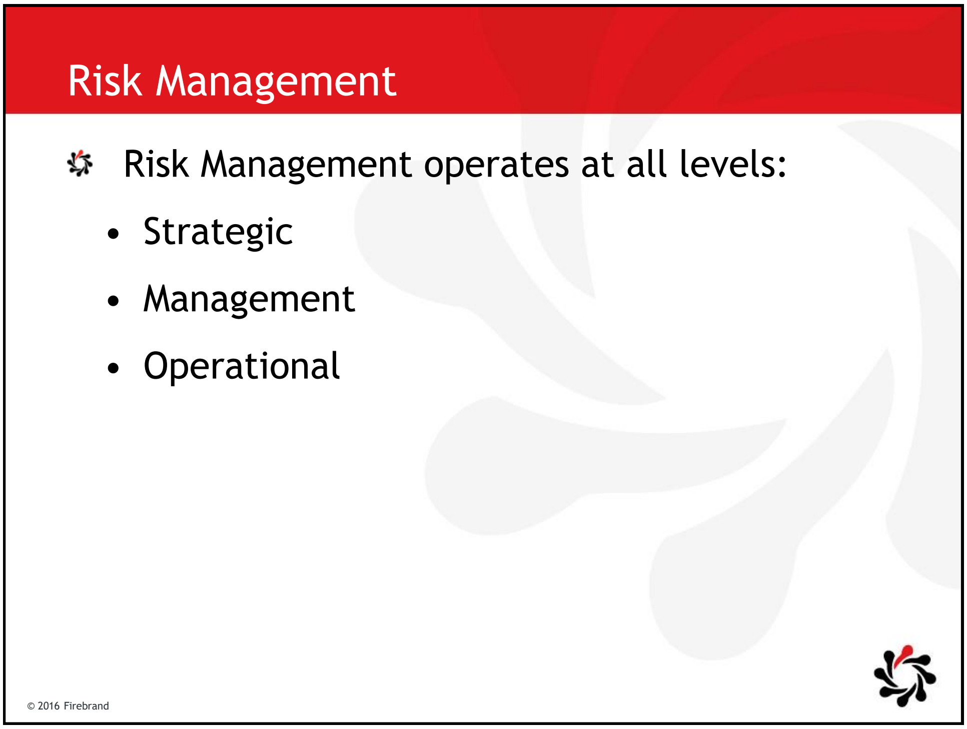
## Controls

- Are designed as part of a risk management framework, which incorporates policies, standards, procedures, practices and organisational structures
- Provide reasonable assurance that business objectives are achieved and undesired events are:
  - Prevented
  - Detected
  - Addressed



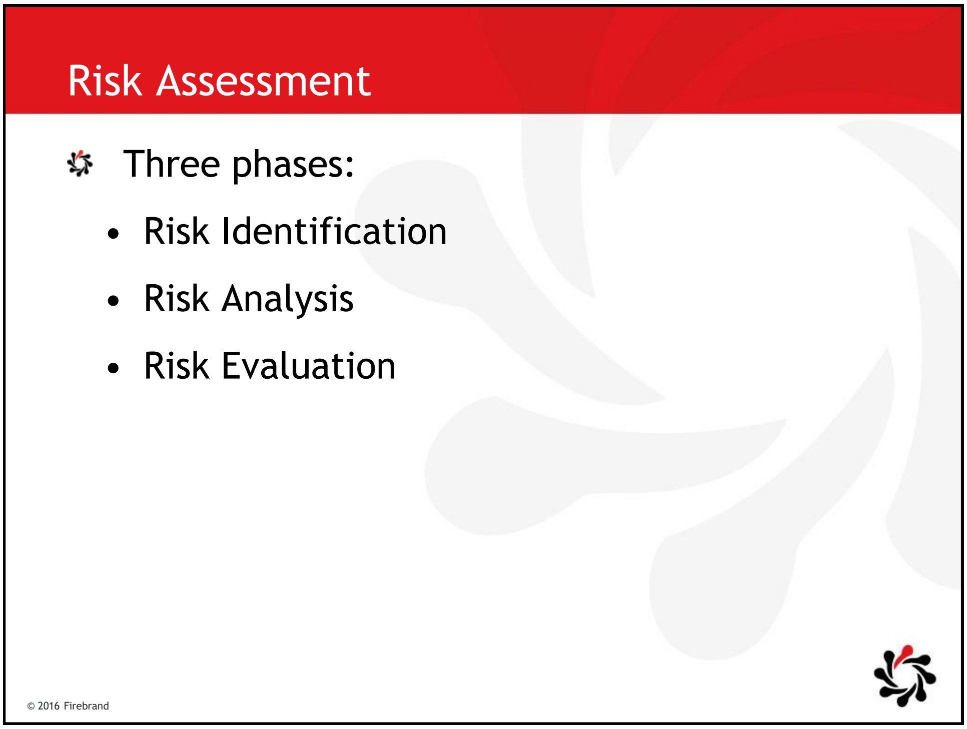
## Countermeasures

- Any process that serves to counter specific threats and can be considered a targeted control
- Reducing internal threats
- Reengineering and modifications to architecture
- Awareness programs for employees



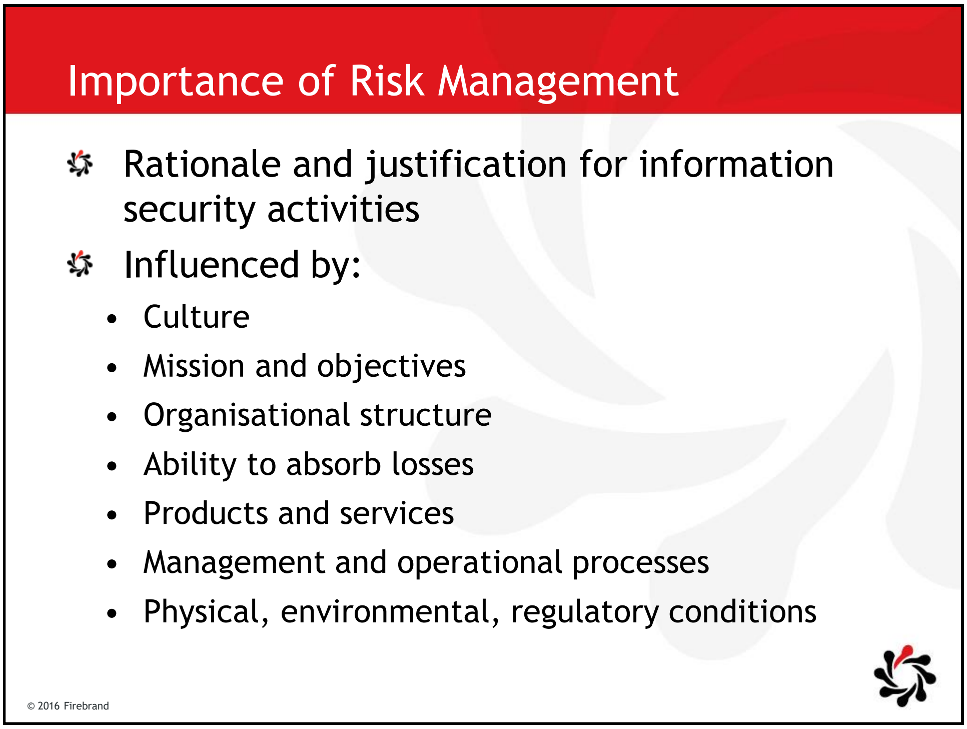
## Risk Management

- Risk Management operates at all levels:
  - Strategic
  - Management
  - Operational



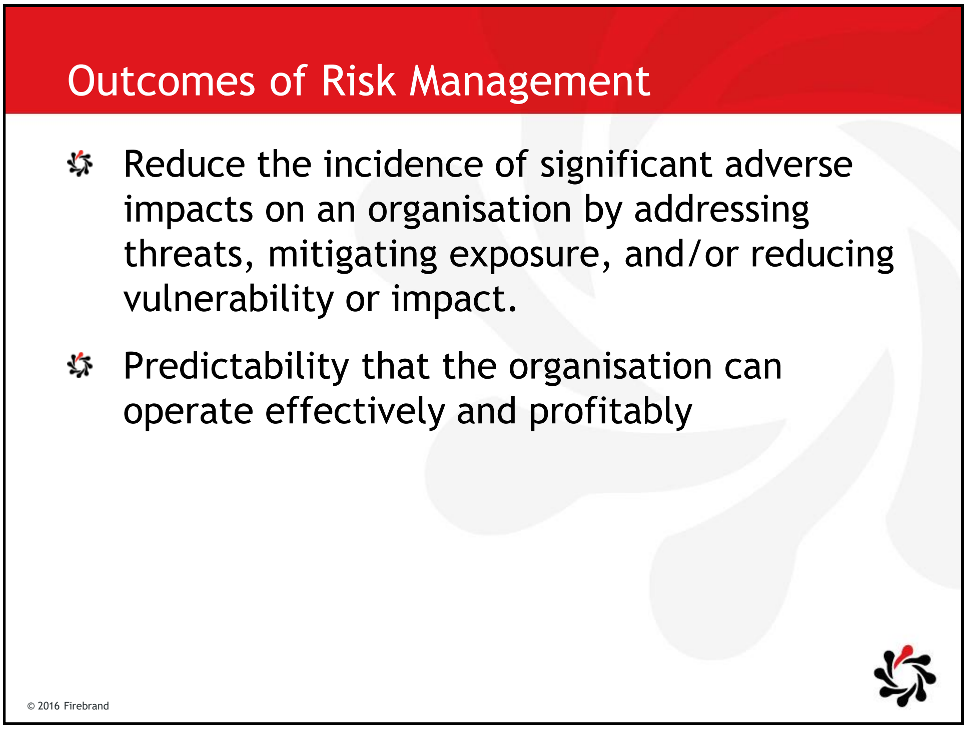
## Risk Assessment

- Three phases:
  - Risk Identification
  - Risk Analysis
  - Risk Evaluation



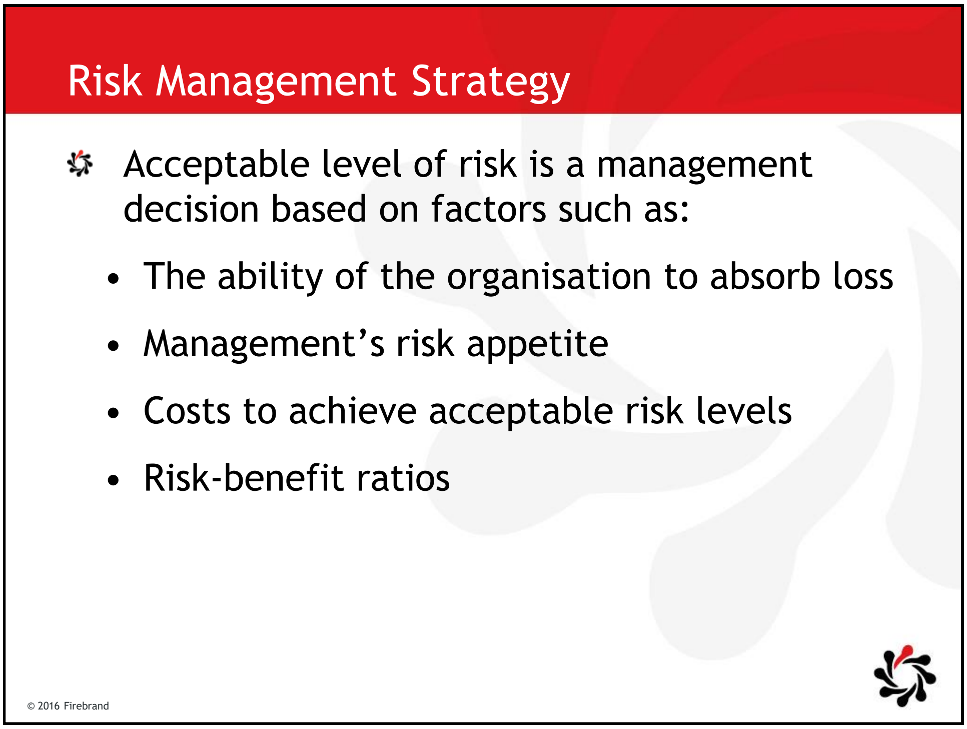
## Importance of Risk Management

- Rationale and justification for information security activities
- Influenced by:
  - Culture
  - Mission and objectives
  - Organisational structure
  - Ability to absorb losses
  - Products and services
  - Management and operational processes
  - Physical, environmental, regulatory conditions



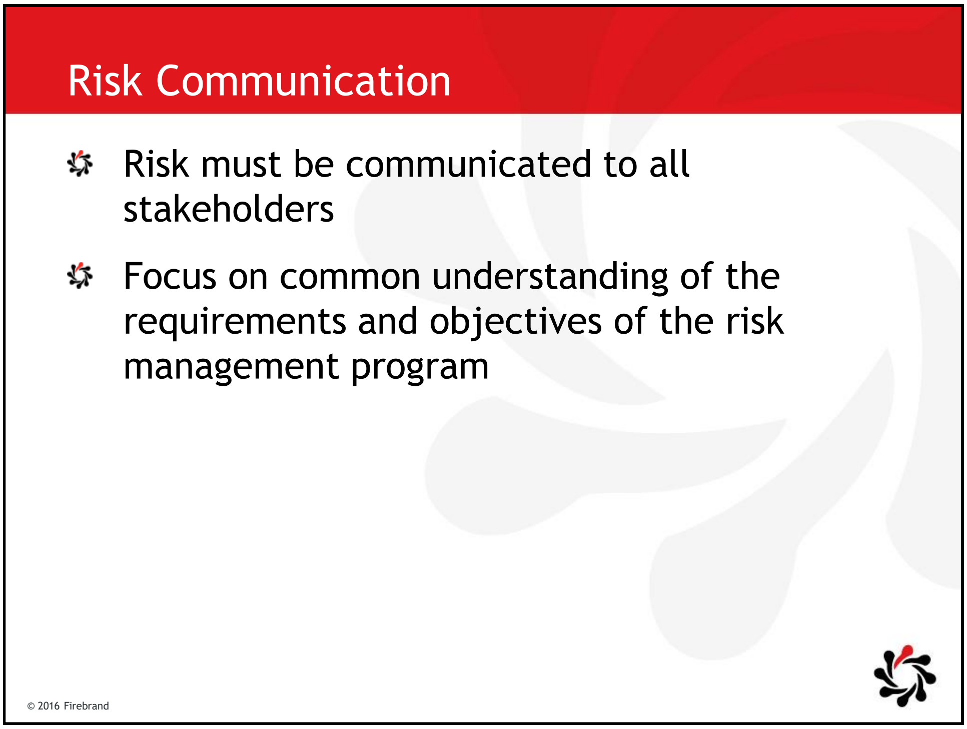
## Outcomes of Risk Management

- Reduce the incidence of significant adverse impacts on an organisation by addressing threats, mitigating exposure, and/or reducing vulnerability or impact.
- Predictability that the organisation can operate effectively and profitably



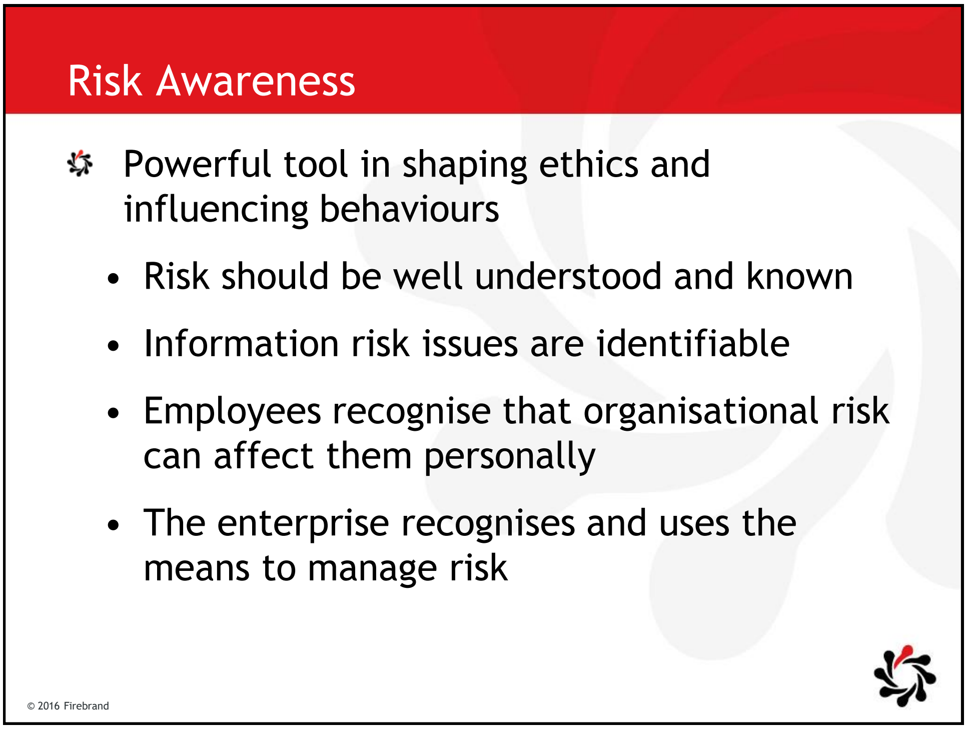
## Risk Management Strategy

- Acceptable level of risk is a management decision based on factors such as:
  - The ability of the organisation to absorb loss
  - Management's risk appetite
  - Costs to achieve acceptable risk levels
  - Risk-benefit ratios



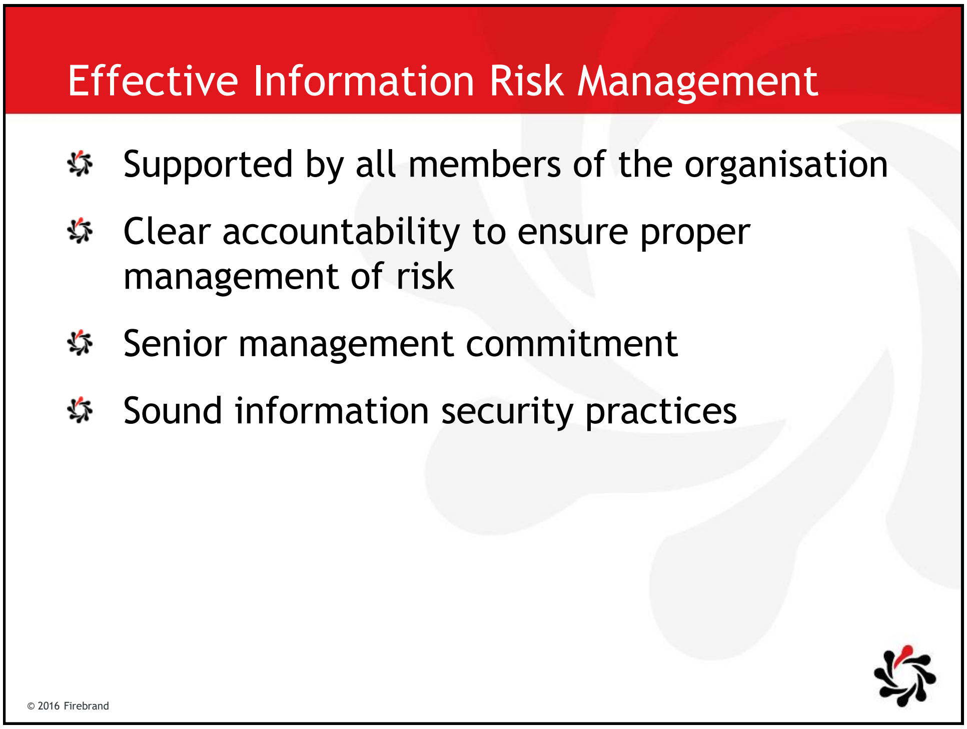
## Risk Communication

- Risk must be communicated to all stakeholders
- Focus on common understanding of the requirements and objectives of the risk management program



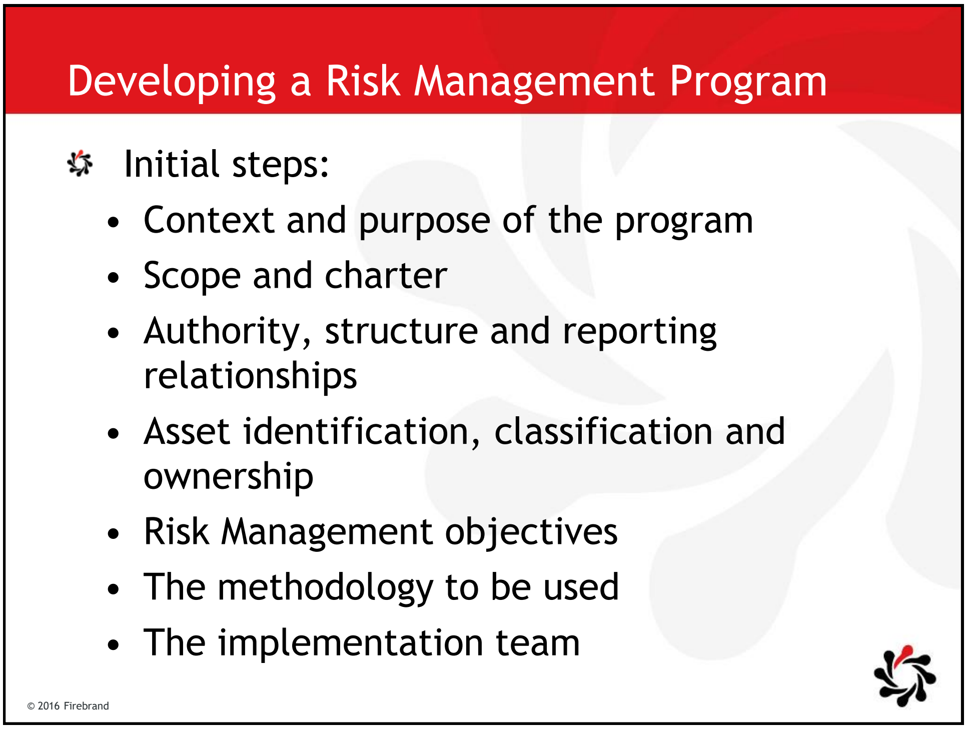
## Risk Awareness

- Powerful tool in shaping ethics and influencing behaviours
  - Risk should be well understood and known
  - Information risk issues are identifiable
  - Employees recognise that organisational risk can affect them personally
  - The enterprise recognises and uses the means to manage risk



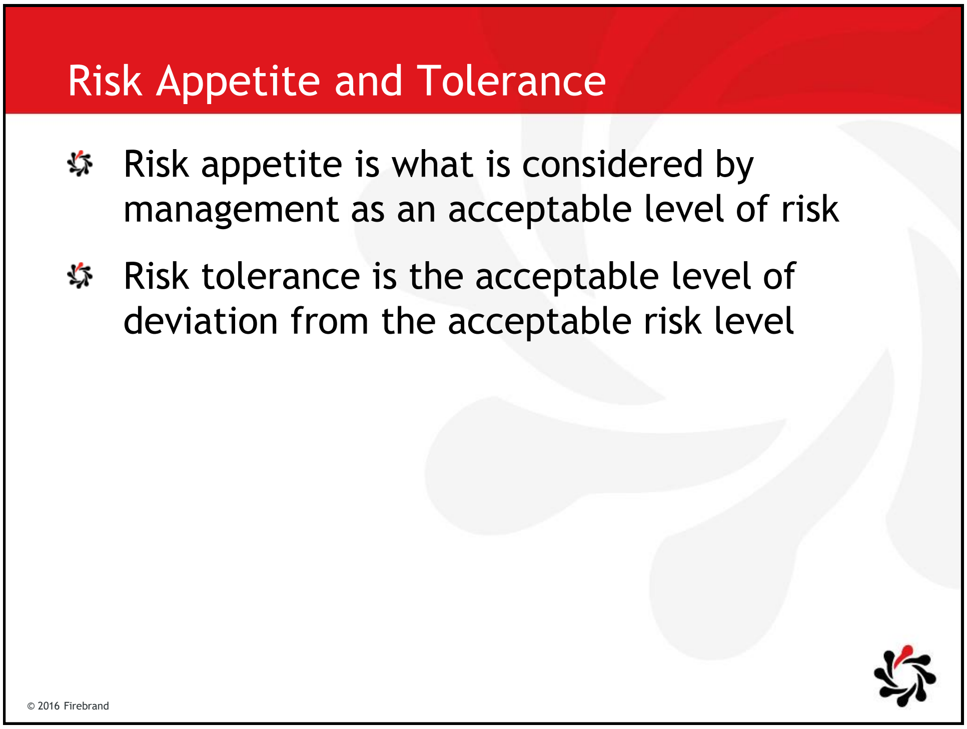
## Effective Information Risk Management

- Supported by all members of the organisation
- Clear accountability to ensure proper management of risk
- Senior management commitment
- Sound information security practices



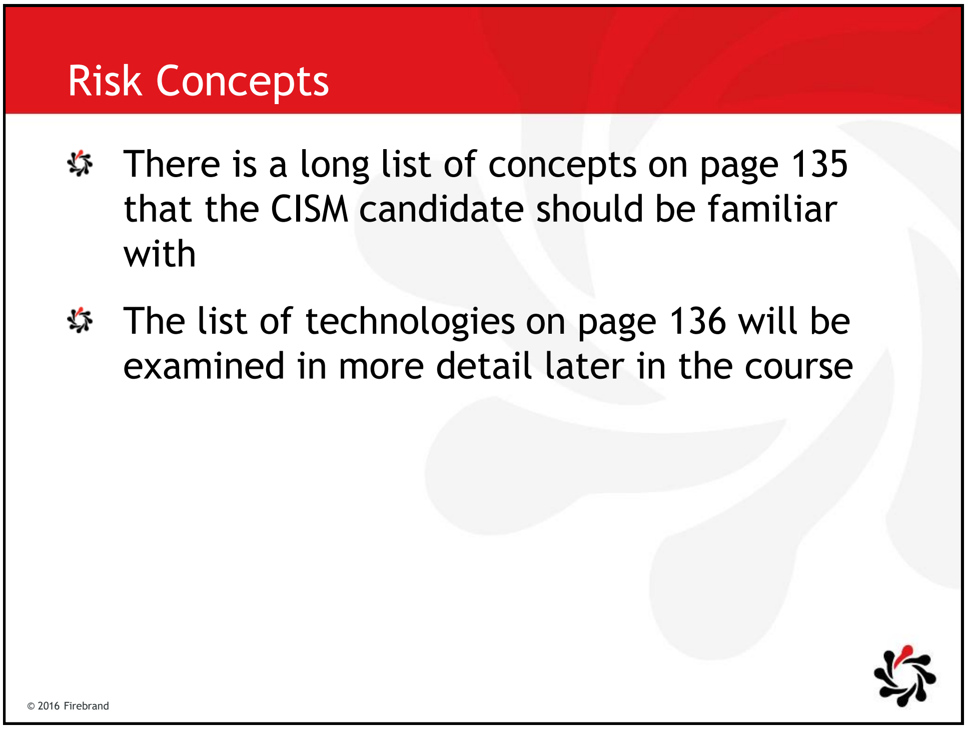
## Developing a Risk Management Program

- Initial steps:
  - Context and purpose of the program
  - Scope and charter
  - Authority, structure and reporting relationships
  - Asset identification, classification and ownership
  - Risk Management objectives
  - The methodology to be used
  - The implementation team



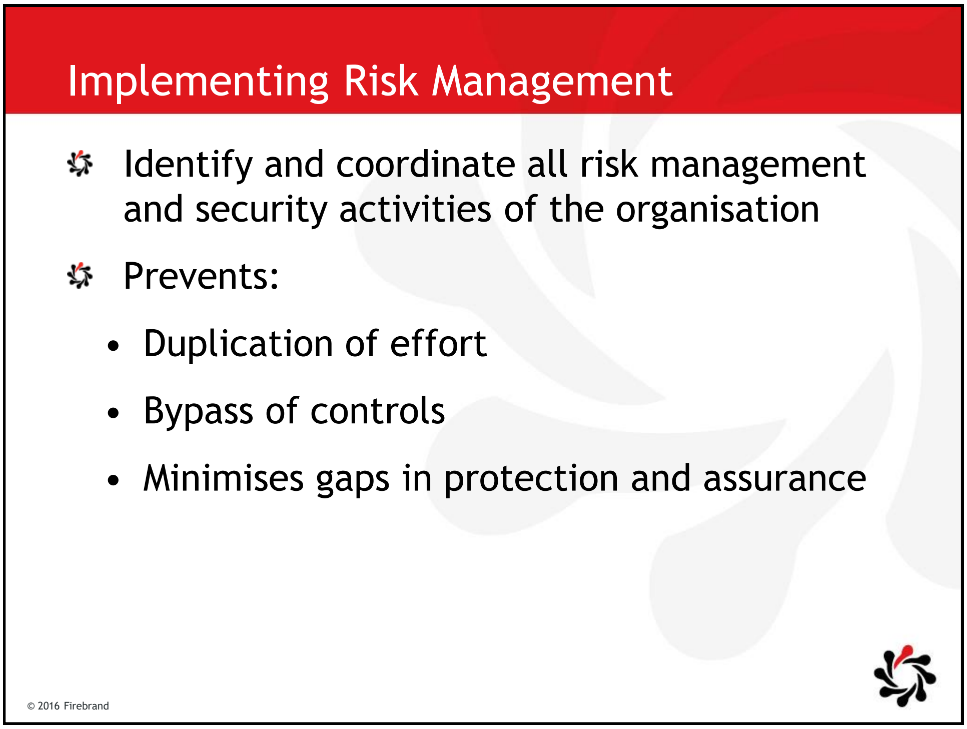
## Risk Appetite and Tolerance

- Risk appetite is what is considered by management as an acceptable level of risk
- Risk tolerance is the acceptable level of deviation from the acceptable risk level



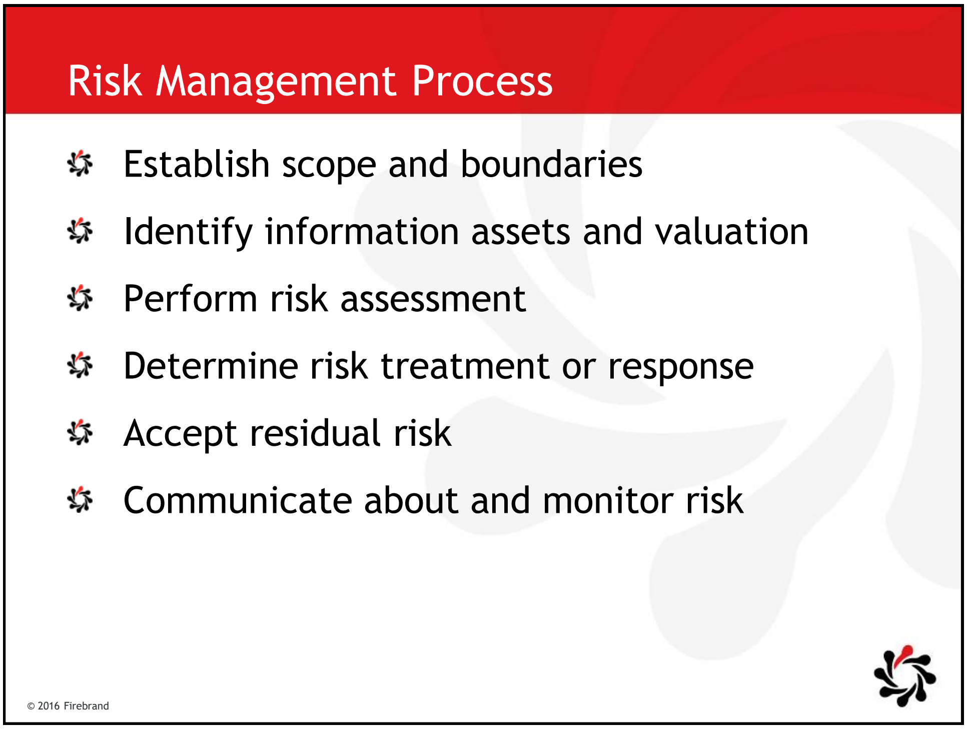
## Risk Concepts

- There is a long list of concepts on page 135 that the CISM candidate should be familiar with
- The list of technologies on page 136 will be examined in more detail later in the course



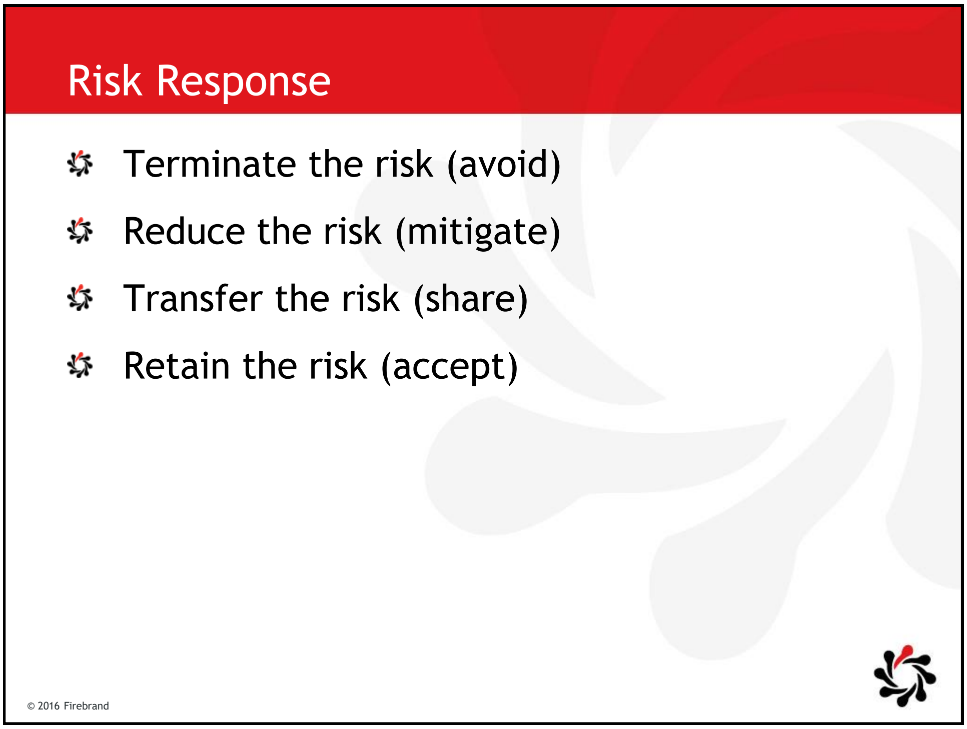
## Implementing Risk Management

- Identify and coordinate all risk management and security activities of the organisation
- Prevents:
  - Duplication of effort
  - Bypass of controls
  - Minimises gaps in protection and assurance



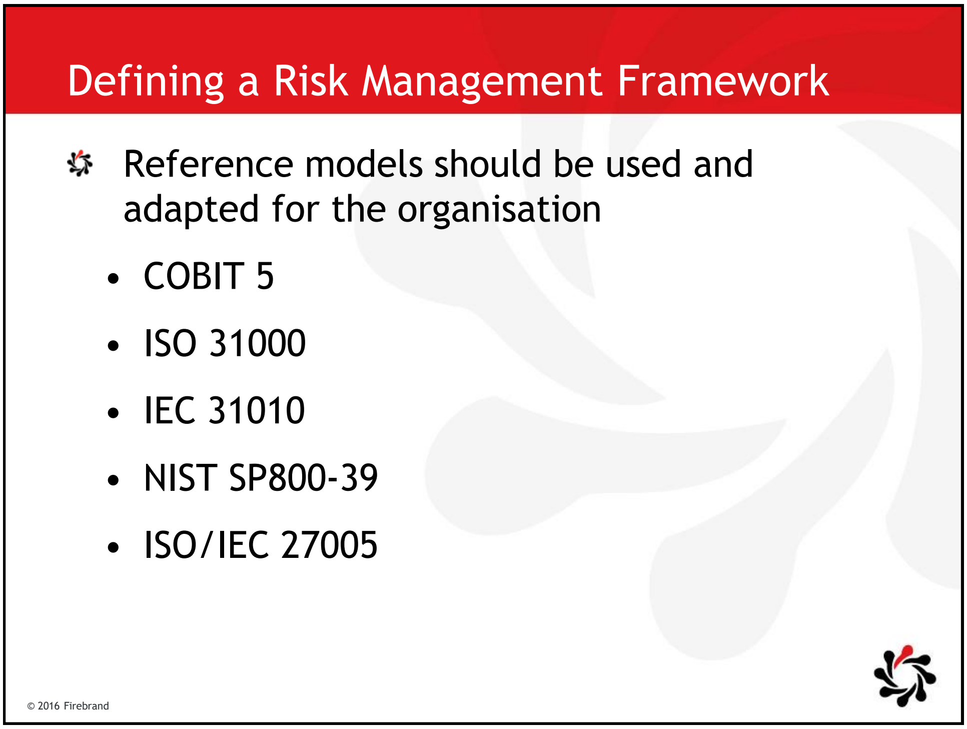
## Risk Management Process

- Establish scope and boundaries
- Identify information assets and valuation
- Perform risk assessment
- Determine risk treatment or response
- Accept residual risk
- Communicate about and monitor risk



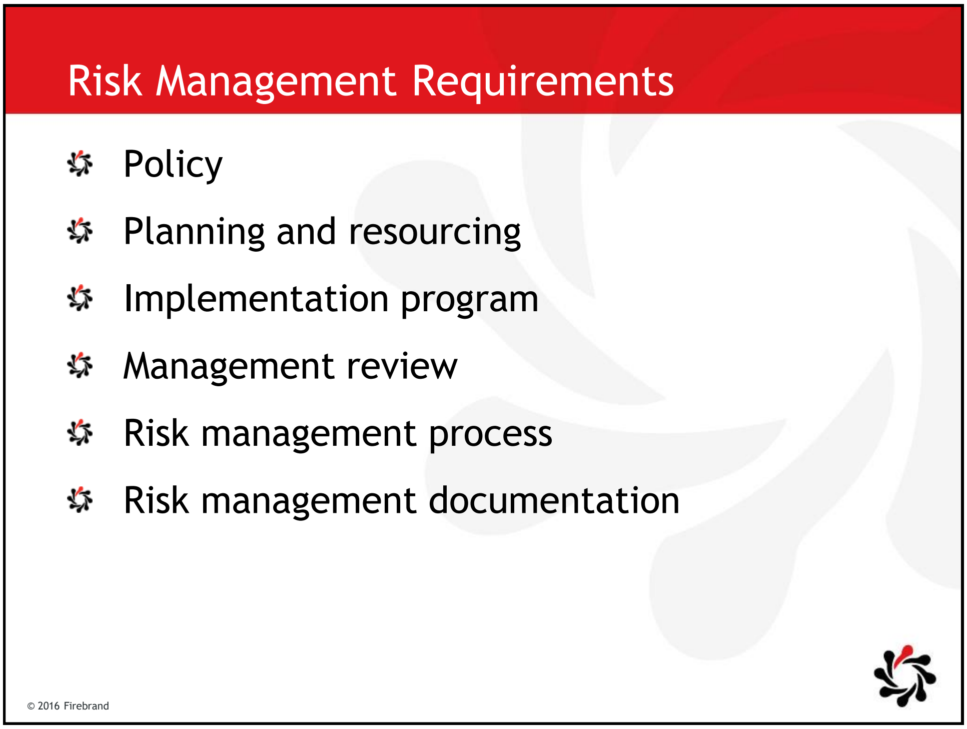
## Risk Response

- Terminate the risk (avoid)
- Reduce the risk (mitigate)
- Transfer the risk (share)
- Retain the risk (accept)



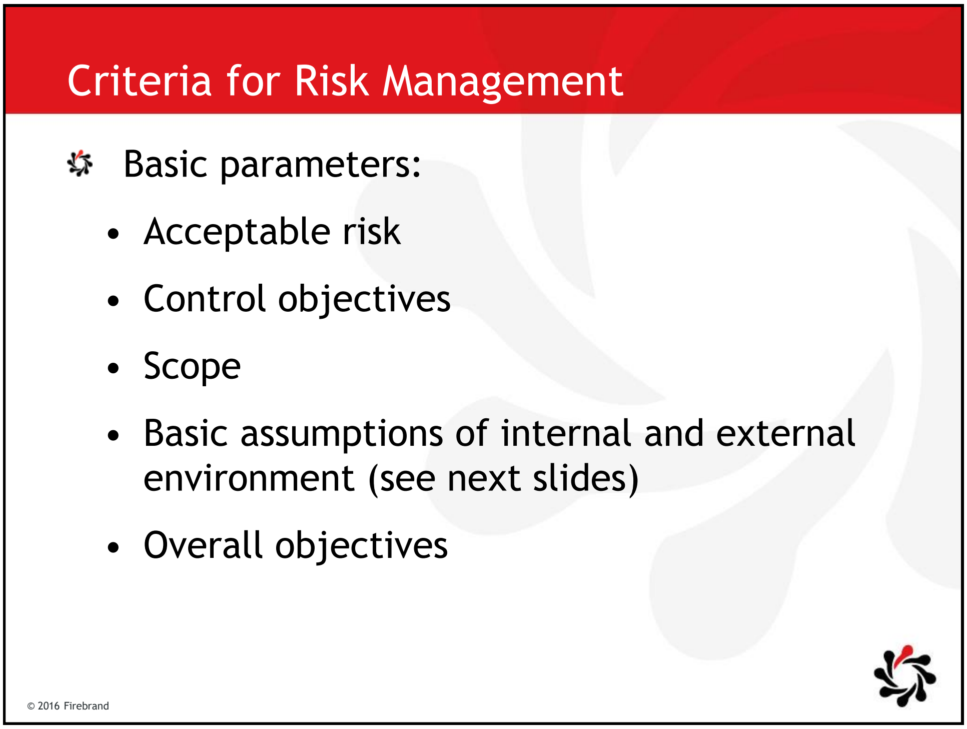
## Defining a Risk Management Framework

- Reference models should be used and adapted for the organisation
  - COBIT 5
  - ISO 31000
  - IEC 31010
  - NIST SP800-39
  - ISO/IEC 27005



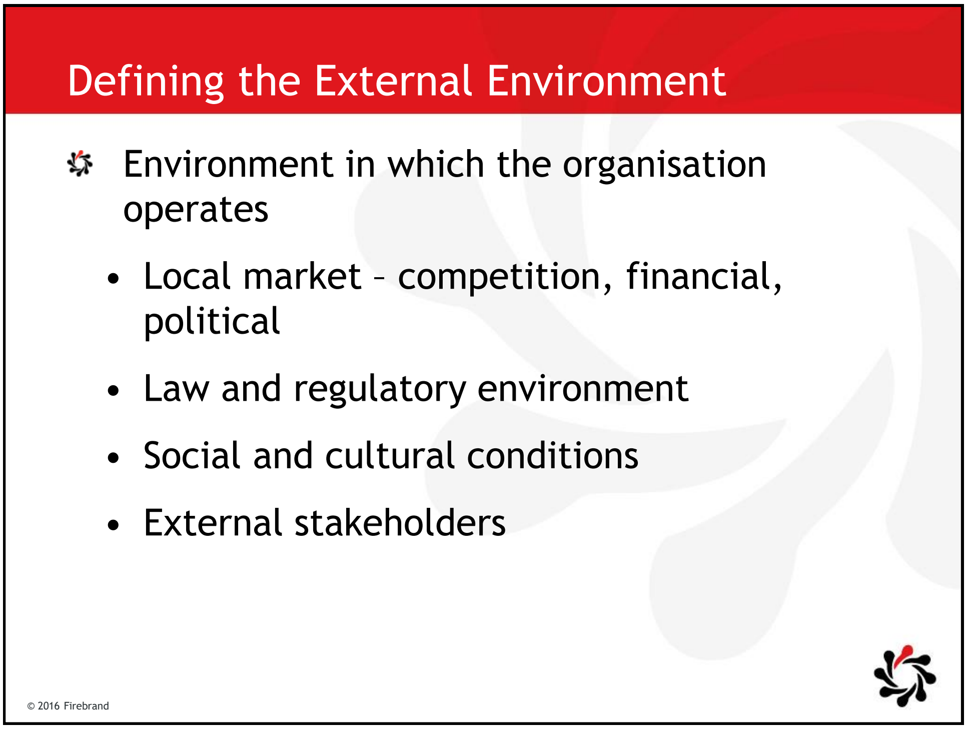
## Risk Management Requirements

- Policy
- Planning and resourcing
- Implementation program
- Management review
- Risk management process
- Risk management documentation



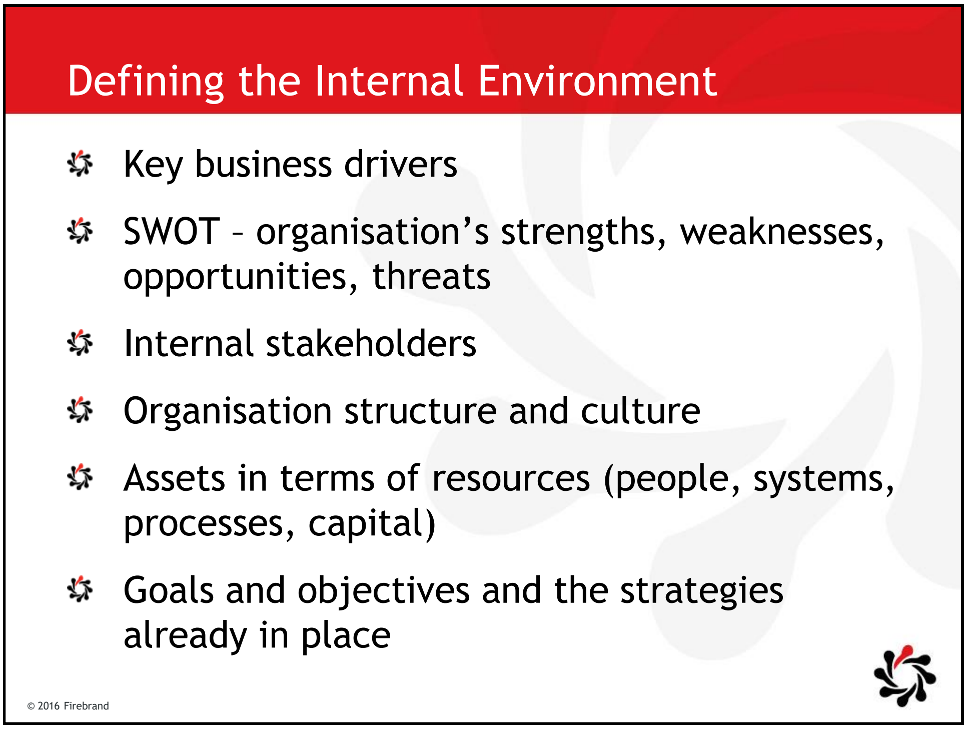
## Criteria for Risk Management

- Basic parameters:
  - Acceptable risk
  - Control objectives
  - Scope
  - Basic assumptions of internal and external environment (see next slides)
  - Overall objectives



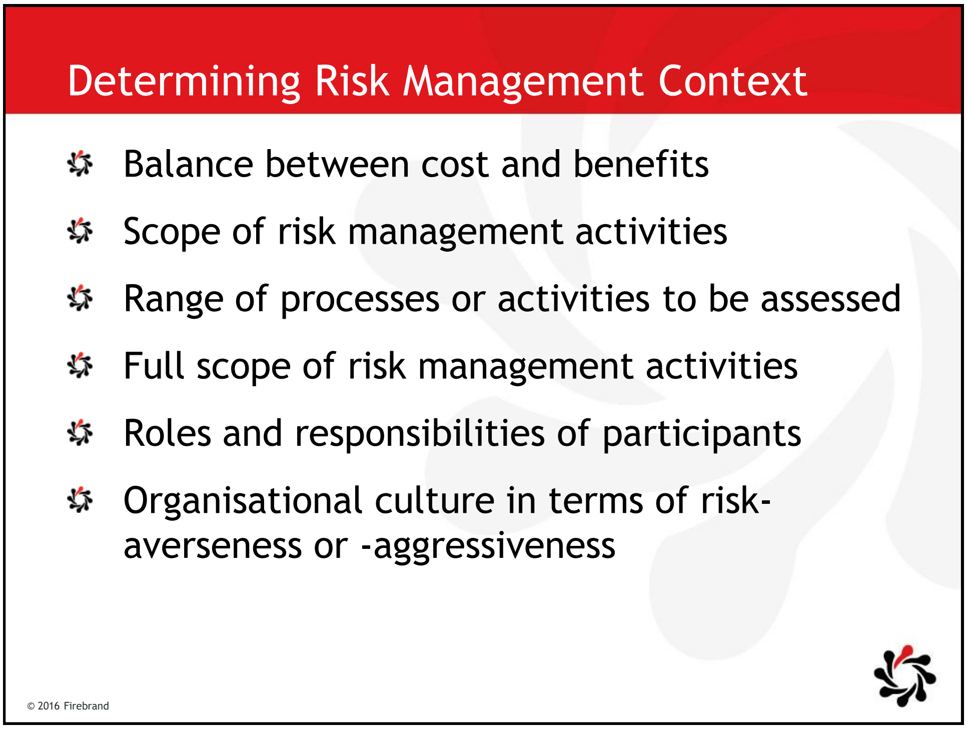
## Defining the External Environment

- Environment in which the organisation operates
  - Local market – competition, financial, political
  - Law and regulatory environment
  - Social and cultural conditions
  - External stakeholders



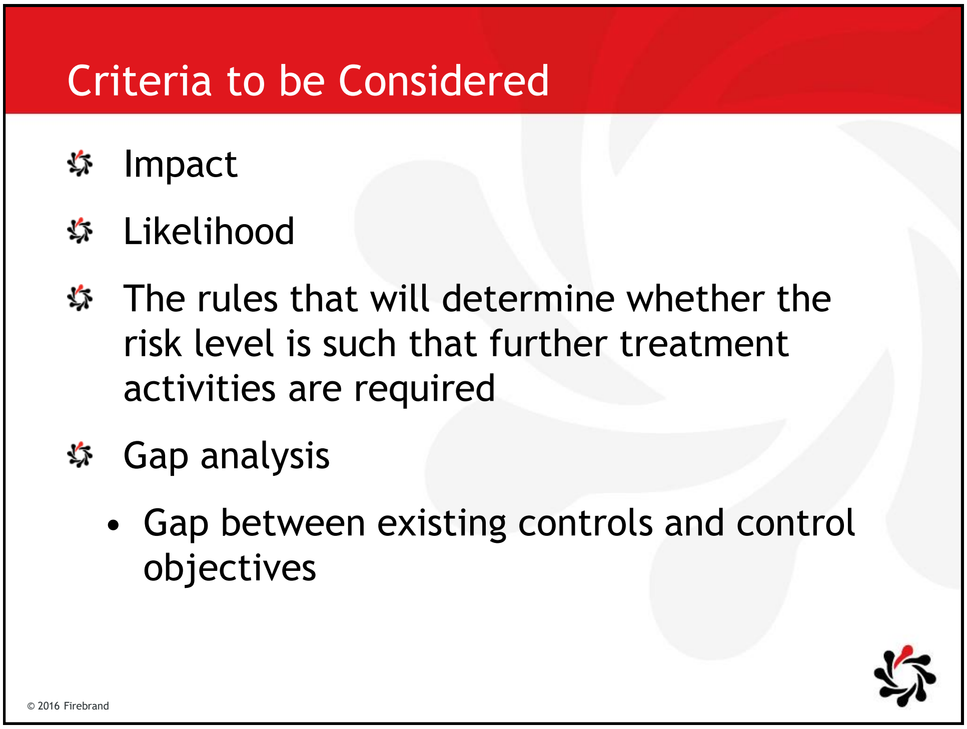
## Defining the Internal Environment

- Key business drivers
- SWOT – organisation’s strengths, weaknesses, opportunities, threats
- Internal stakeholders
- Organisation structure and culture
- Assets in terms of resources (people, systems, processes, capital)
- Goals and objectives and the strategies already in place



## Determining Risk Management Context

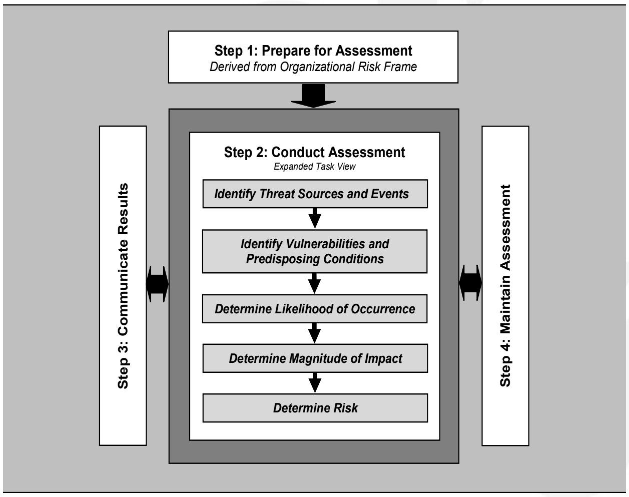
- Balance between cost and benefits
- Scope of risk management activities
- Range of processes or activities to be assessed
- Full scope of risk management activities
- Roles and responsibilities of participants
- Organisational culture in terms of risk-averseness or -aggressiveness



## Criteria to be Considered

- Impact
- Likelihood
- The rules that will determine whether the risk level is such that further treatment activities are required
- Gap analysis
  - Gap between existing controls and control objectives

# Risk Assessment and Analysis Methodologies



**Step 1: Prepare for Assessment**
*Derived from Organizational Risk Frame*

**Step 2: Conduct Assessment**
*Expanded Task View*

*Identify Threat Sources and Events*

*Identify Vulnerabilities and Predisposing Conditions*

*Determine Likelihood of Occurrence*

*Determine Magnitude of Impact*

*Determine Risk*

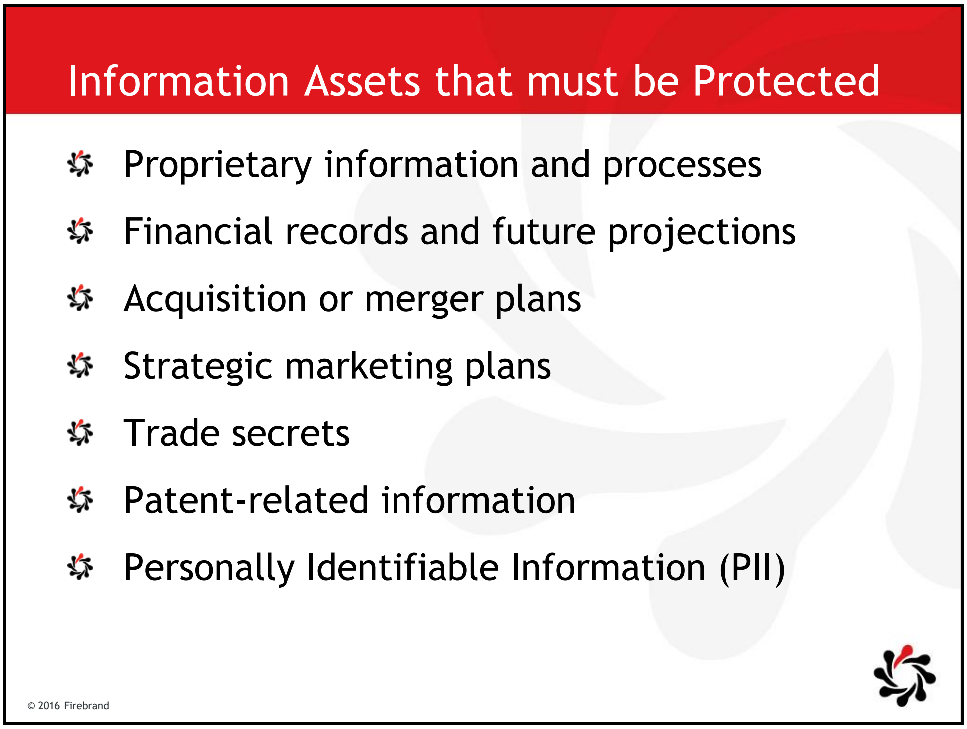
**Step 3: Communicate Results**

**Step 4: Maintain Assessment**

Courtesy of NIST - used with permission

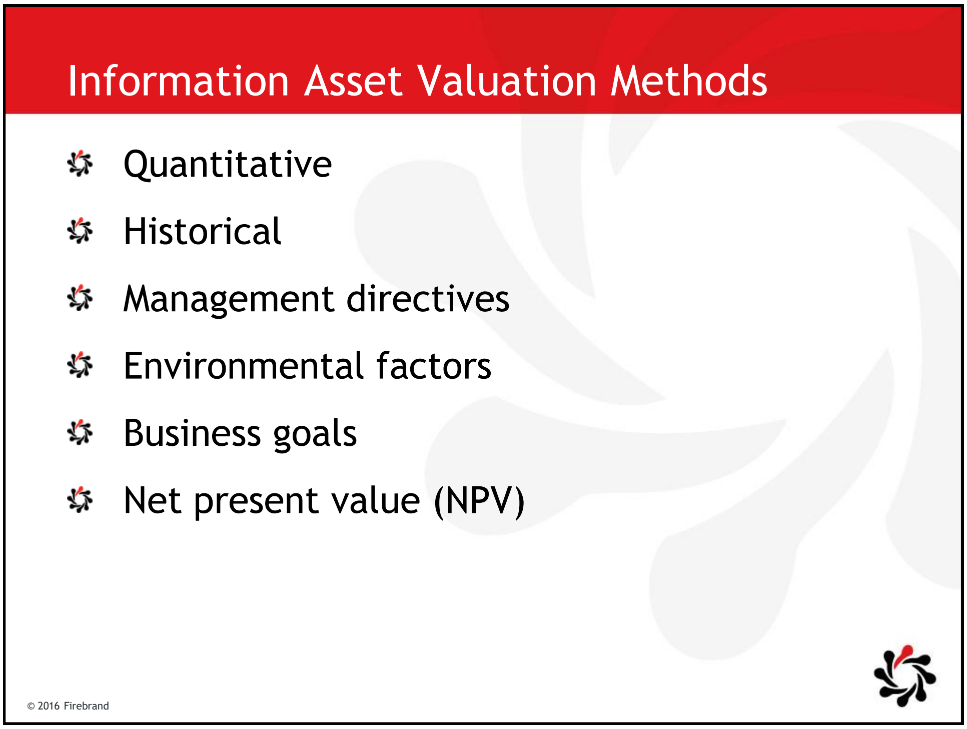
# Information Asset Identification and Valuation

- Relative value to the business
  - Criticality and/or sensitivity
- Replacement value
- Cost to restore or rebuild
- Loss of revenue
- Regulatory sanctions / contractual defaults
- Reputational damage
- Intrinsic value



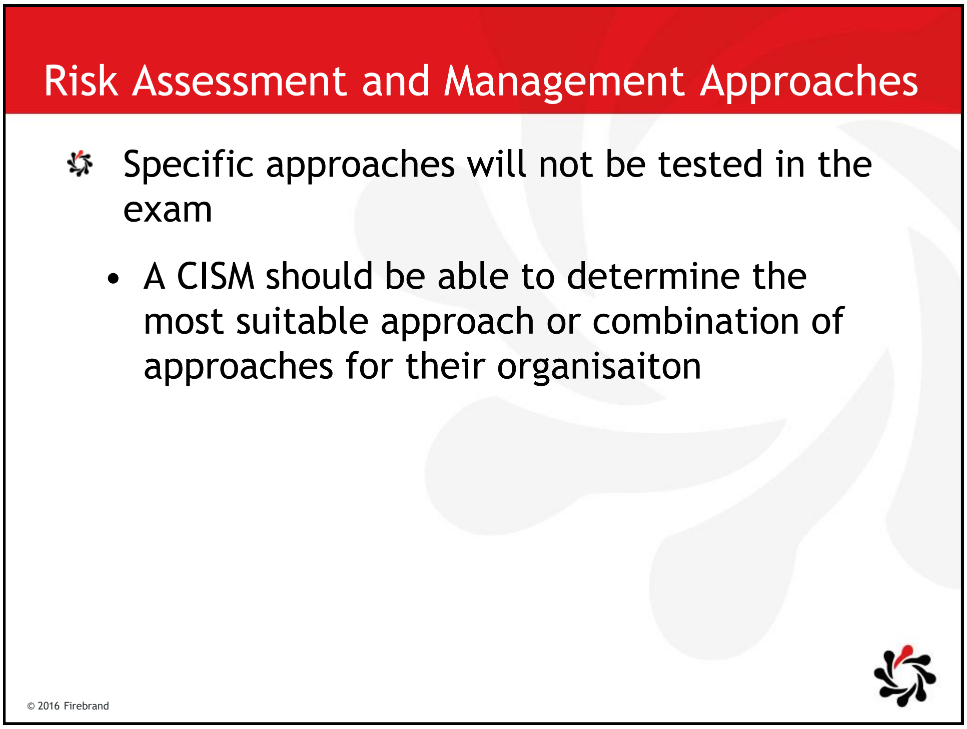
## Information Assets that must be Protected

- Proprietary information and processes
- Financial records and future projections
- Acquisition or merger plans
- Strategic marketing plans
- Trade secrets
- Patent-related information
- Personally Identifiable Information (PII)



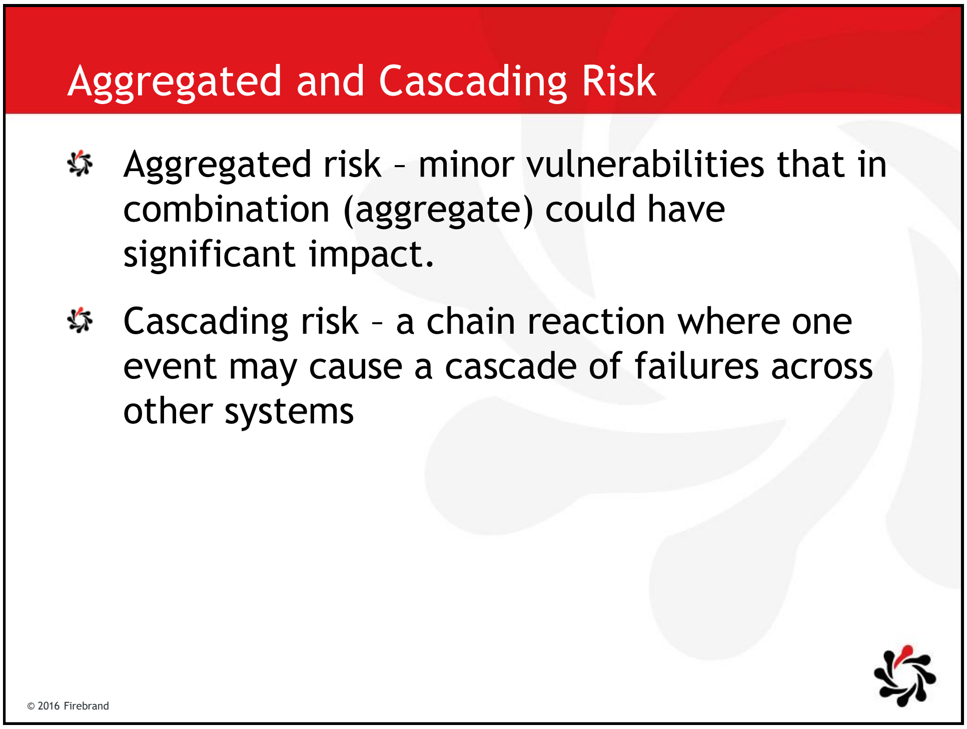
## Information Asset Valuation Methods

- Quantitative
- Historical
- Management directives
- Environmental factors
- Business goals
- Net present value (NPV)



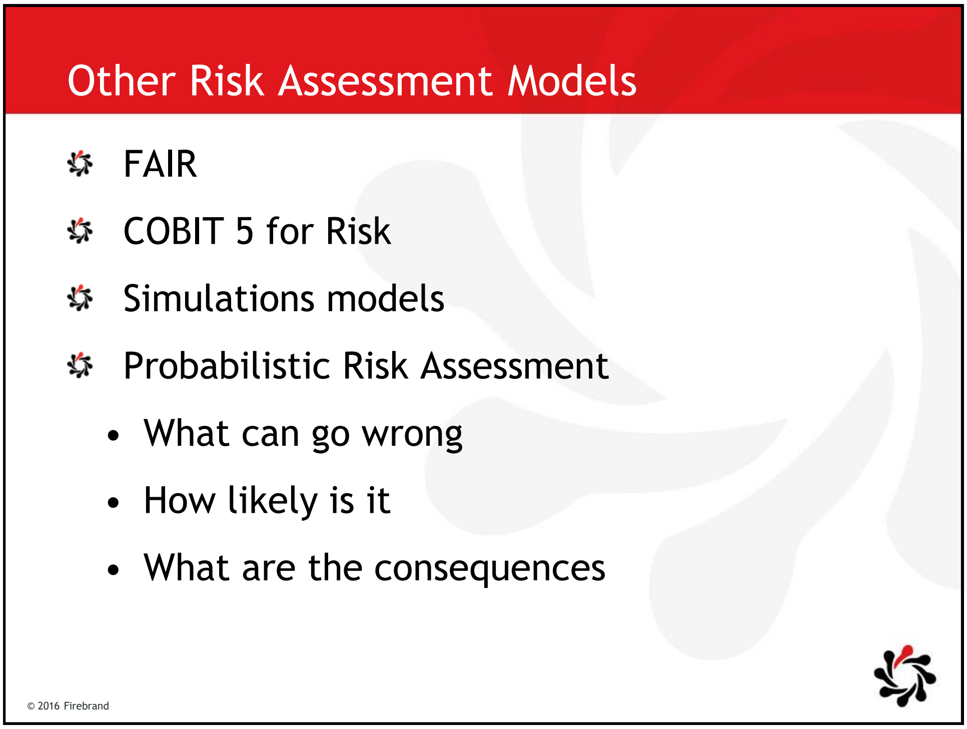
## Risk Assessment and Management Approaches

- Specific approaches will not be tested in the exam
  - A CISM should be able to determine the most suitable approach or combination of approaches for their organisaiton



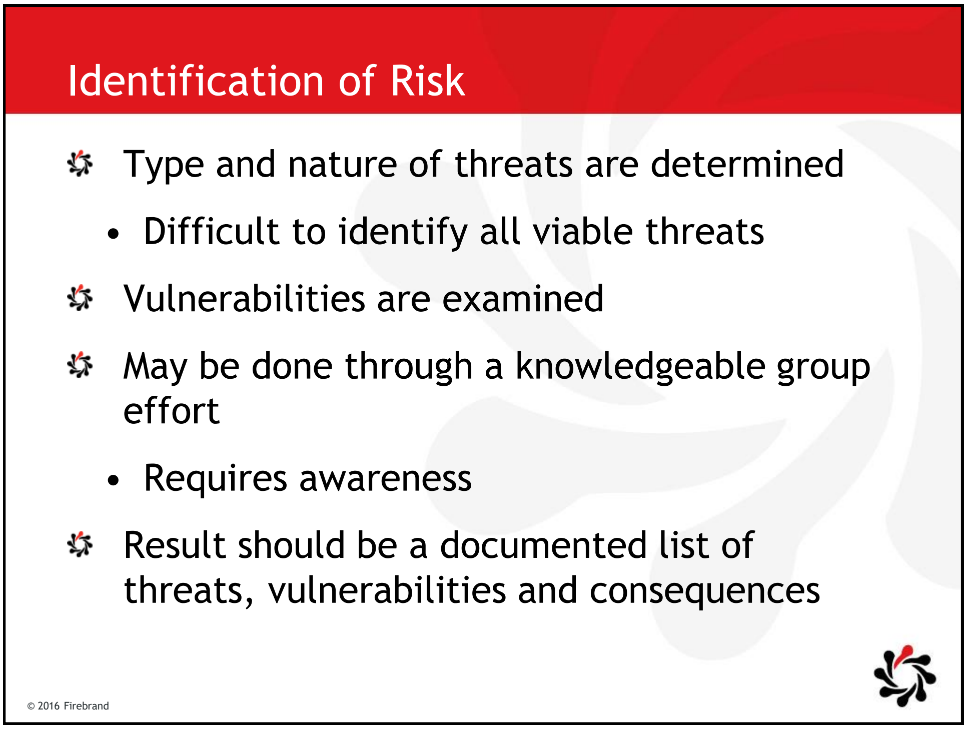
## Aggregated and Cascading Risk

- Aggregated risk – minor vulnerabilities that in combination (aggregate) could have significant impact.
- Cascading risk – a chain reaction where one event may cause a cascade of failures across other systems



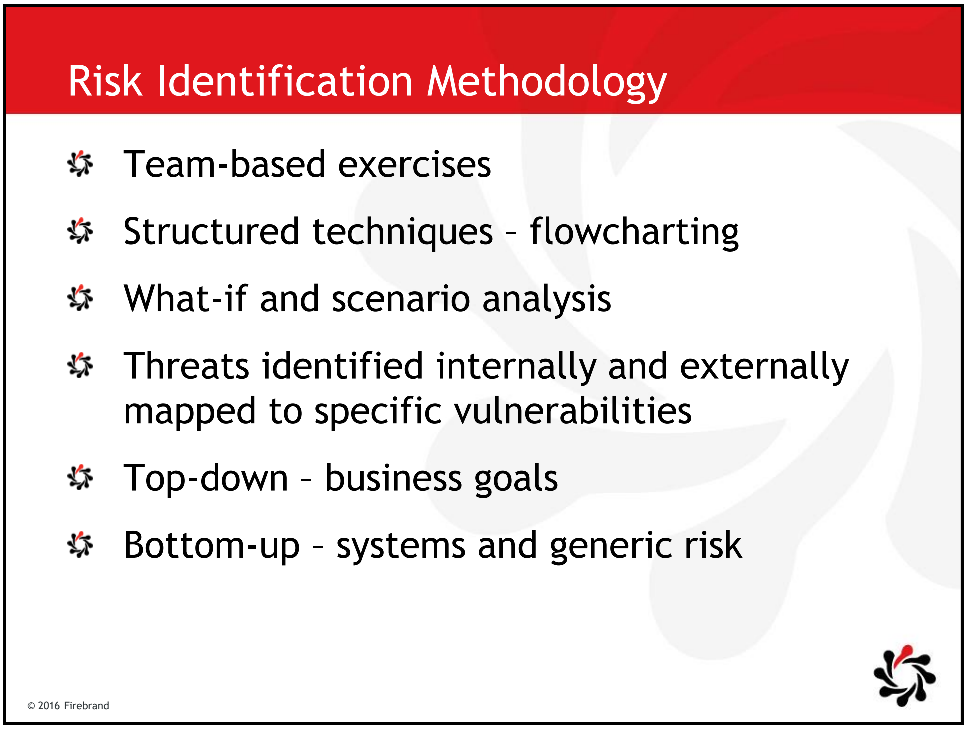
## Other Risk Assessment Models

- FAIR
- COBIT 5 for Risk
- Simulations models
- Probabilistic Risk Assessment
  - What can go wrong
  - How likely is it
  - What are the consequences



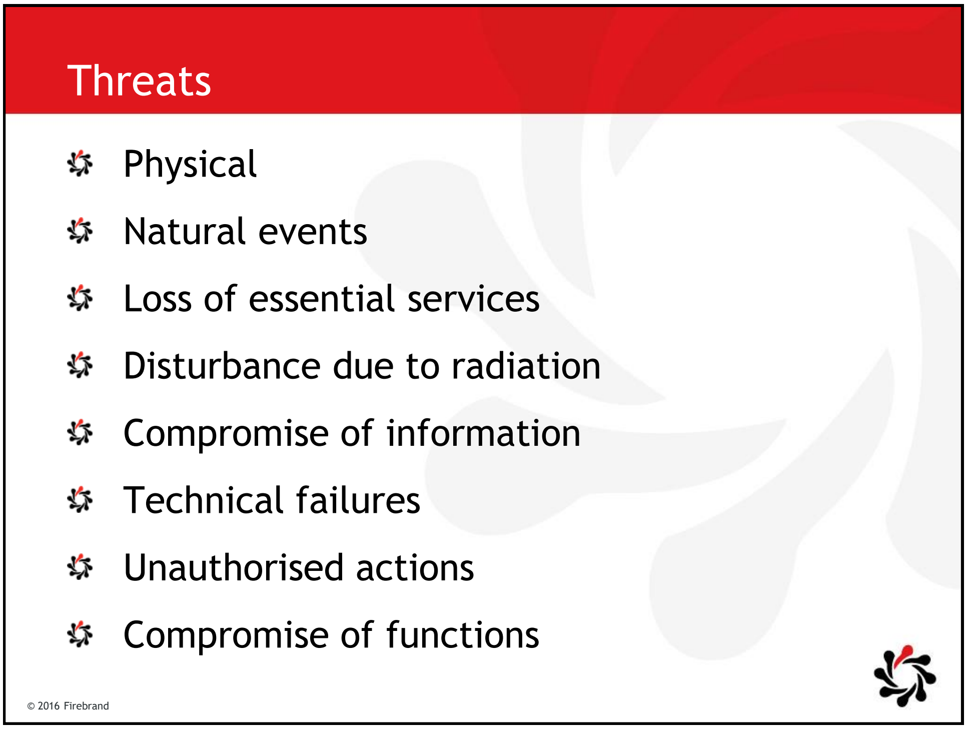
## Identification of Risk

- Type and nature of threats are determined
  - Difficult to identify all viable threats
- Vulnerabilities are examined
- May be done through a knowledgeable group effort
  - Requires awareness
- Result should be a documented list of threats, vulnerabilities and consequences



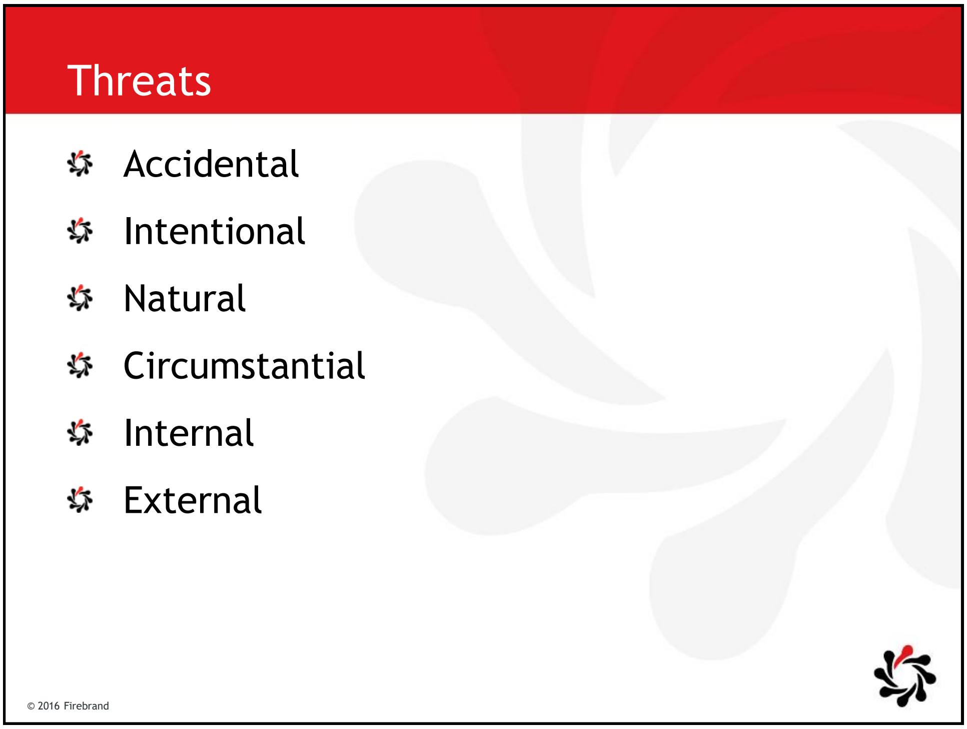
## Risk Identification Methodology

- Team-based exercises
- Structured techniques – flowcharting
- What-if and scenario analysis
- Threats identified internally and externally mapped to specific vulnerabilities
- Top-down – business goals
- Bottom-up – systems and generic risk



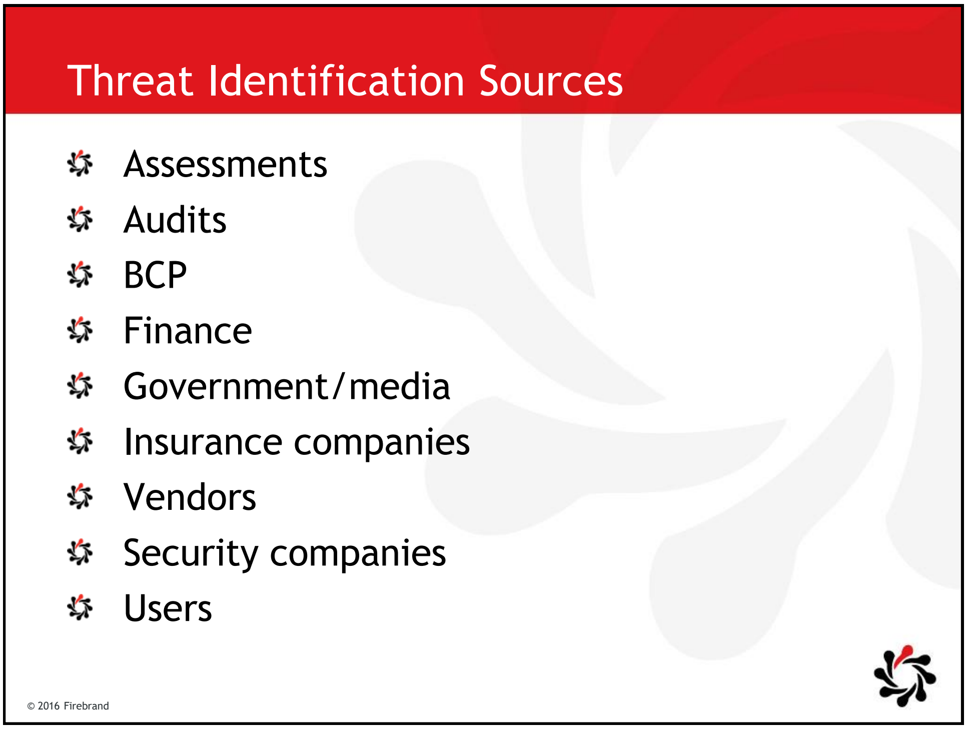
## Threats

- Physical
- Natural events
- Loss of essential services
- Disturbance due to radiation
- Compromise of information
- Technical failures
- Unauthorised actions
- Compromise of functions



## Threats

- Accidental
- Intentional
- Natural
- Circumstantial
- Internal
- External

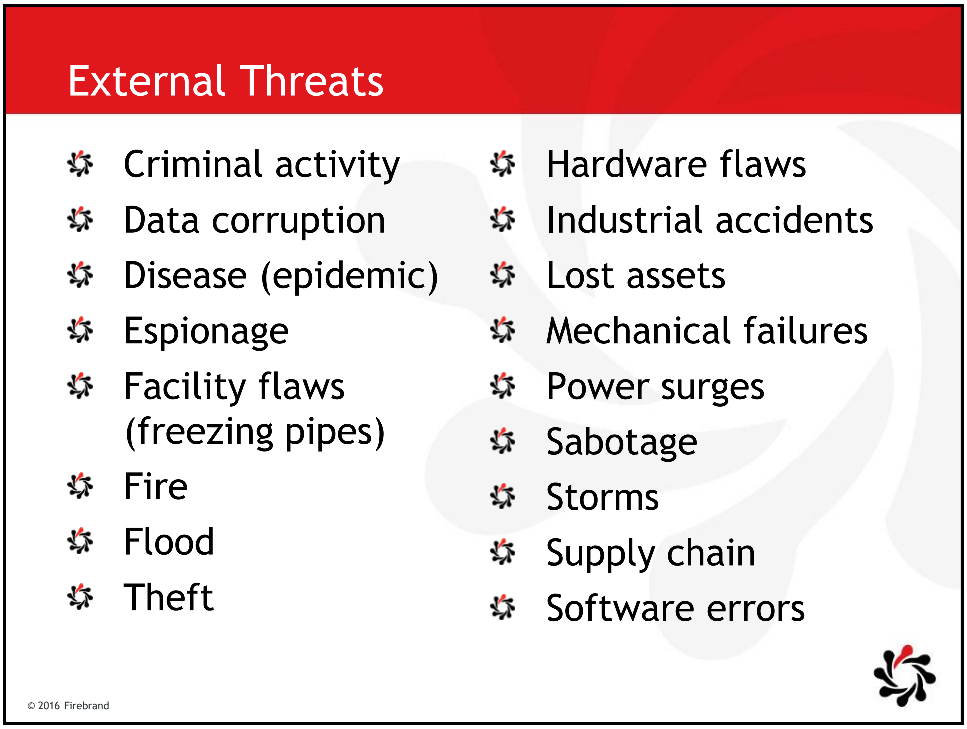


## Threat Identification Sources

- Assessments
- Audits
- BCP
- Finance
- Government/media
- Insurance companies
- Vendors
- Security companies
- Users

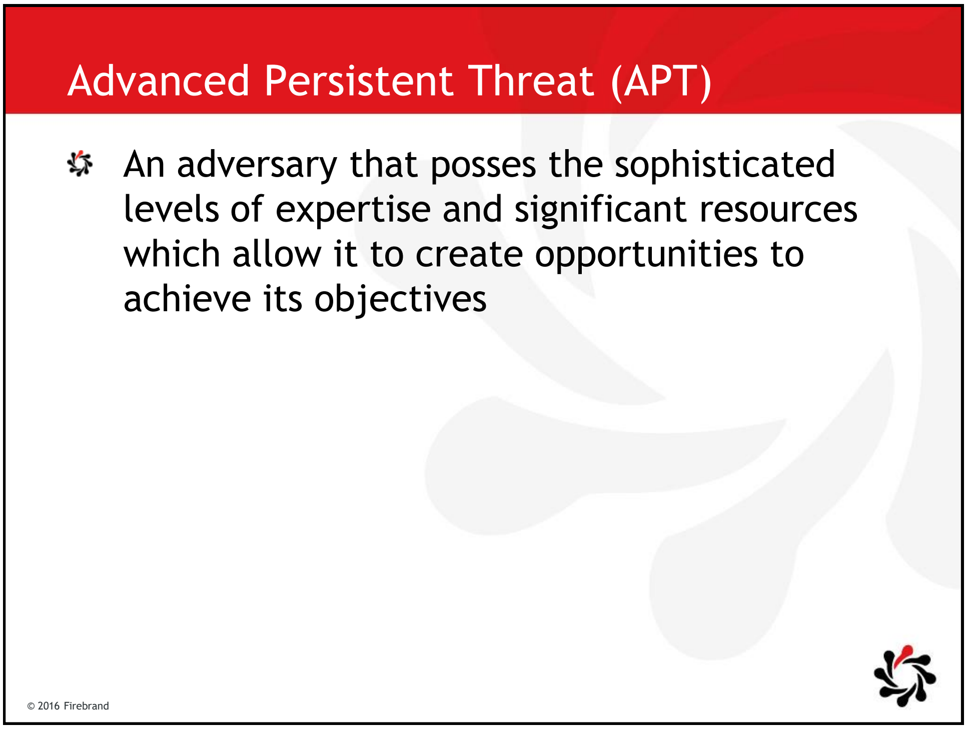
## Internal Threats

- Employees
  - Unhappy
  - Loss of key staff
  - Pressure to perform
  - Excessive access rights
- Contractors or ex-employees



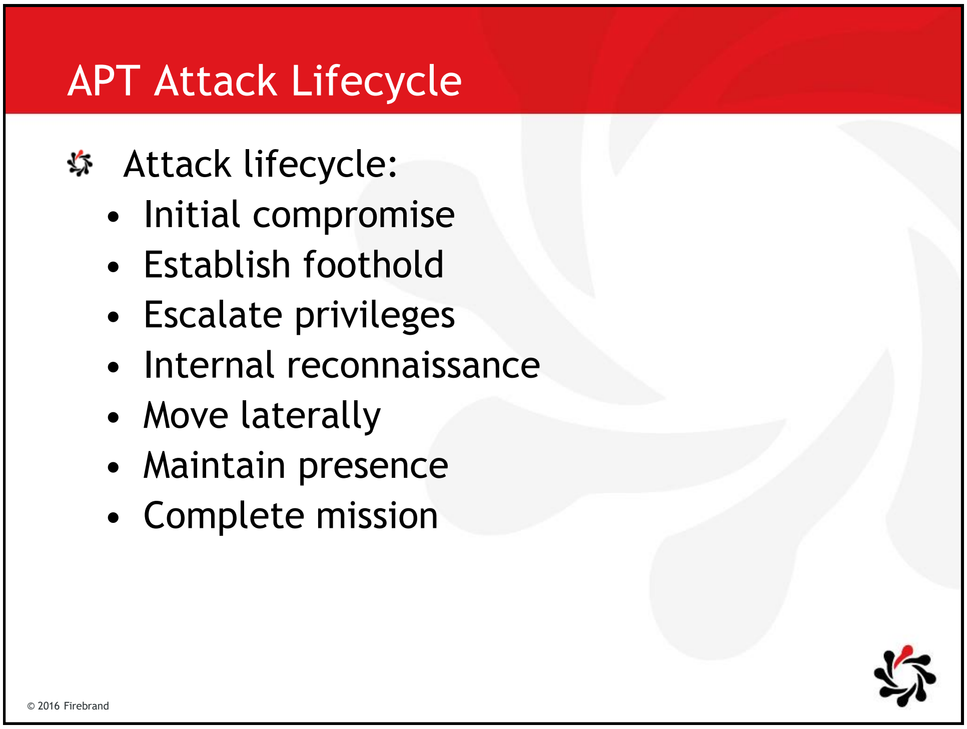
## External Threats

- Criminal activity
- Data corruption
- Disease (epidemic)
- Espionage
- Facility flaws (freezing pipes)
- Fire
- Flood
- Theft
- Hardware flaws
- Industrial accidents
- Lost assets
- Mechanical failures
- Power surges
- Sabotage
- Storms
- Supply chain
- Software errors



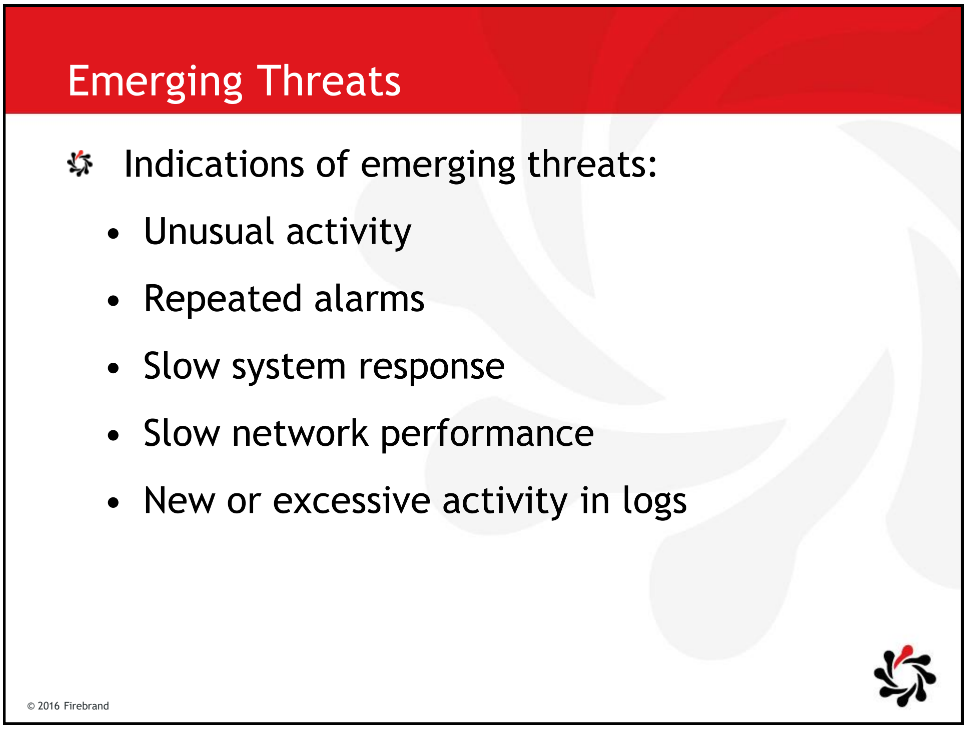
## Advanced Persistent Threat (APT)

- An adversary that posses the sophisticated levels of expertise and significant resources which allow it to create opportunities to achieve its objectives



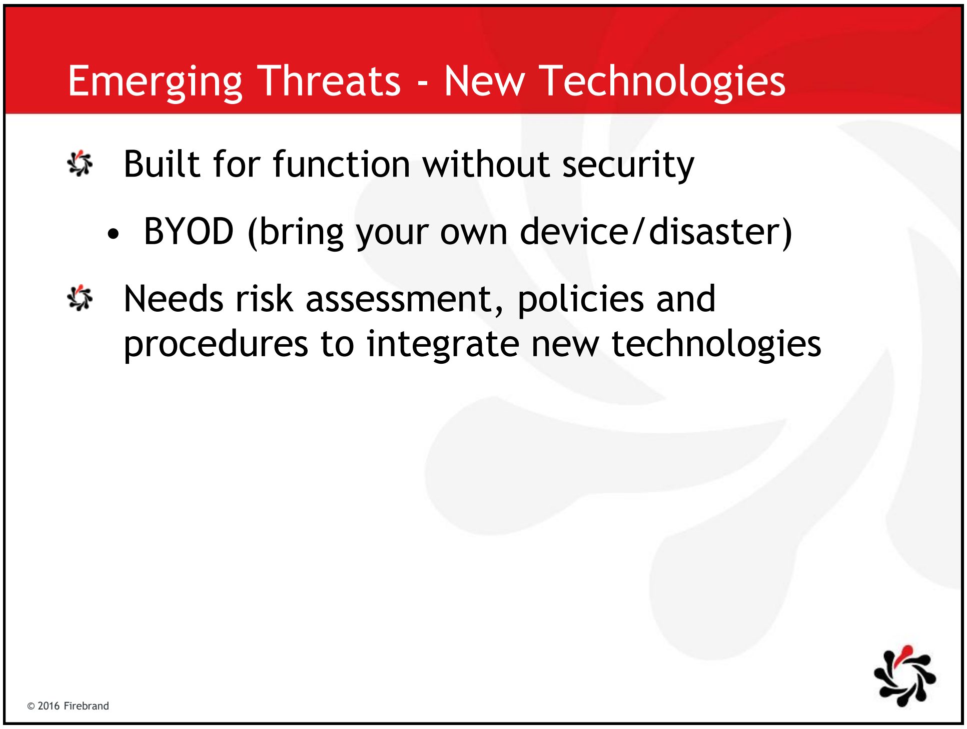
## APT Attack Lifecycle

- Attack lifecycle:
  - Initial compromise
  - Establish foothold
  - Escalate privileges
  - Internal reconnaissance
  - Move laterally
  - Maintain presence
  - Complete mission



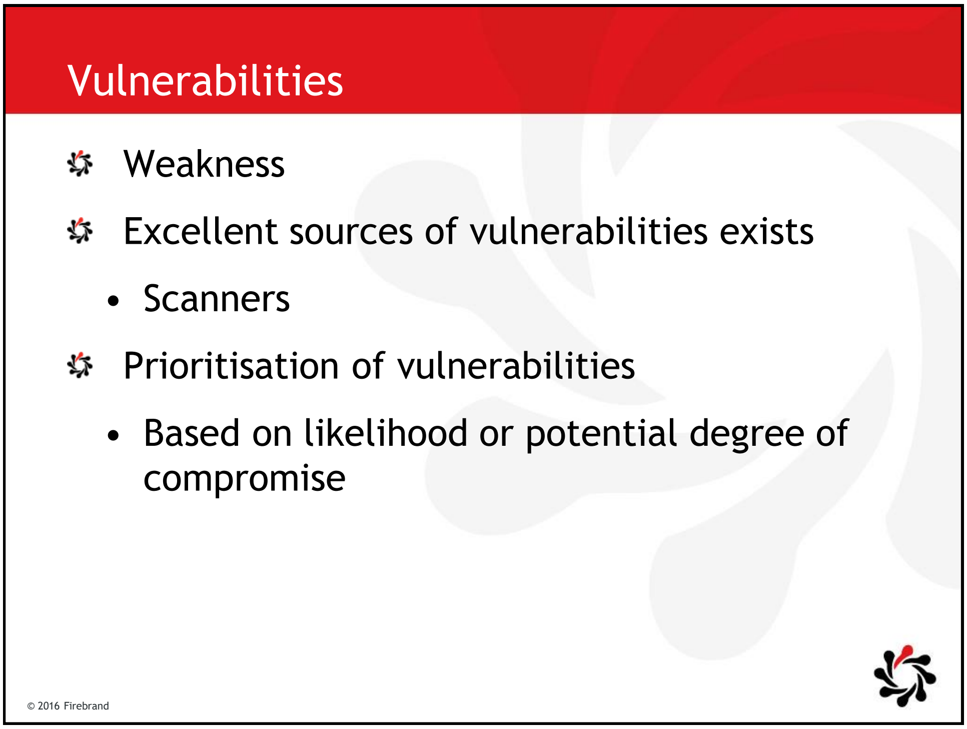
## Emerging Threats

- Indications of emerging threats:
  - Unusual activity
  - Repeated alarms
  - Slow system response
  - Slow network performance
  - New or excessive activity in logs



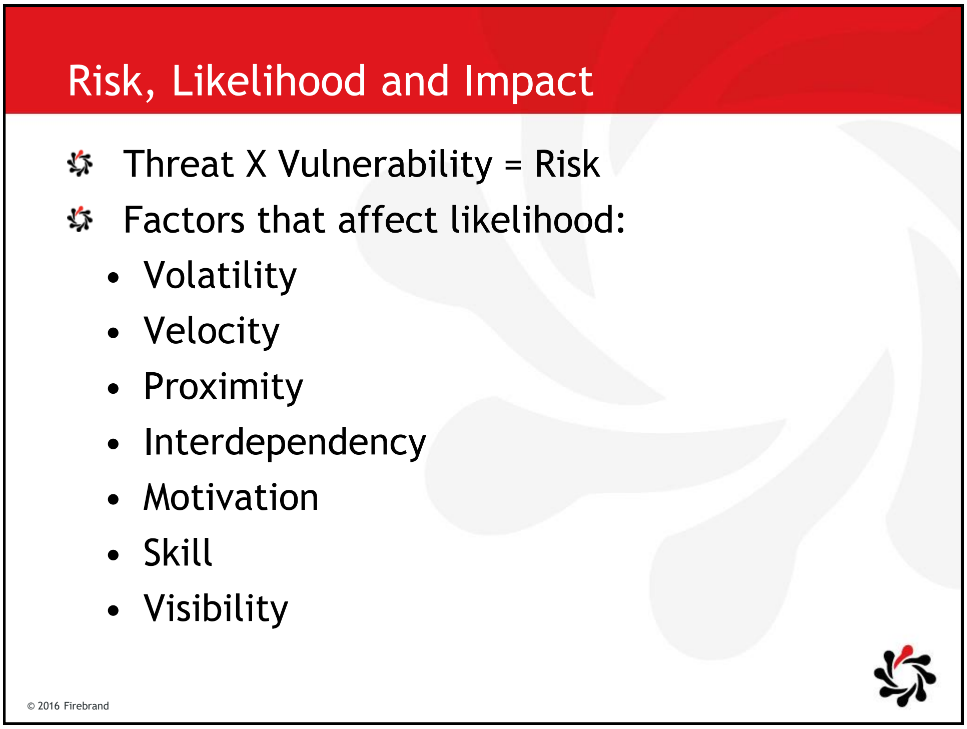
## Emerging Threats - New Technologies

- Built for function without security
  - BYOD (bring your own device/disaster)
- Needs risk assessment, policies and procedures to integrate new technologies



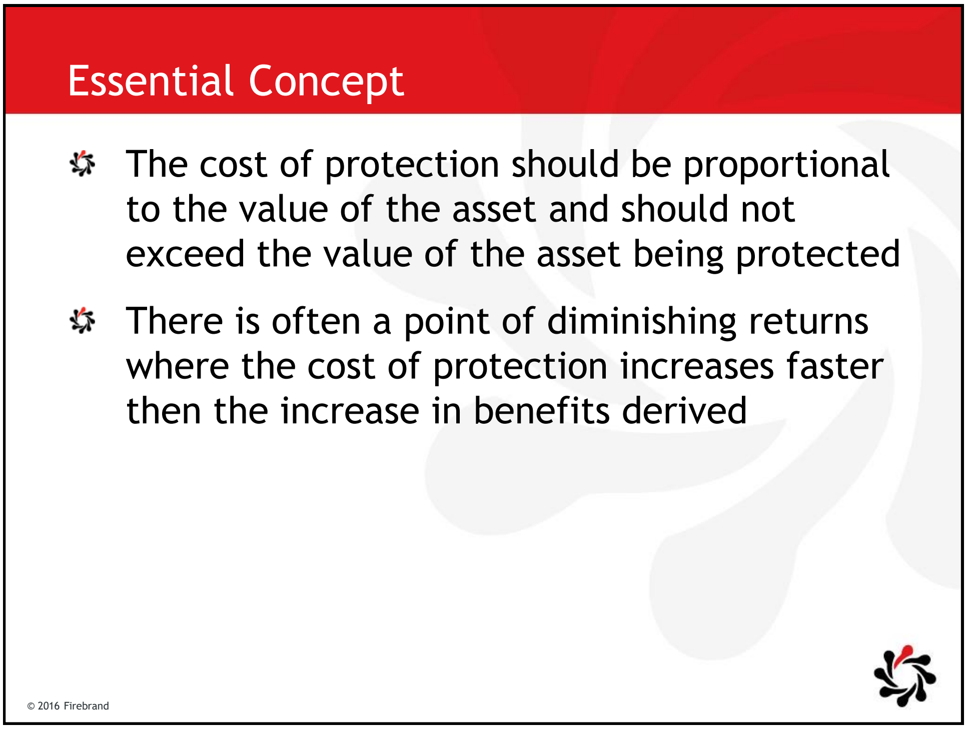
## Vulnerabilities

- Weakness
- Excellent sources of vulnerabilities exists
  - Scanners
- Prioritisation of vulnerabilities
  - Based on likelihood or potential degree of compromise



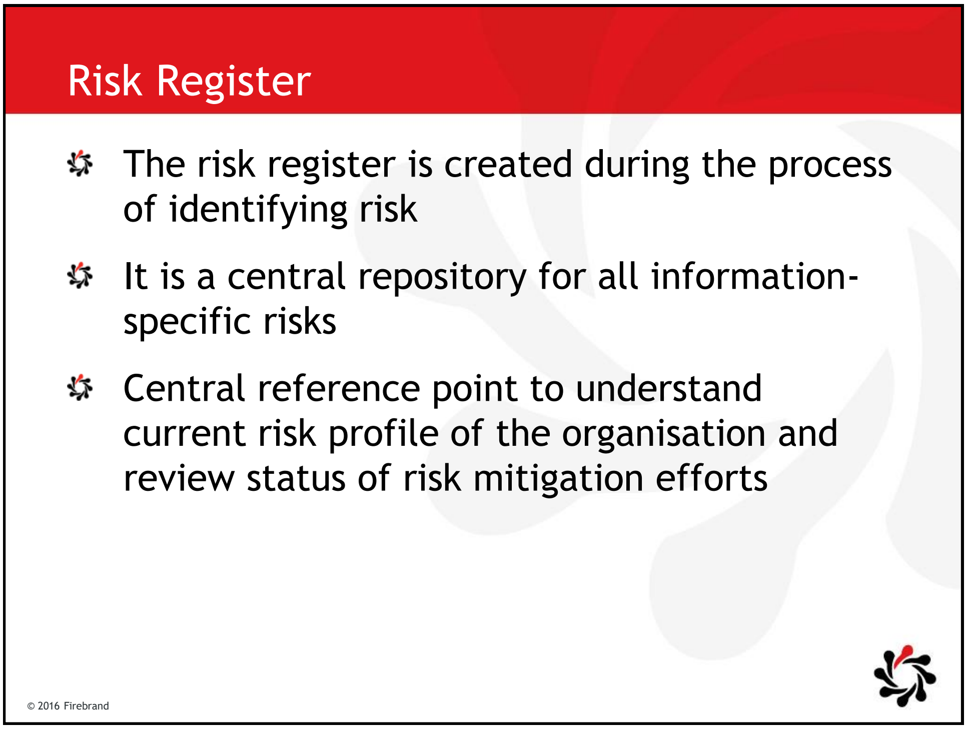
## Risk, Likelihood and Impact

- Threat X Vulnerability = Risk
- Factors that affect likelihood:
  - Volatility
  - Velocity
  - Proximity
  - Interdependency
  - Motivation
  - Skill
  - Visibility



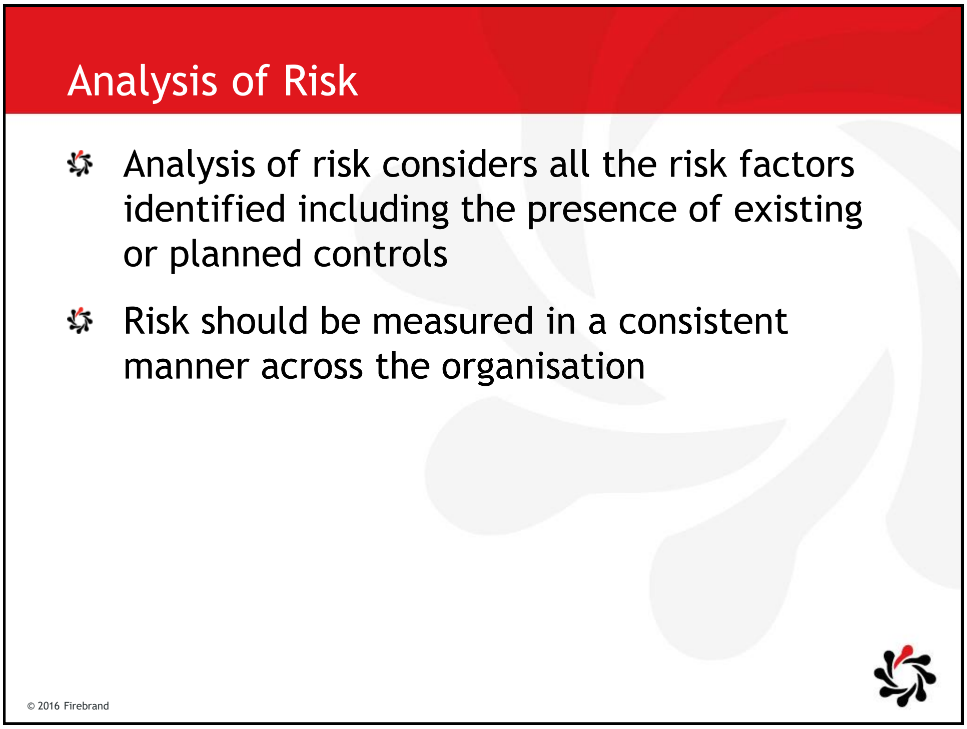
## Essential Concept

- The cost of protection should be proportional to the value of the asset and should not exceed the value of the asset being protected
- There is often a point of diminishing returns where the cost of protection increases faster then the increase in benefits derived



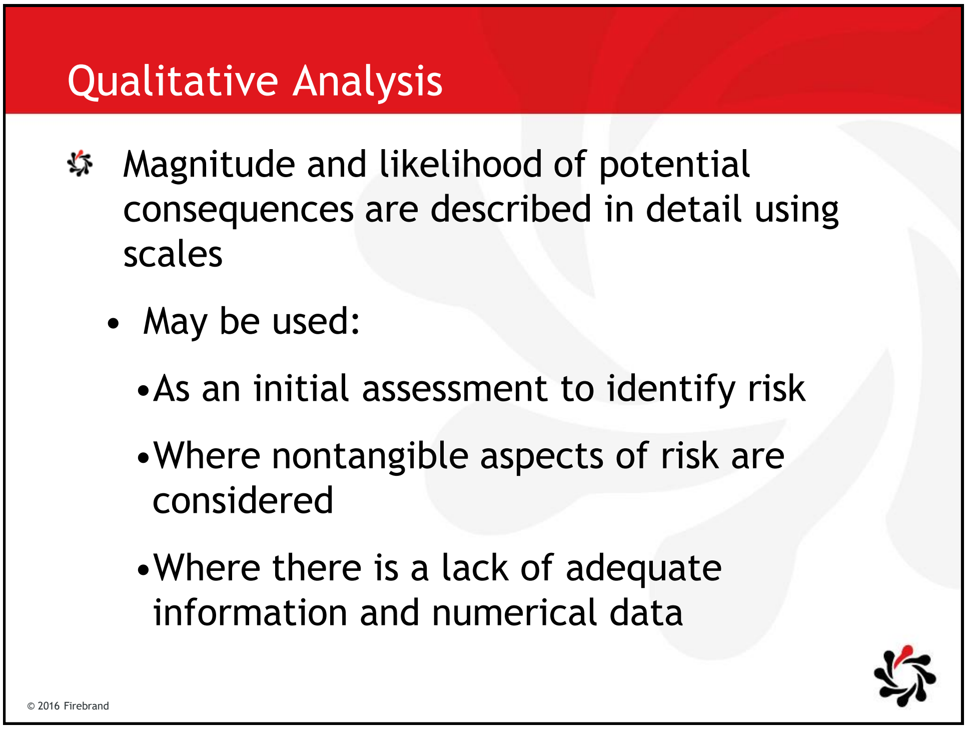
## Risk Register

- The risk register is created during the process of identifying risk
- It is a central repository for all information-specific risks
- Central reference point to understand current risk profile of the organisation and review status of risk mitigation efforts



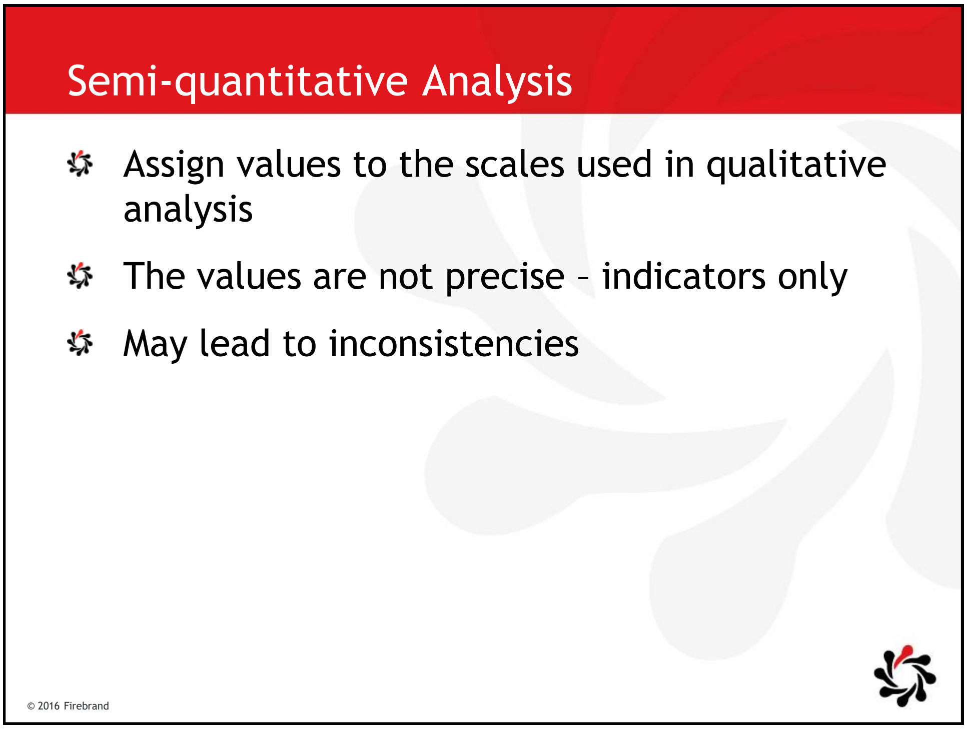
## Analysis of Risk

- Analysis of risk considers all the risk factors identified including the presence of existing or planned controls
- Risk should be measured in a consistent manner across the organisation



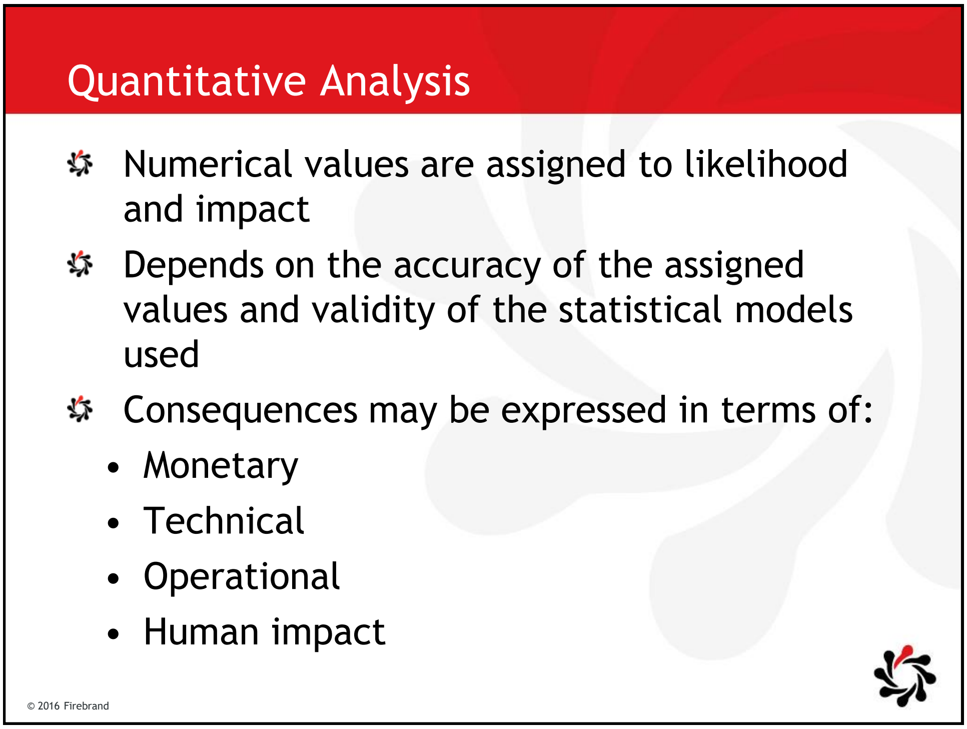
## Qualitative Analysis

- Magnitude and likelihood of potential consequences are described in detail using scales
  - May be used:
    - As an initial assessment to identify risk
    - Where nontangible aspects of risk are considered
    - Where there is a lack of adequate information and numerical data



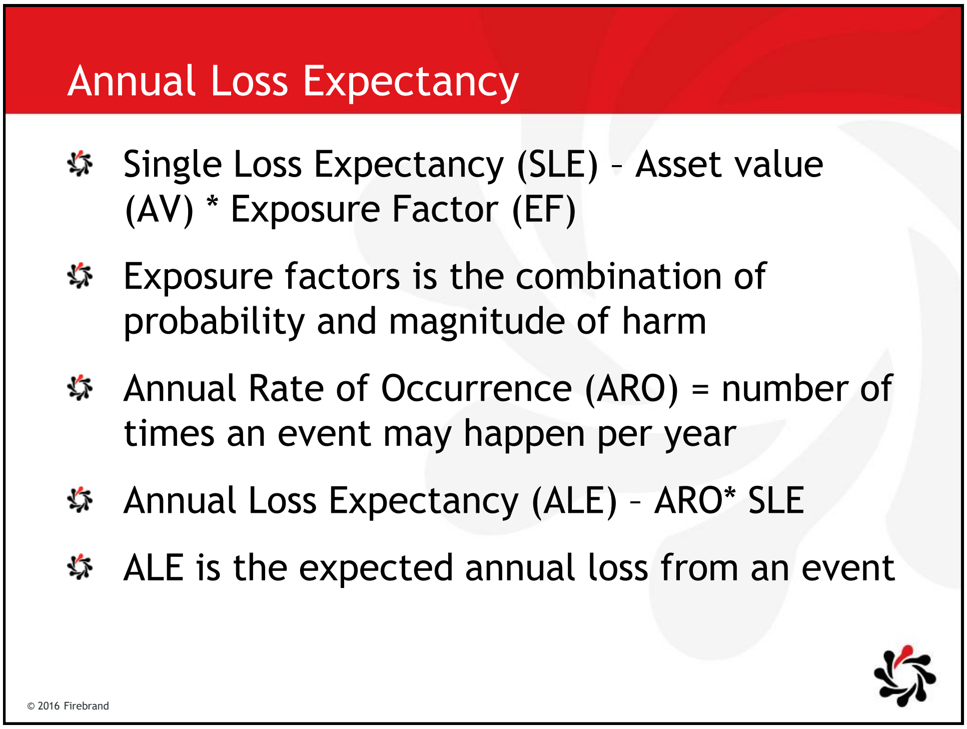
## Semi-quantitative Analysis

- Assign values to the scales used in qualitative analysis
- The values are not precise – indicators only
- May lead to inconsistencies



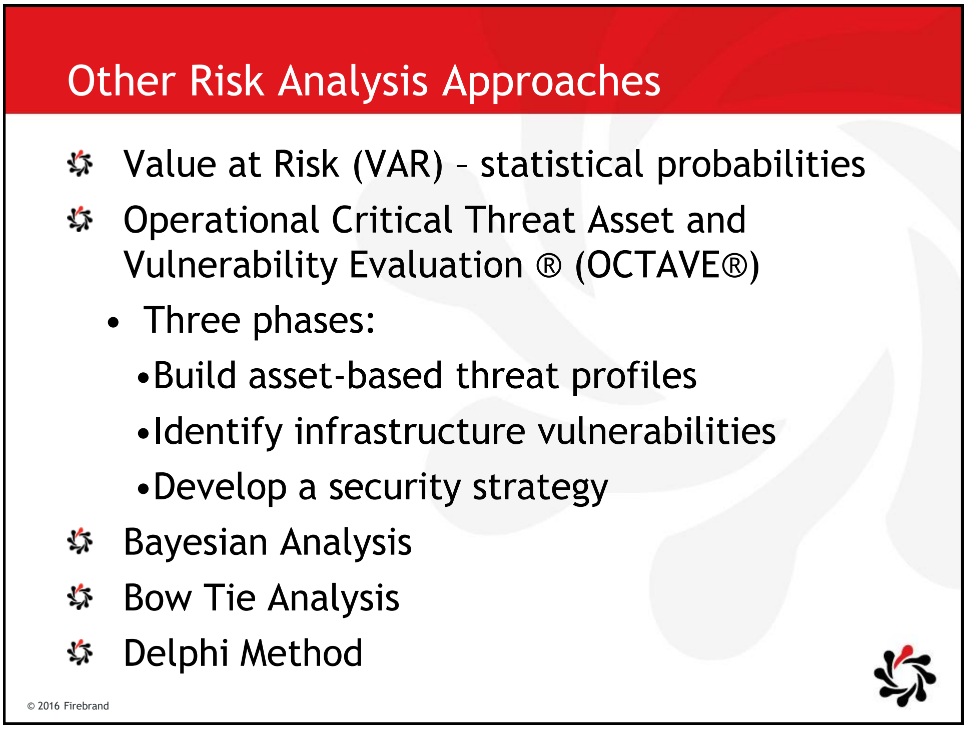
## Quantitative Analysis

- Numerical values are assigned to likelihood and impact
- Depends on the accuracy of the assigned values and validity of the statistical models used
- Consequences may be expressed in terms of:
  - Monetary
  - Technical
  - Operational
  - Human impact



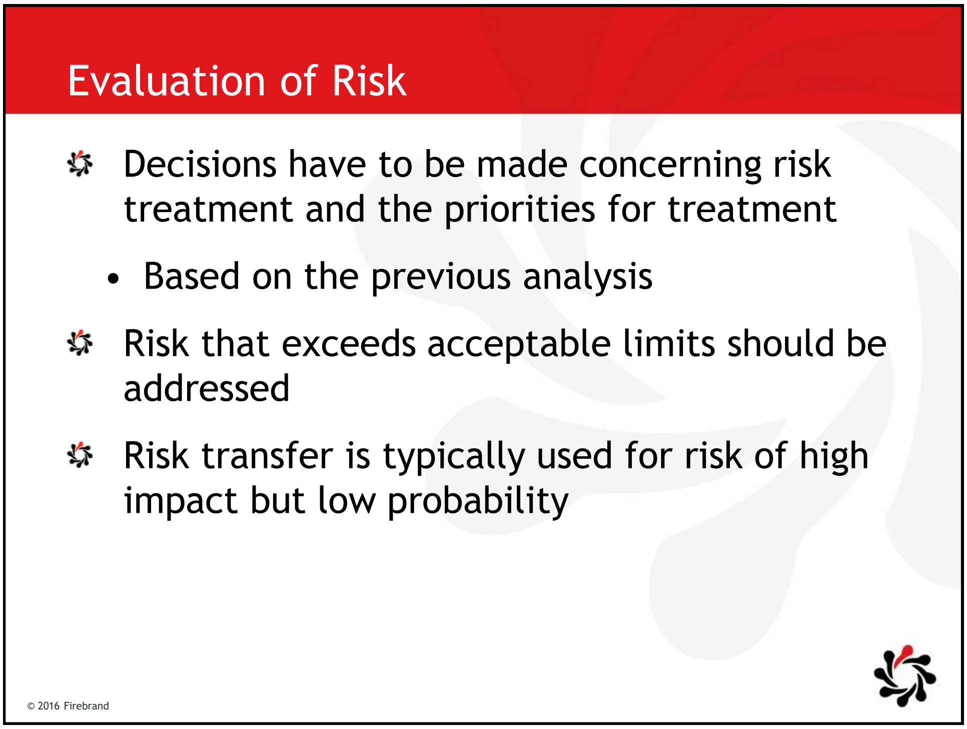
## Annual Loss Expectancy

- Single Loss Expectancy (SLE) – Asset value (AV) * Exposure Factor (EF)
- Exposure factors is the combination of probability and magnitude of harm
- Annual Rate of Occurrence (ARO) = number of times an event may happen per year
- Annual Loss Expectancy (ALE) – ARO* SLE
- ALE is the expected annual loss from an event



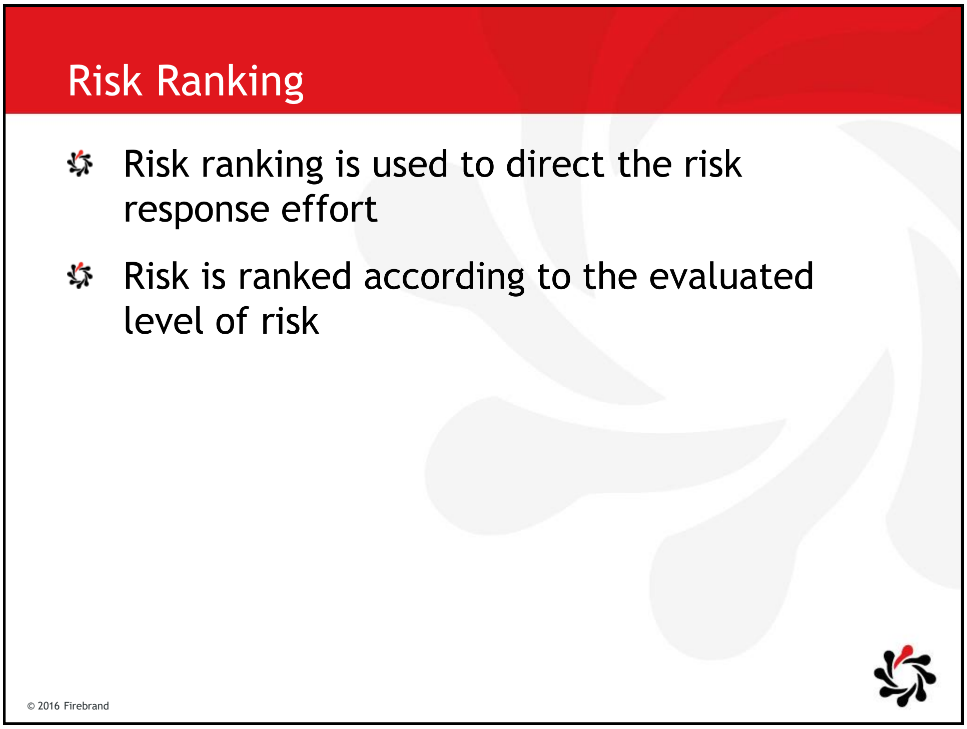
## Other Risk Analysis Approaches

- Value at Risk (VAR) – statistical probabilities
- Operational Critical Threat Asset and Vulnerability Evaluation ® (OCTAVE®)
  - Three phases:
    - Build asset-based threat profiles
    - Identify infrastructure vulnerabilities
    - Develop a security strategy
- Bayesian Analysis
- Bow Tie Analysis
- Delphi Method



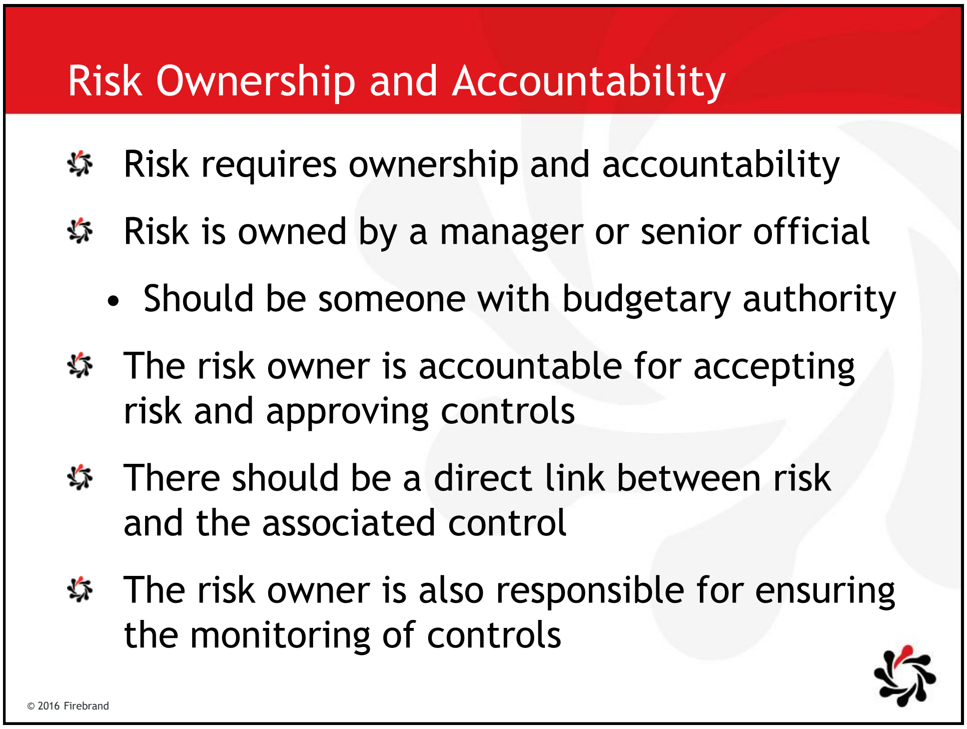
## Evaluation of Risk

- Decisions have to be made concerning risk treatment and the priorities for treatment
  - Based on the previous analysis
- Risk that exceeds acceptable limits should be addressed
- Risk transfer is typically used for risk of high impact but low probability



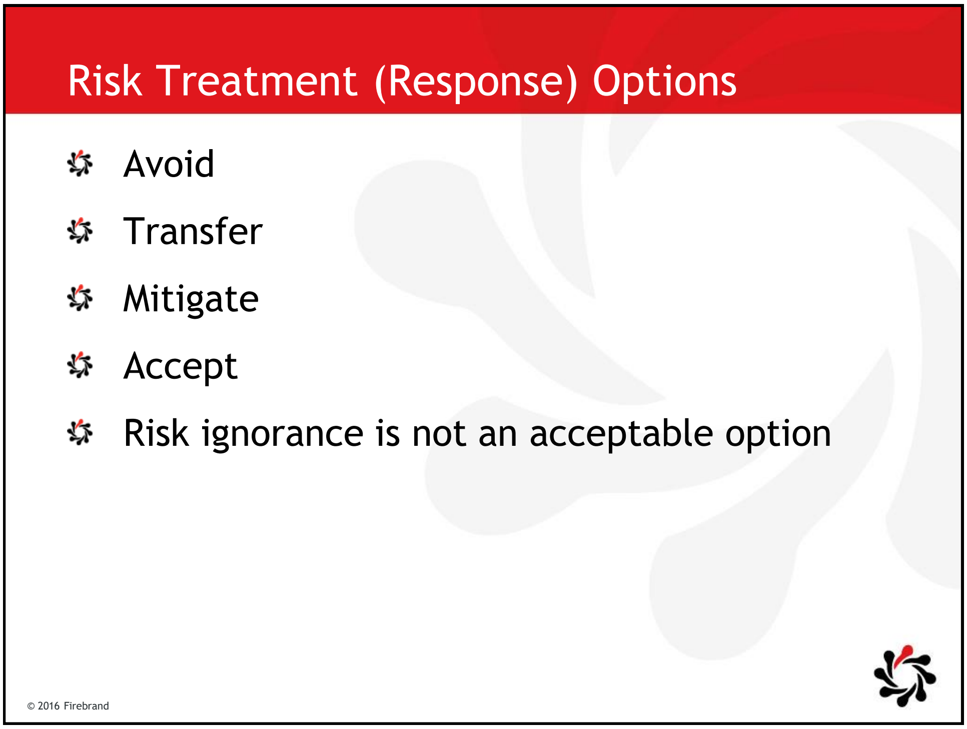
## Risk Ranking

- Risk ranking is used to direct the risk response effort
- Risk is ranked according to the evaluated level of risk



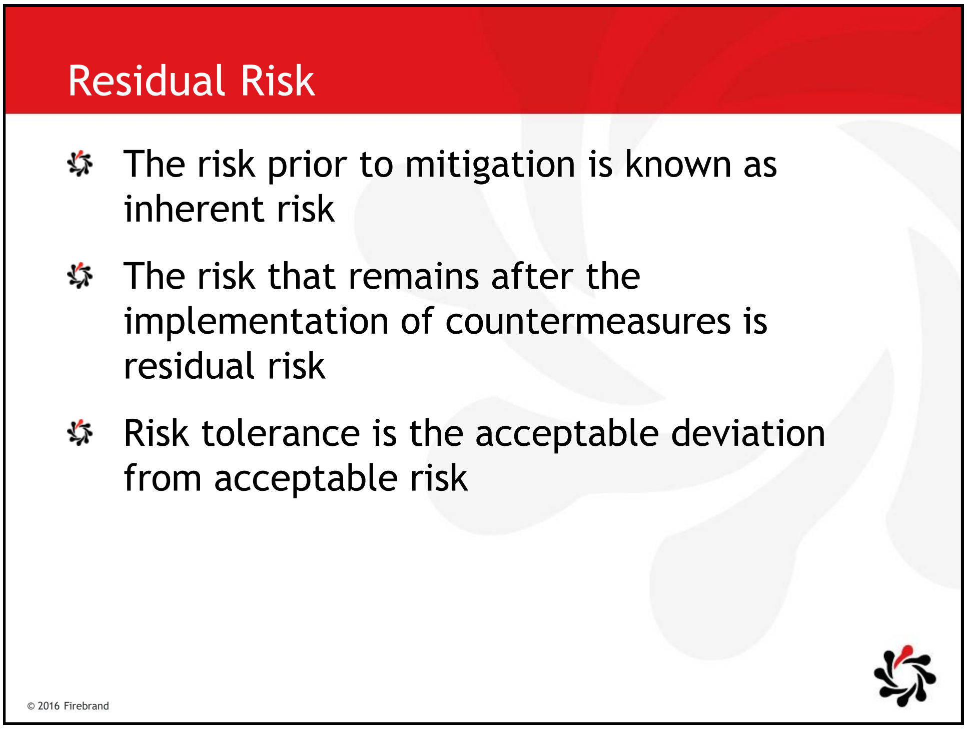
## Risk Ownership and Accountability

- Risk requires ownership and accountability
- Risk is owned by a manager or senior official
  - Should be someone with budgetary authority
- The risk owner is accountable for accepting risk and approving controls
- There should be a direct link between risk and the associated control
- The risk owner is also responsible for ensuring the monitoring of controls



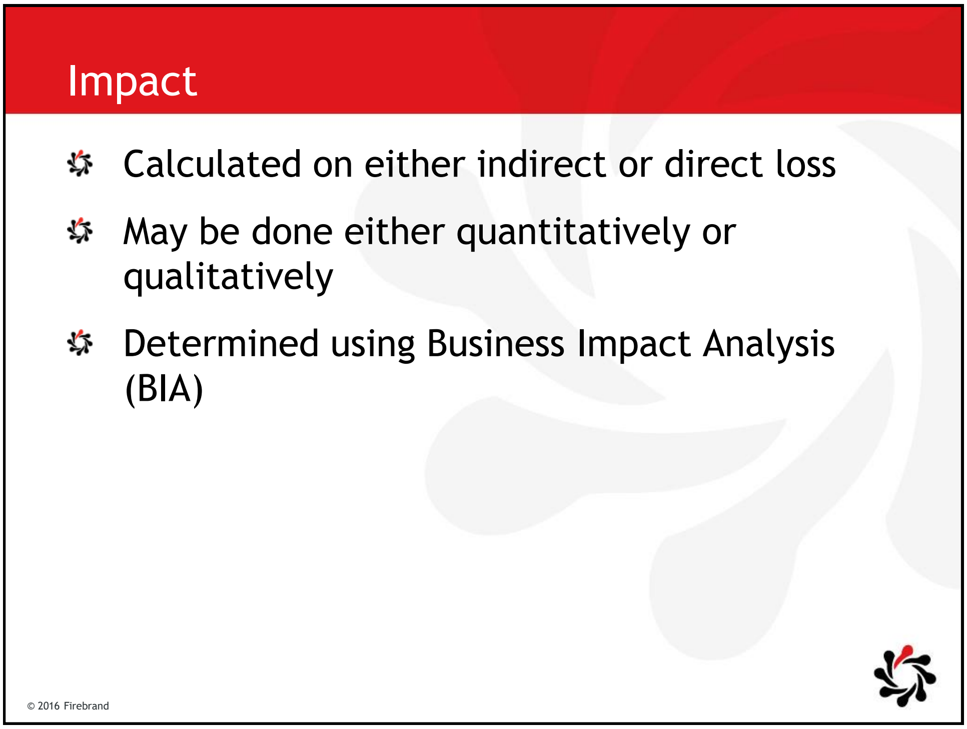
## Risk Treatment (Response) Options

- Avoid
- Transfer
- Mitigate
- Accept
- Risk ignorance is not an acceptable option



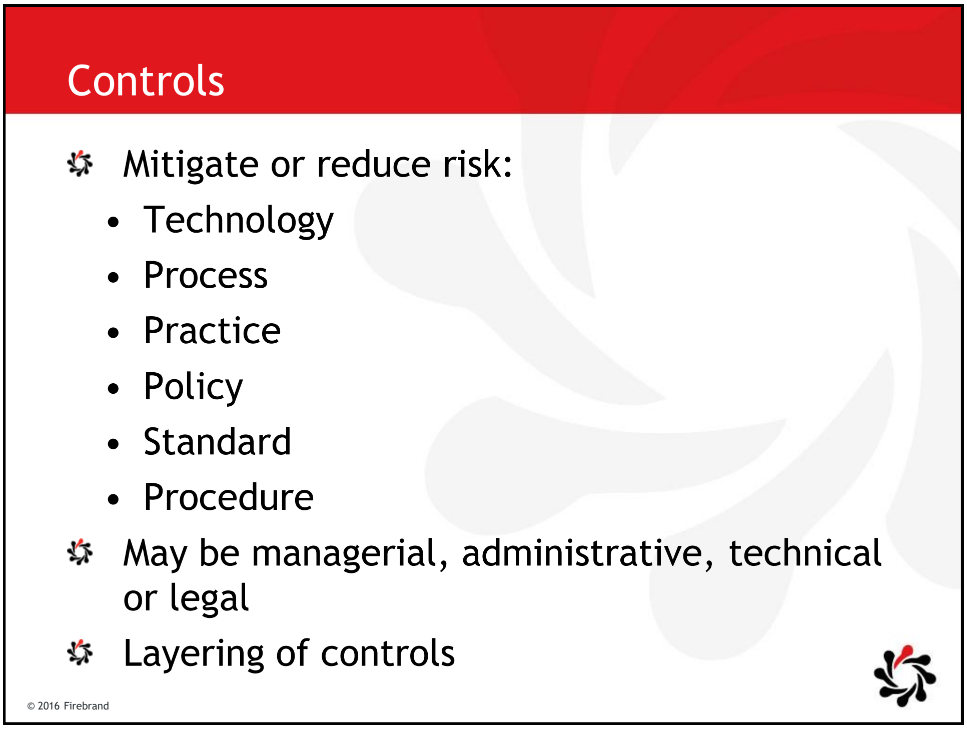
## Residual Risk

- The risk prior to mitigation is known as inherent risk
- The risk that remains after the implementation of countermeasures is residual risk
- Risk tolerance is the acceptable deviation from acceptable risk



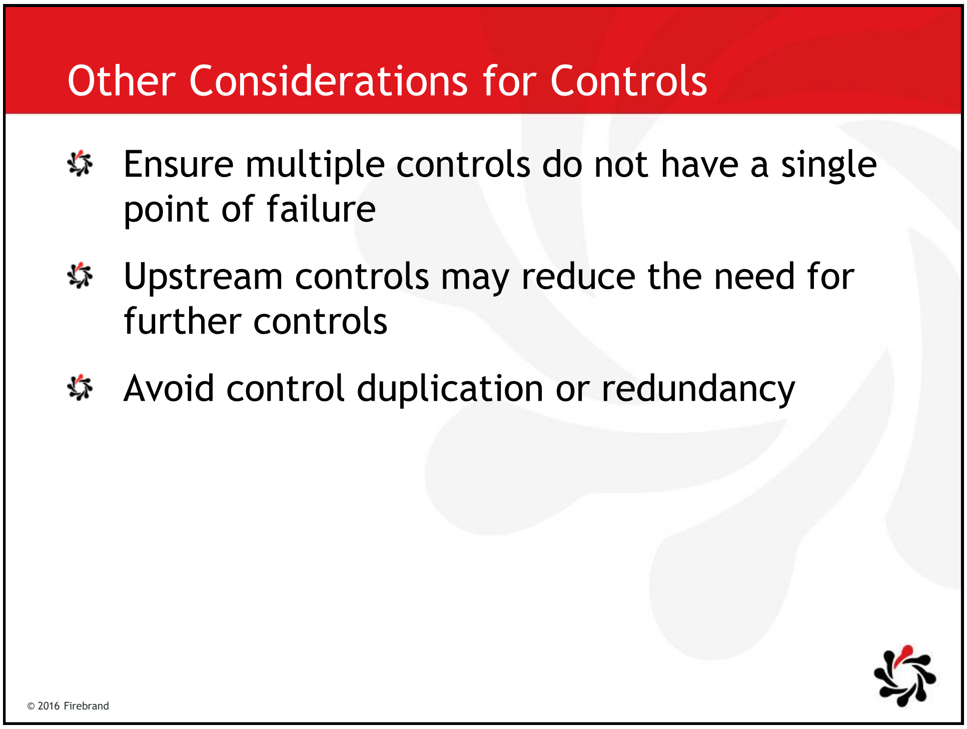
## Impact

- Calculated on either indirect or direct loss
- May be done either quantitatively or qualitatively
- Determined using Business Impact Analysis (BIA)



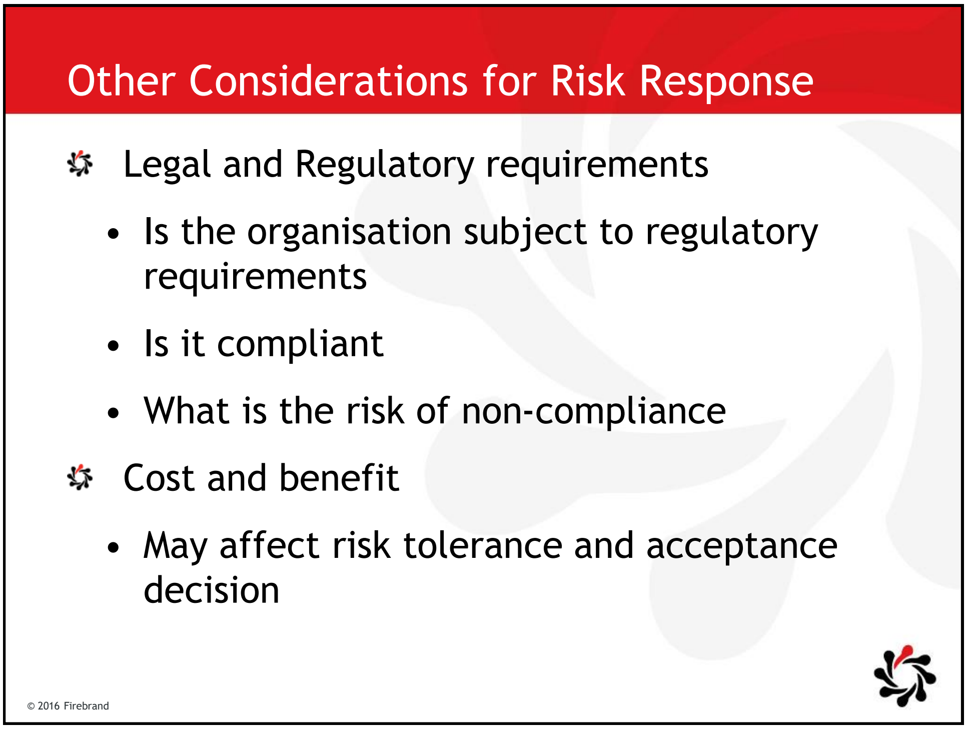
## Controls

- Mitigate or reduce risk:
  - Technology
  - Process
  - Practice
  - Policy
  - Standard
  - Procedure
- May be managerial, administrative, technical or legal
- Layering of controls



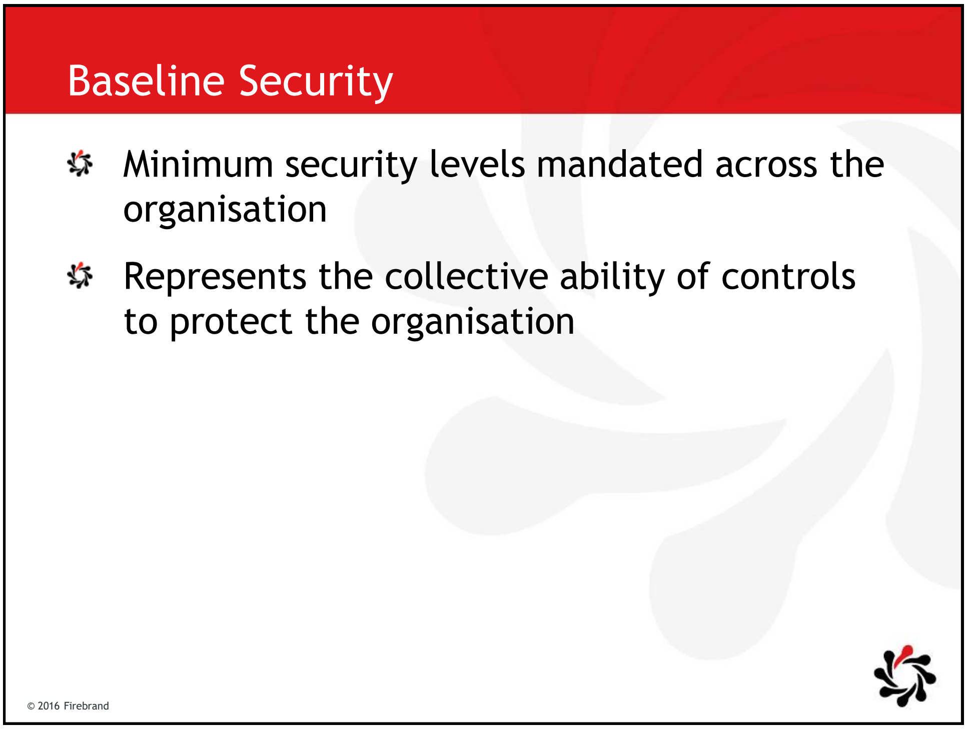
## Other Considerations for Controls

- Ensure multiple controls do not have a single point of failure
- Upstream controls may reduce the need for further controls
- Avoid control duplication or redundancy



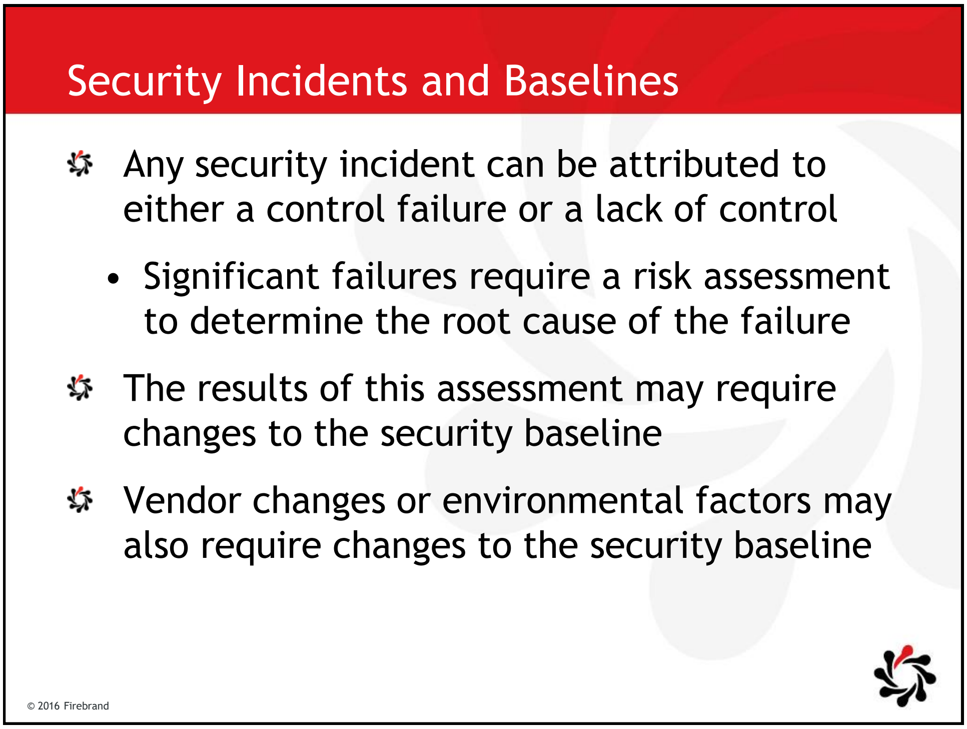
## Other Considerations for Risk Response

- Legal and Regulatory requirements
  - Is the organisation subject to regulatory requirements
  - Is it compliant
  - What is the risk of non-compliance
- Cost and benefit
  - May affect risk tolerance and acceptance decision



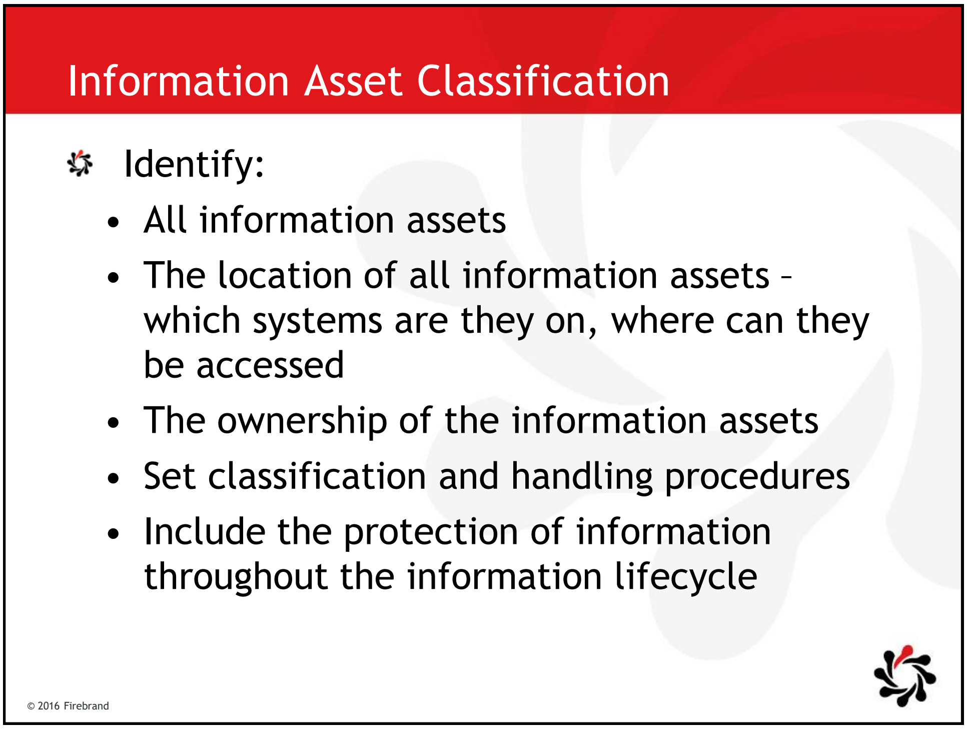
## Baseline Security

- Minimum security levels mandated across the organisation
- Represents the collective ability of controls to protect the organisation



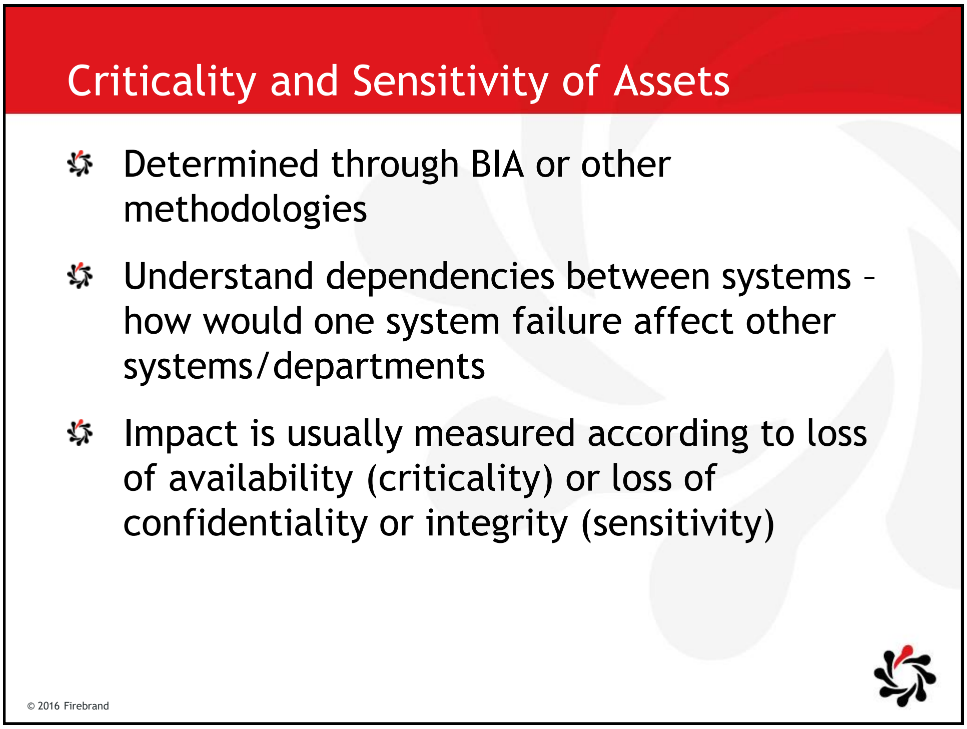
## Security Incidents and Baselines

- Any security incident can be attributed to either a control failure or a lack of control
  - Significant failures require a risk assessment to determine the root cause of the failure
- The results of this assessment may require changes to the security baseline
- Vendor changes or environmental factors may also require changes to the security baseline



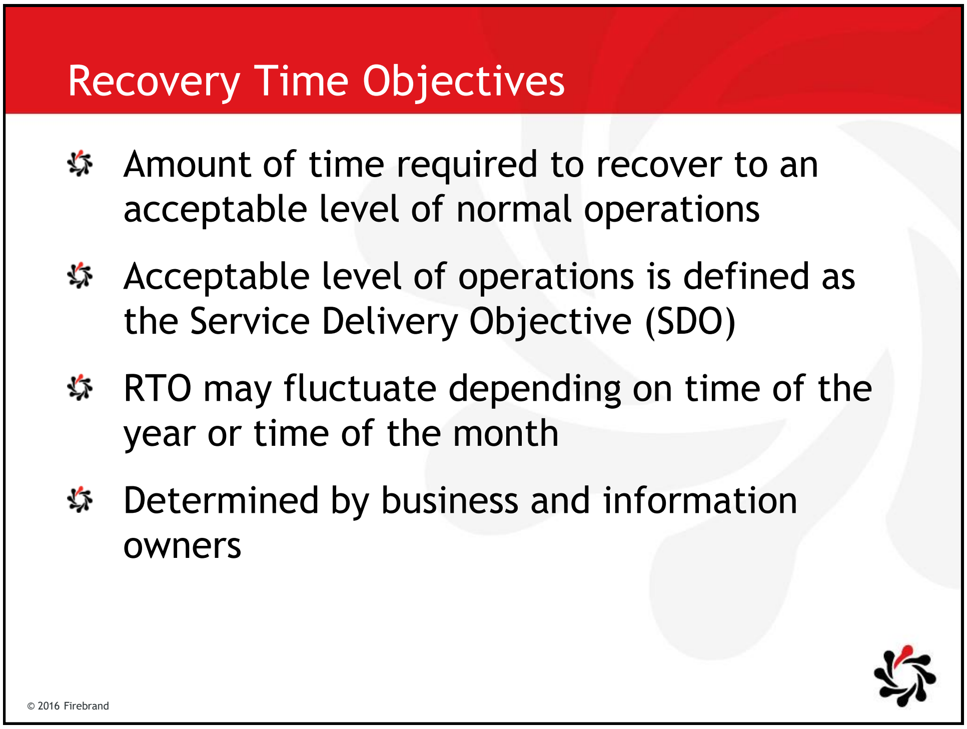
## Information Asset Classification

- Identify:
  - All information assets
  - The location of all information assets – which systems are they on, where can they be accessed
  - The ownership of the information assets
  - Set classification and handling procedures
  - Include the protection of information throughout the information lifecycle



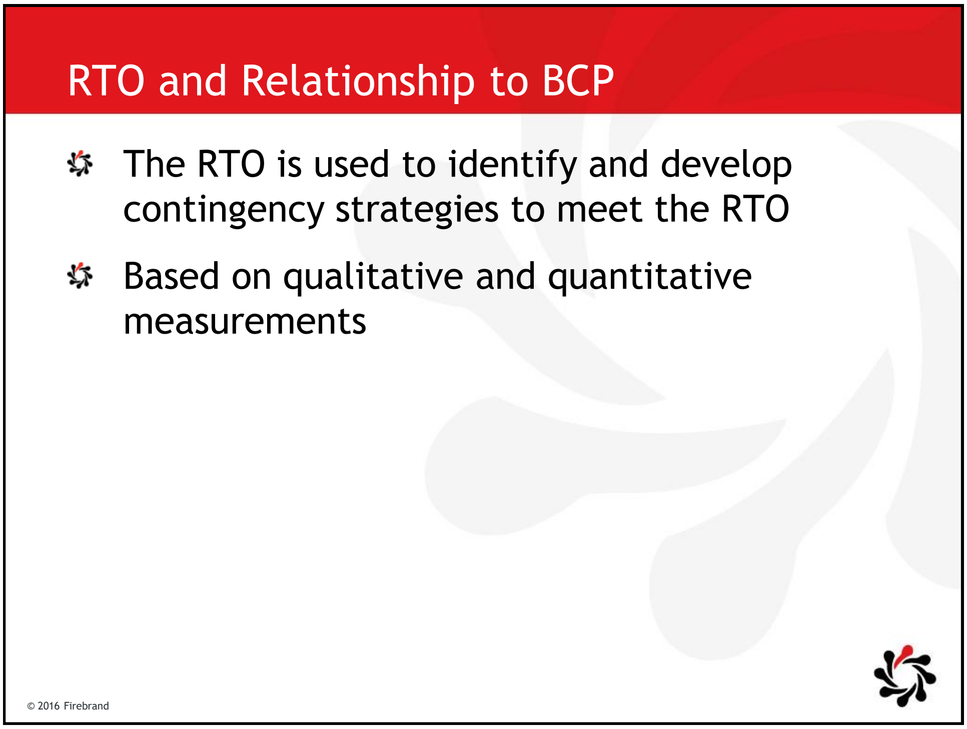
## Criticality and Sensitivity of Assets

- Determined through BIA or other methodologies
- Understand dependencies between systems – how would one system failure affect other systems/departments
- Impact is usually measured according to loss of availability (criticality) or loss of confidentiality or integrity (sensitivity)



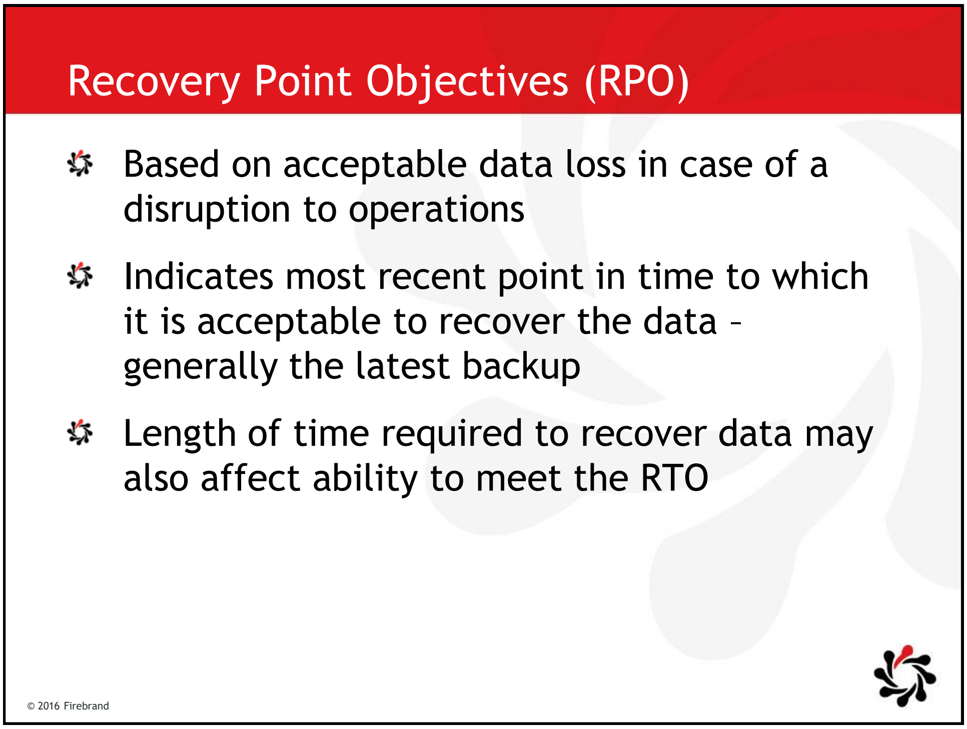
## Recovery Time Objectives

- Amount of time required to recover to an acceptable level of normal operations
- Acceptable level of operations is defined as the Service Delivery Objective (SDO)
- RTO may fluctuate depending on time of the year or time of the month
- Determined by business and information owners



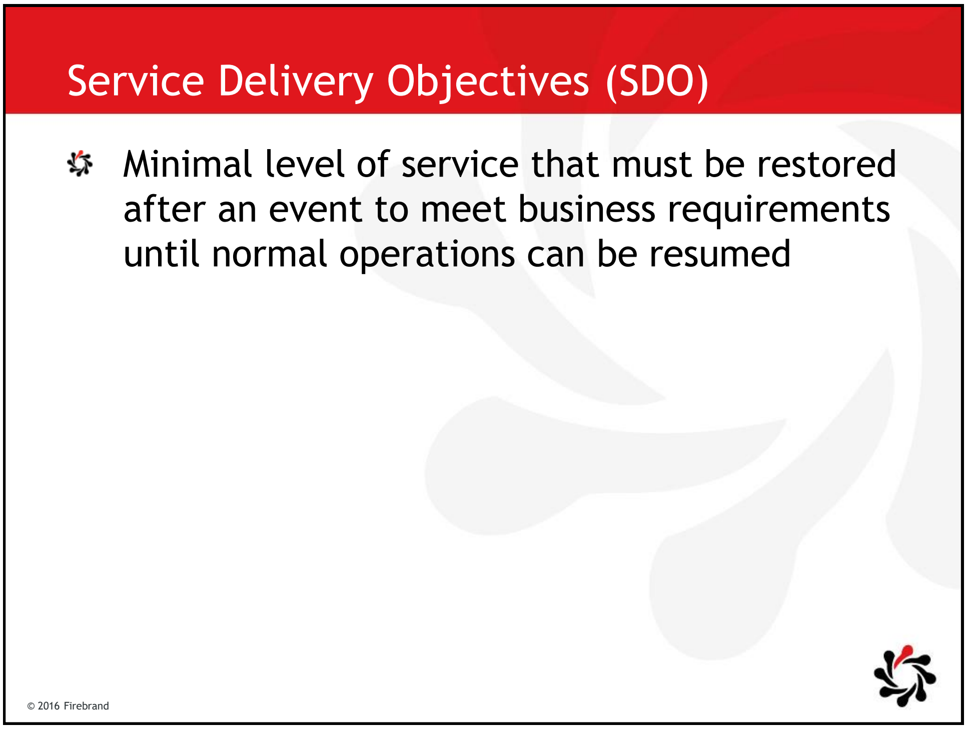
## RTO and Relationship to BCP

- The RTO is used to identify and develop contingency strategies to meet the RTO
- Based on qualitative and quantitative measurements



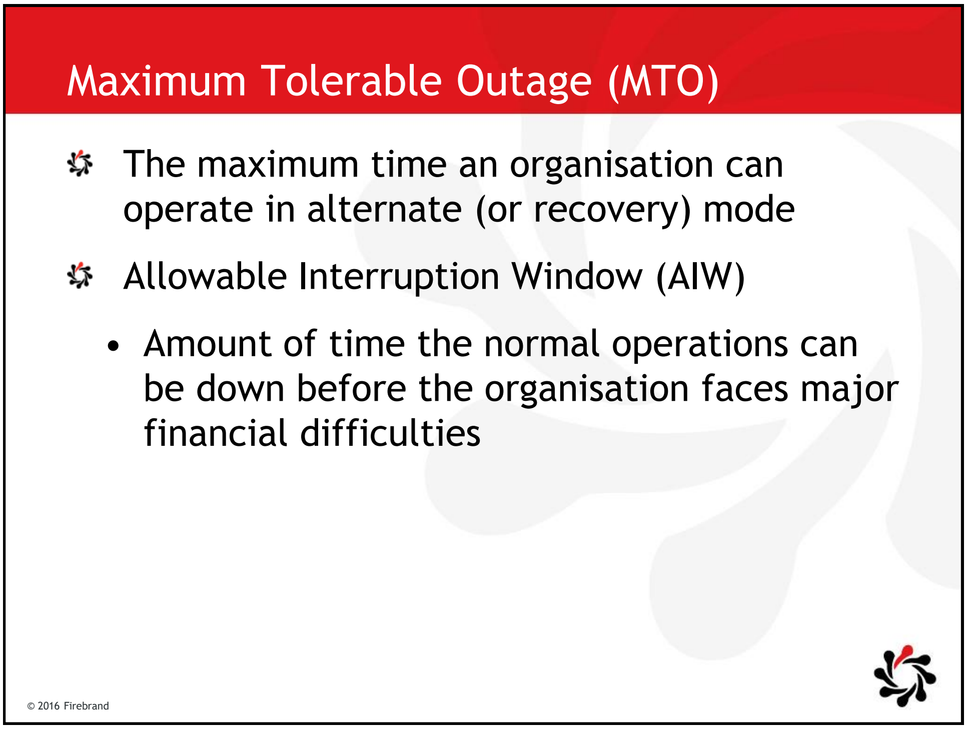
## Recovery Point Objectives (RPO)

- Based on acceptable data loss in case of a disruption to operations
- Indicates most recent point in time to which it is acceptable to recover the data – generally the latest backup
- Length of time required to recover data may also affect ability to meet the RTO



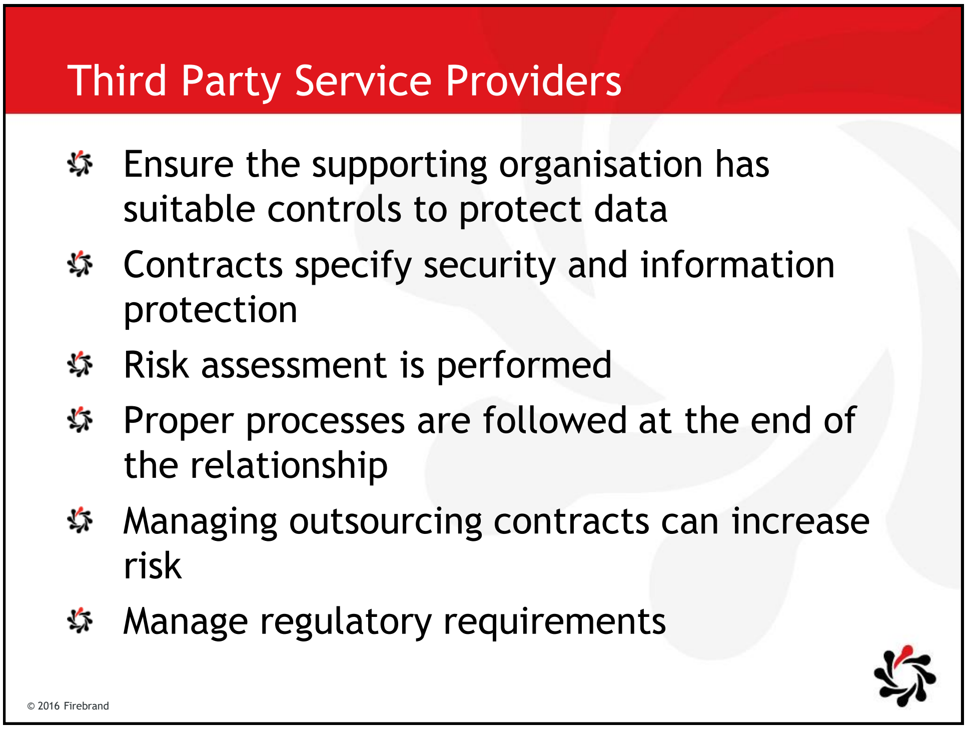
## Service Delivery Objectives (SDO)

- Minimal level of service that must be restored after an event to meet business requirements until normal operations can be resumed



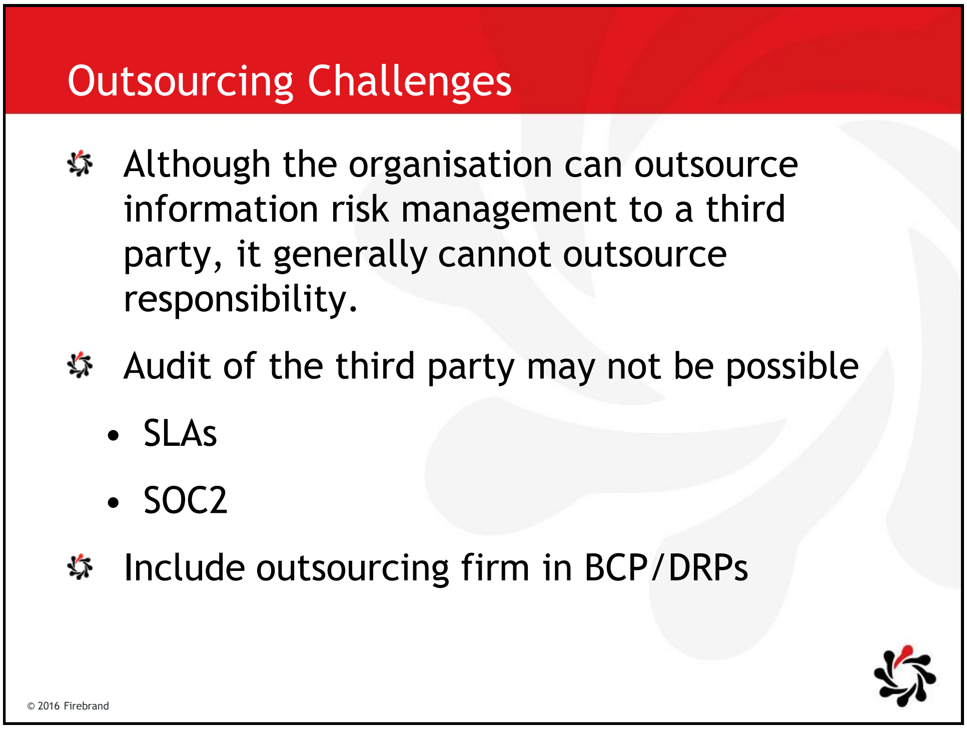
## Maximum Tolerable Outage (MTO)

- The maximum time an organisation can operate in alternate (or recovery) mode
- Allowable Interruption Window (AIW)
  - Amount of time the normal operations can be down before the organisation faces major financial difficulties



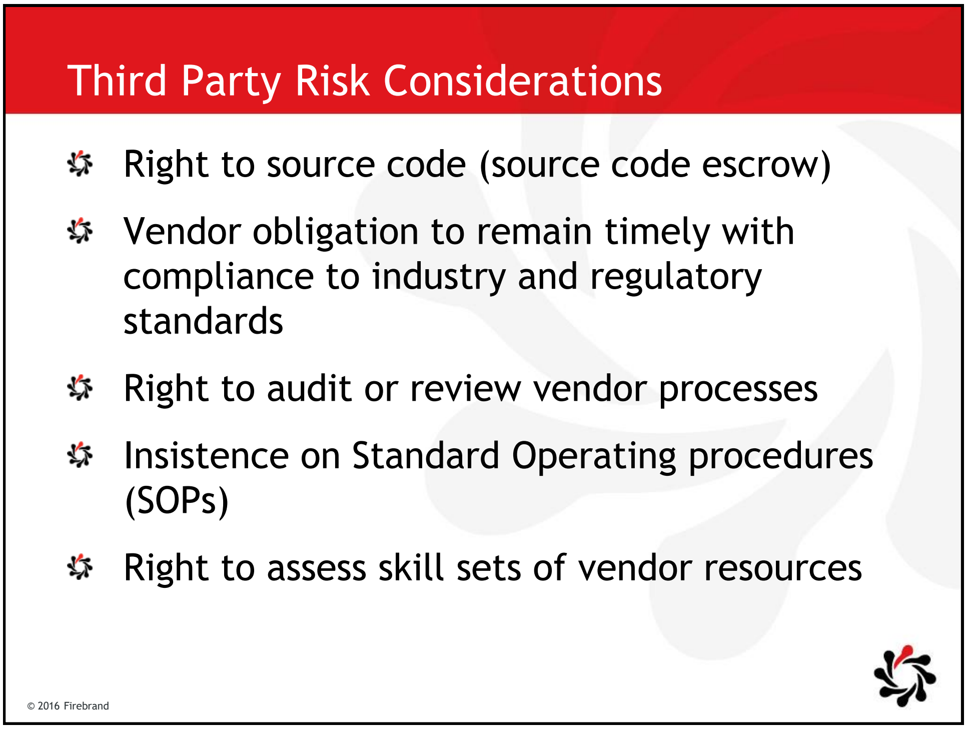
## Third Party Service Providers

- Ensure the supporting organisation has suitable controls to protect data
- Contracts specify security and information protection
- Risk assessment is performed
- Proper processes are followed at the end of the relationship
- Managing outsourcing contracts can increase risk
- Manage regulatory requirements



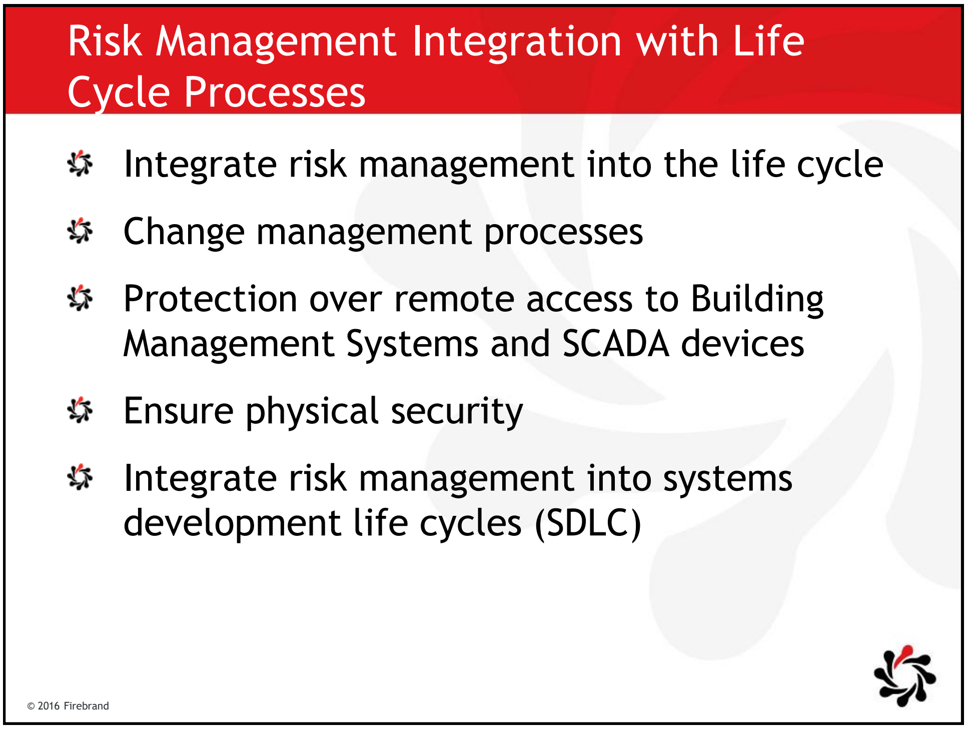
## Outsourcing Challenges

- Although the organisation can outsource information risk management to a third party, it generally cannot outsource responsibility.
- Audit of the third party may not be possible
  - SLAs
  - SOC2
- Include outsourcing firm in BCP/DRPs



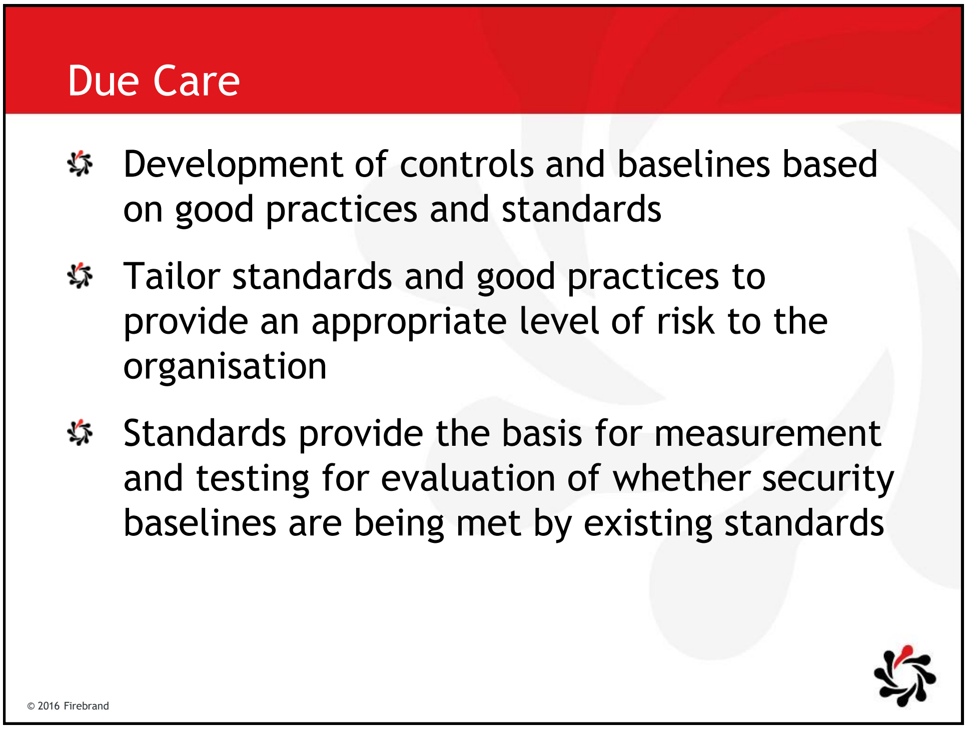
## Third Party Risk Considerations

- Right to source code (source code escrow)
- Vendor obligation to remain timely with compliance to industry and regulatory standards
- Right to audit or review vendor processes
- Insistence on Standard Operating procedures (SOPs)
- Right to assess skill sets of vendor resources



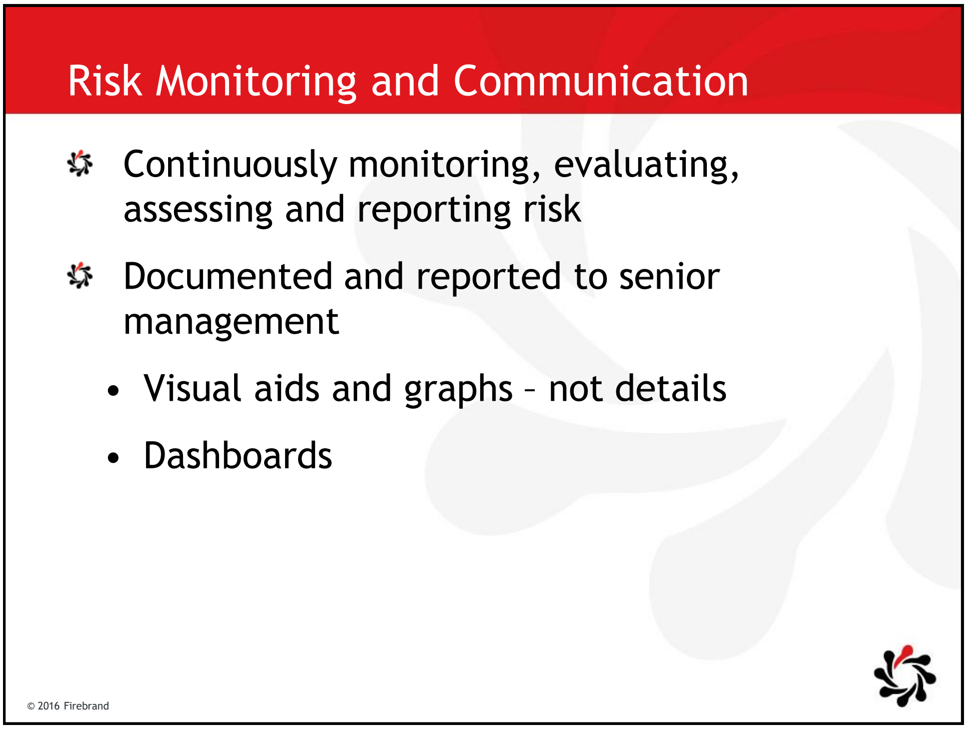
## Risk Management Integration with Life Cycle Processes

- Integrate risk management into the life cycle
- Change management processes
- Protection over remote access to Building Management Systems and SCADA devices
- Ensure physical security
- Integrate risk management into systems development life cycles (SDLC)



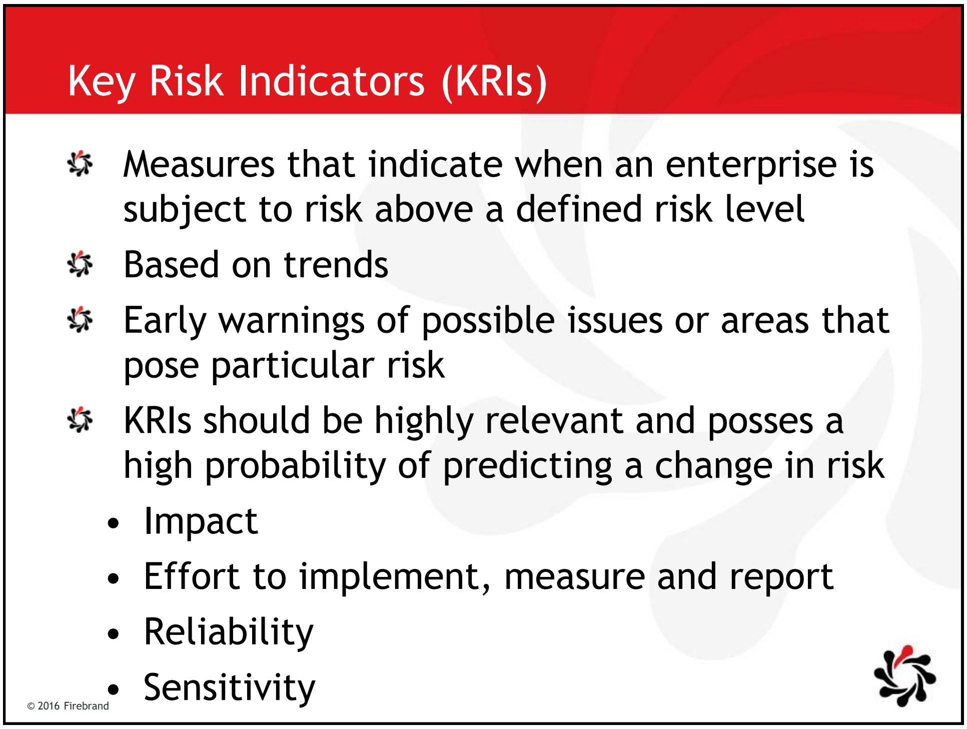
## Due Care

- Development of controls and baselines based on good practices and standards
- Tailor standards and good practices to provide an appropriate level of risk to the organisation
- Standards provide the basis for measurement and testing for evaluation of whether security baselines are being met by existing standards



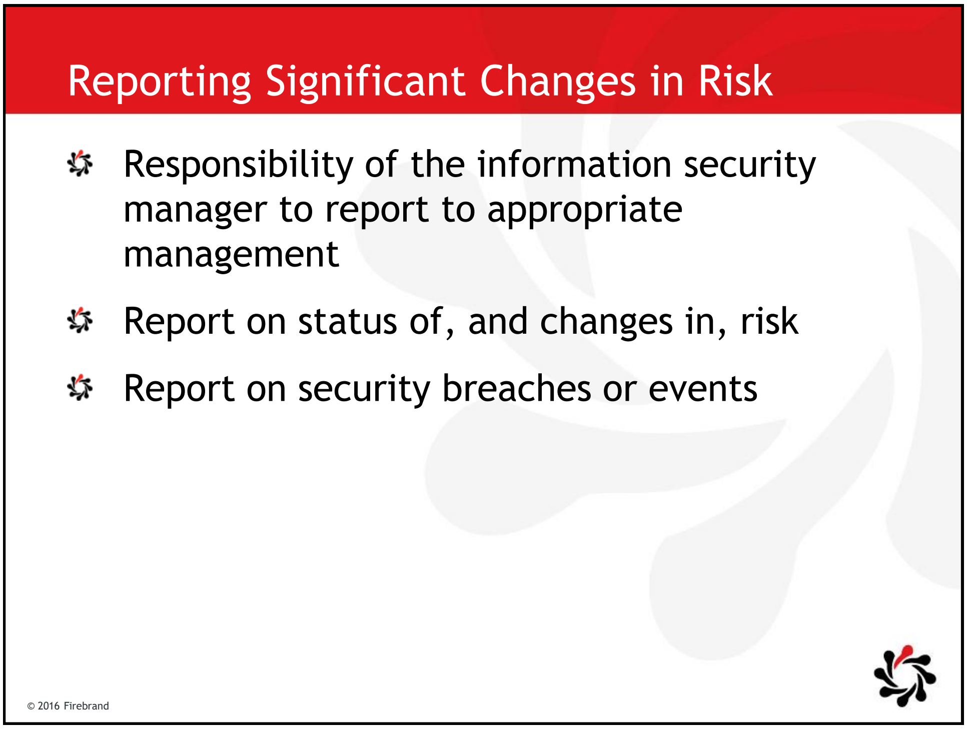
## Risk Monitoring and Communication

- Continuously monitoring, evaluating, assessing and reporting risk
- Documented and reported to senior management
  - Visual aids and graphs – not details
  - Dashboards



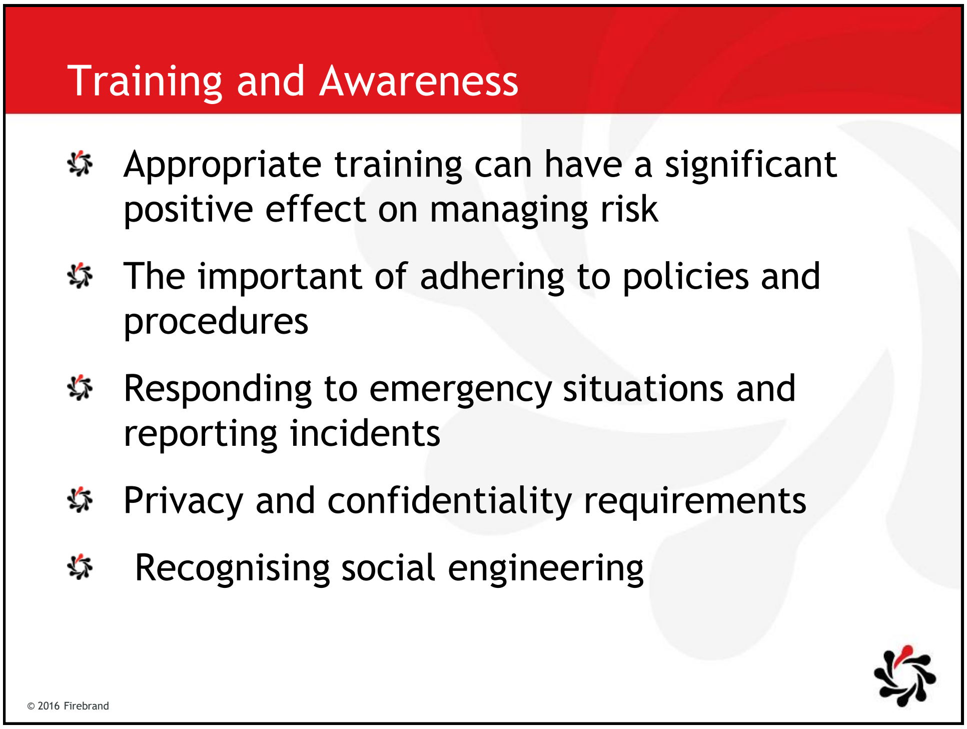
## Key Risk Indicators (KRIs)

- Measures that indicate when an enterprise is subject to risk above a defined risk level
- Based on trends
- Early warnings of possible issues or areas that pose particular risk
- KRIs should be highly relevant and posses a high probability of predicting a change in risk
  - Impact
  - Effort to implement, measure and report
  - Reliability
  - Sensitivity



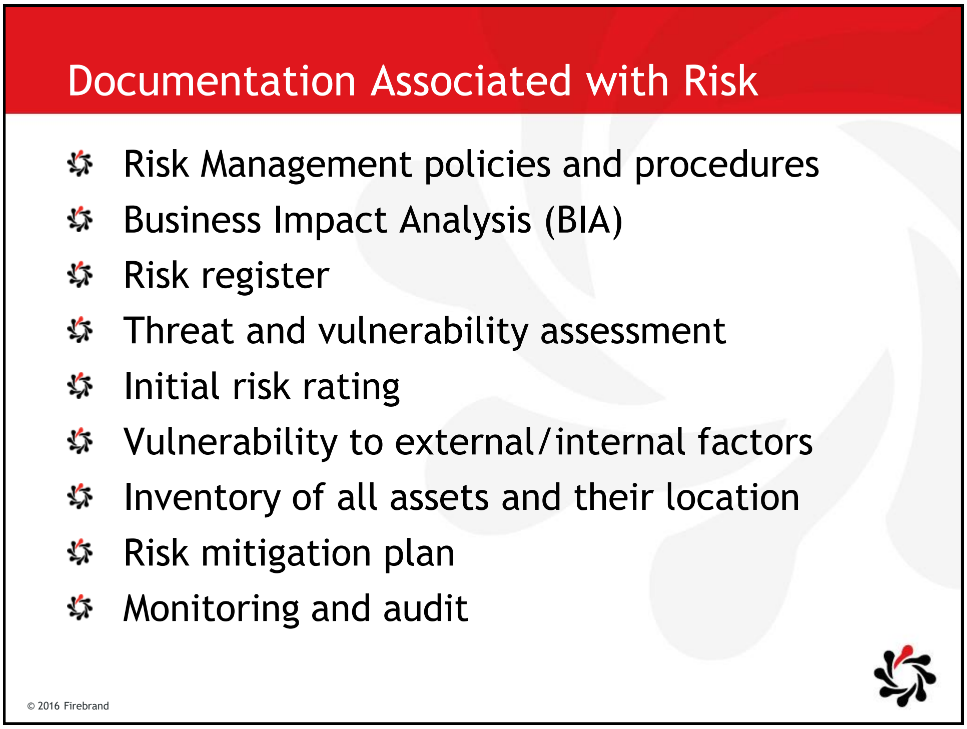
## Reporting Significant Changes in Risk

- Responsibility of the information security manager to report to appropriate management
- Report on status of, and changes in, risk
- Report on security breaches or events



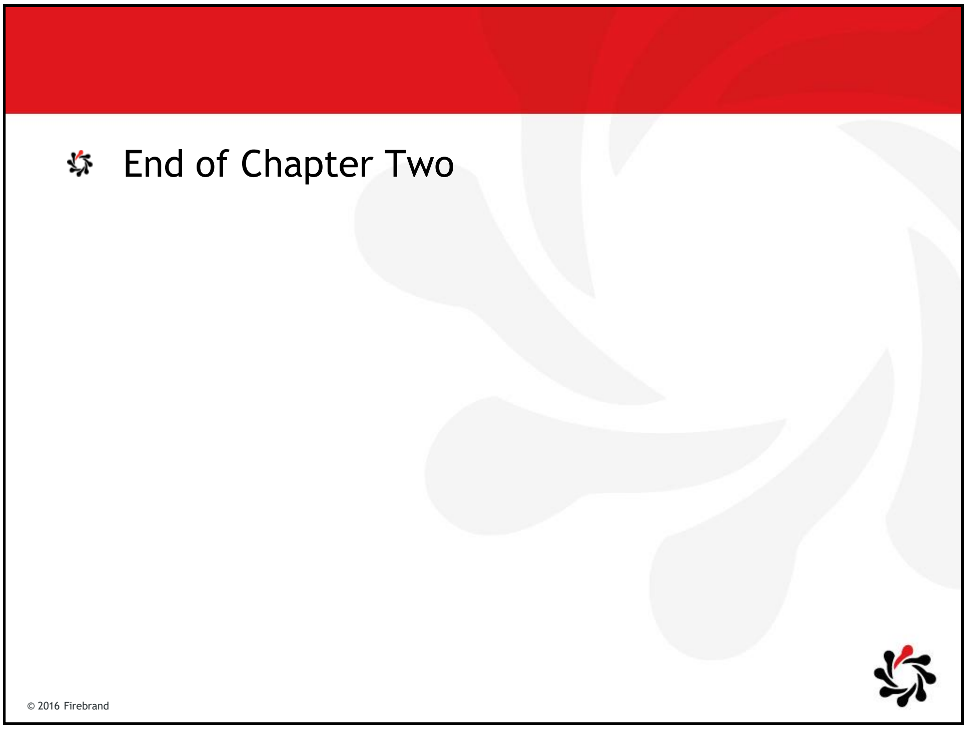
## Training and Awareness

- Appropriate training can have a significant positive effect on managing risk
- The important of adhering to policies and procedures
- Responding to emergency situations and reporting incidents
- Privacy and confidentiality requirements
- Recognising social engineering



## Documentation Associated with Risk

- Risk Management policies and procedures
- Business Impact Analysis (BIA)
- Risk register
- Threat and vulnerability assessment
- Initial risk rating
- Vulnerability to external/internal factors
- Inventory of all assets and their location
- Risk mitigation plan
- Monitoring and audit

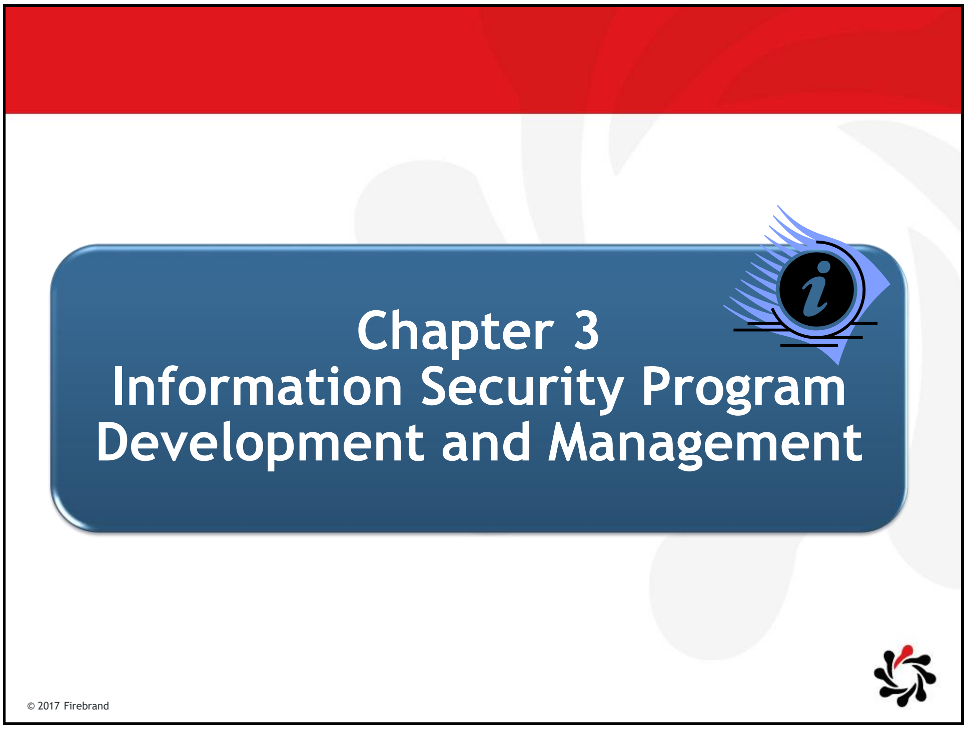


- End of Chapter Two

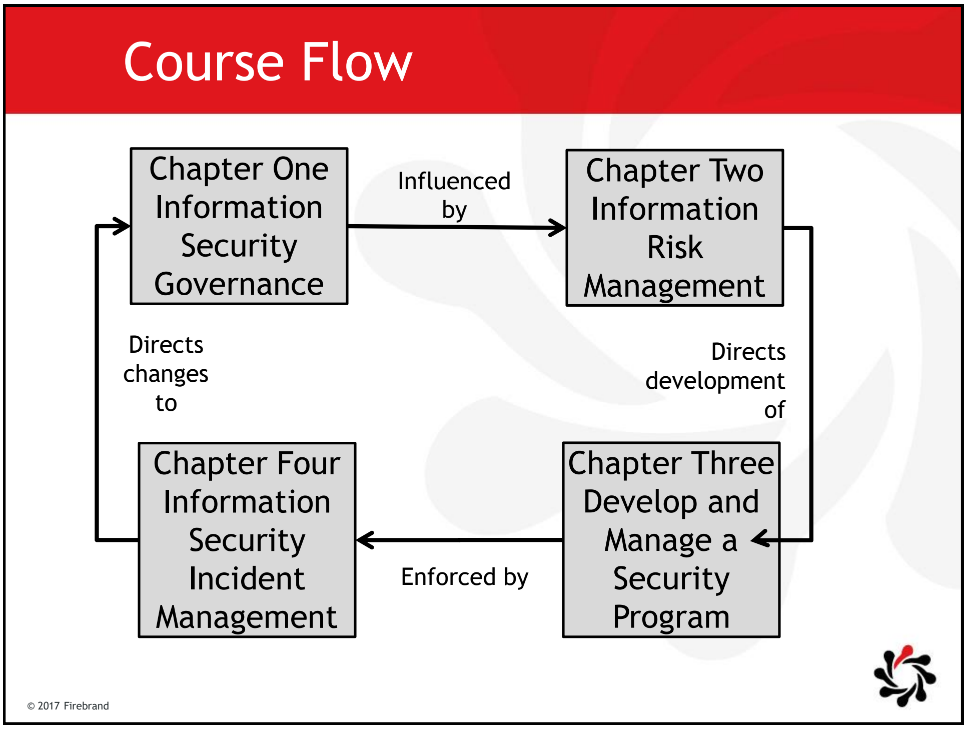
# CISM™

## Certified Information Security Manager

Firebrand Custom Designed Courseware



# Chapter 3 Information Security Program Development and Management



## Course Flow

Chapter One Information Security Governance

Influenced by

Chapter Two Information Risk Management

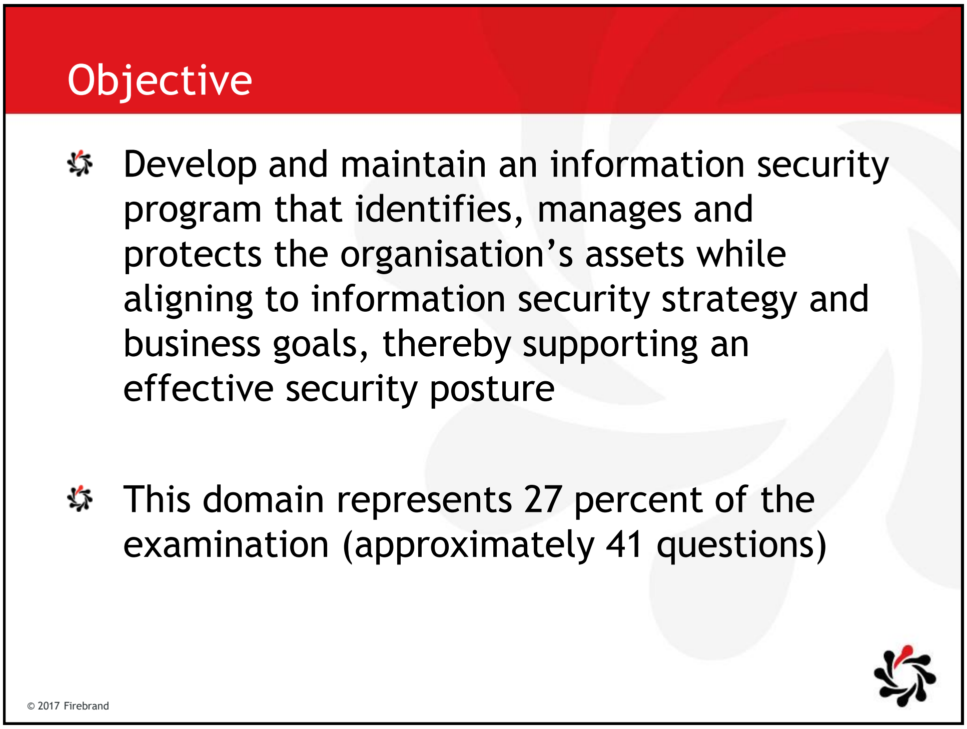
Directs development of

Chapter Three Develop and Manage a Security Program

Enforced by

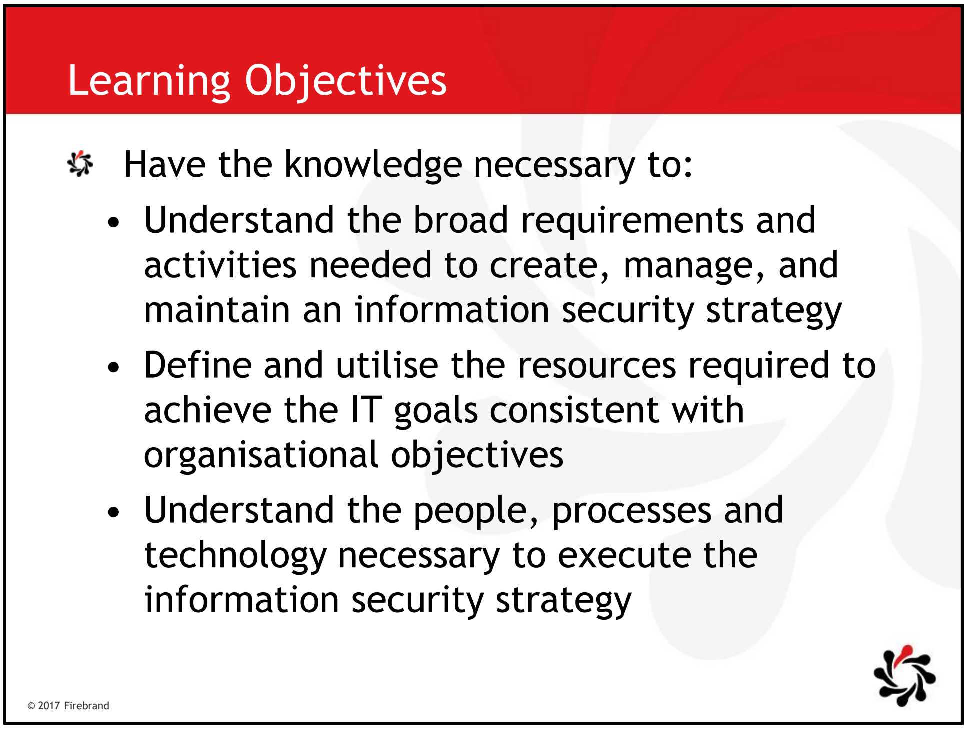
Chapter Four Information Security Incident Management

Directs changes to



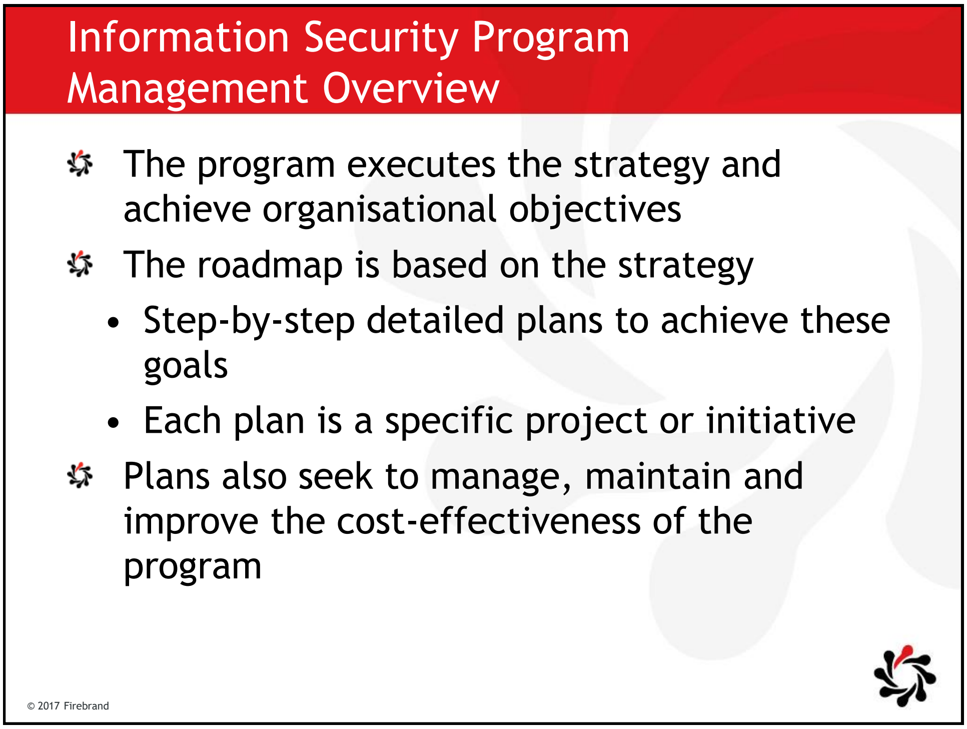
## Objective

- Develop and maintain an information security program that identifies, manages and protects the organisation’s assets while aligning to information security strategy and business goals, thereby supporting an effective security posture
- This domain represents 27 percent of the examination (approximately 41 questions)



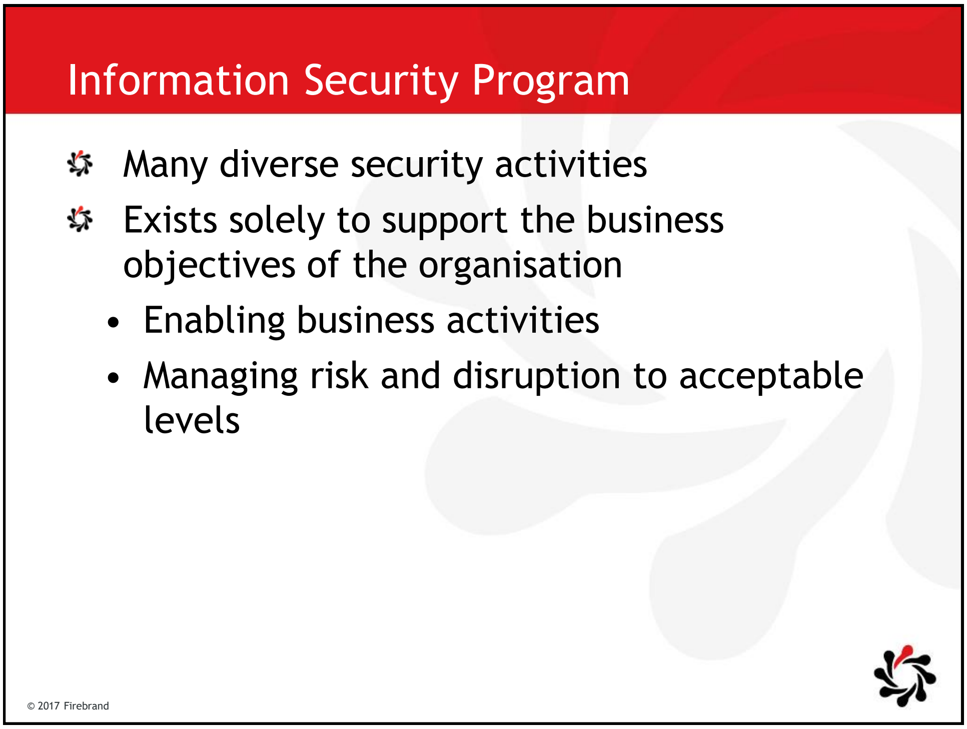
## Learning Objectives

- Have the knowledge necessary to:
  - Understand the broad requirements and activities needed to create, manage, and maintain an information security strategy
  - Define and utilise the resources required to achieve the IT goals consistent with organisational objectives
  - Understand the people, processes and technology necessary to execute the information security strategy



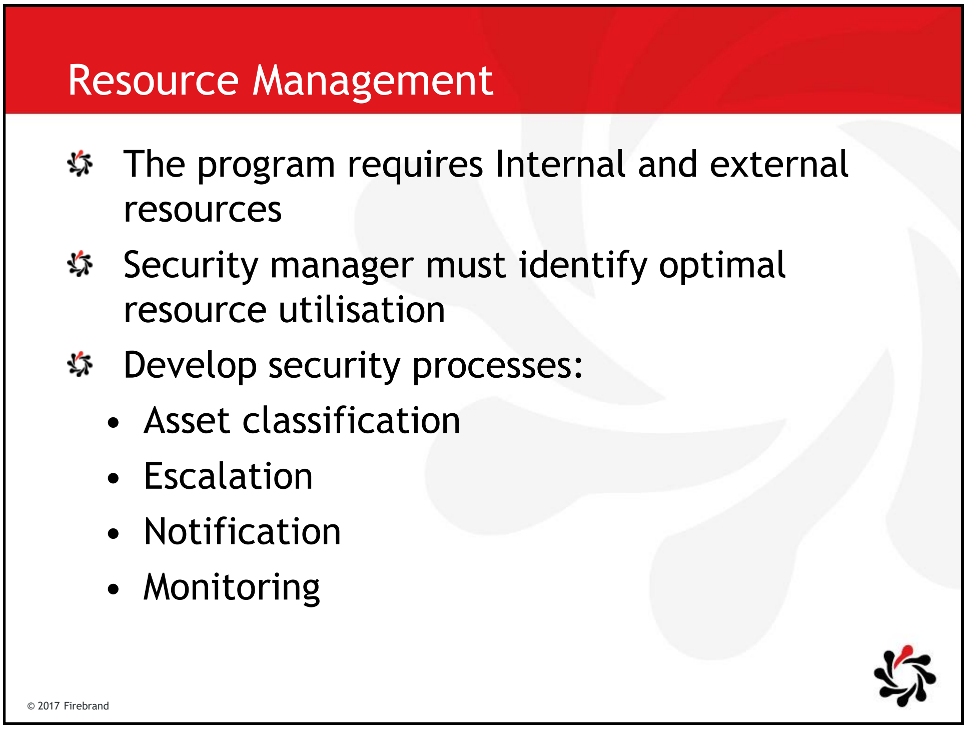
## Information Security Program Management Overview

- The program executes the strategy and achieve organisational objectives
- The roadmap is based on the strategy
  - Step-by-step detailed plans to achieve these goals
  - Each plan is a specific project or initiative
- Plans also seek to manage, maintain and improve the cost-effectiveness of the program



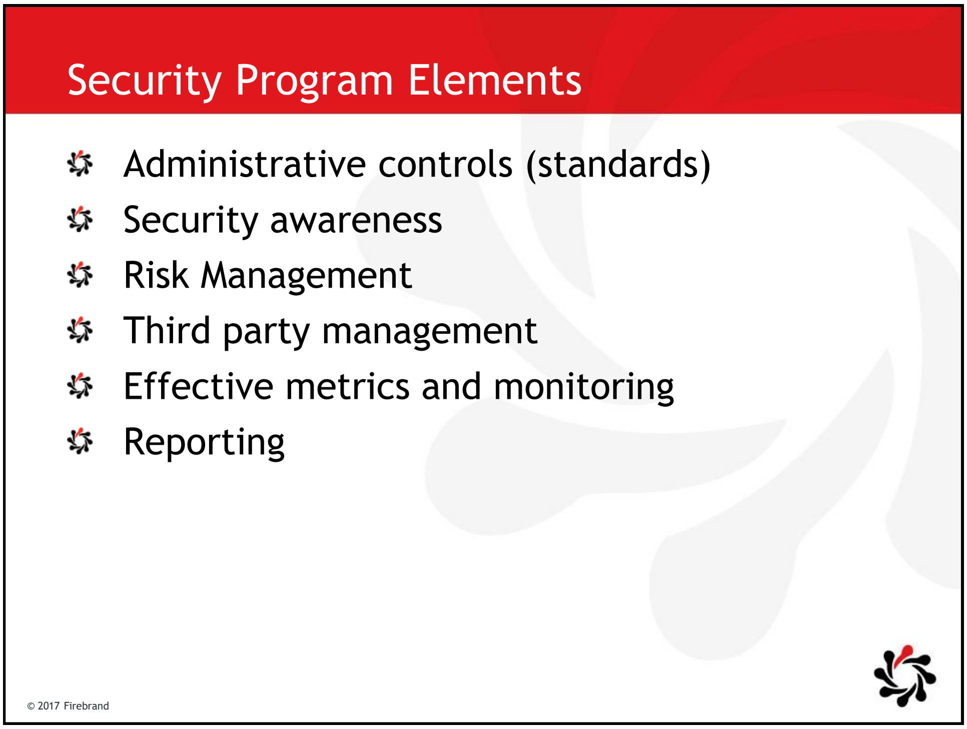
## Information Security Program

- Many diverse security activities
- Exists solely to support the business objectives of the organisation
  - Enabling business activities
  - Managing risk and disruption to acceptable levels



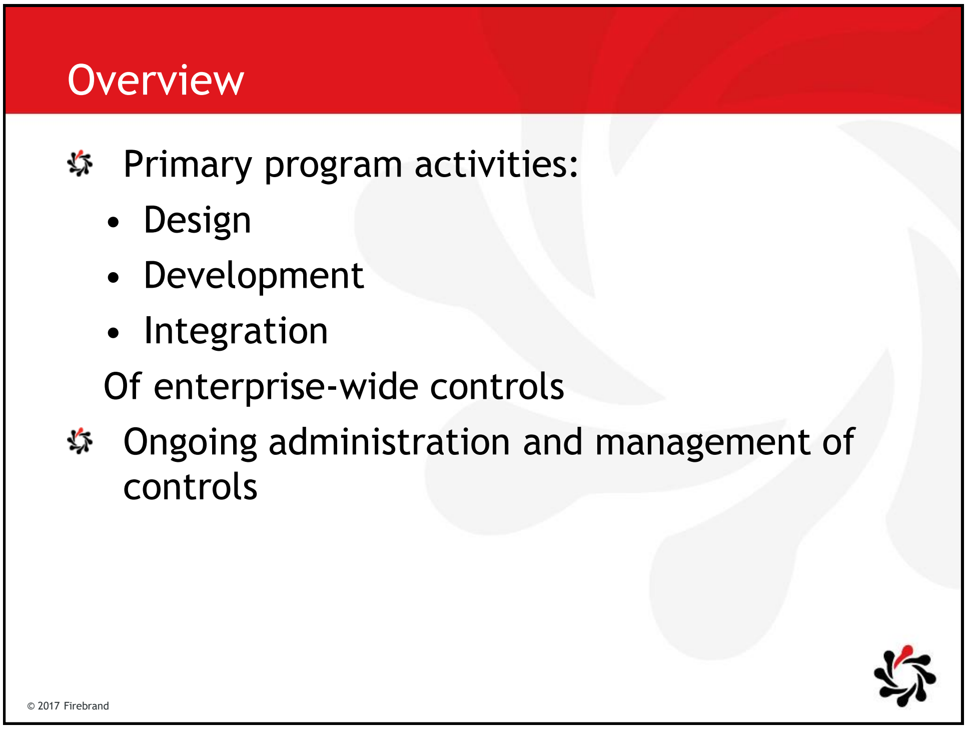
## Resource Management

- The program requires Internal and external resources
- Security manager must identify optimal resource utilisation
- Develop security processes:
  - Asset classification
  - Escalation
  - Notification
  - Monitoring



## Security Program Elements

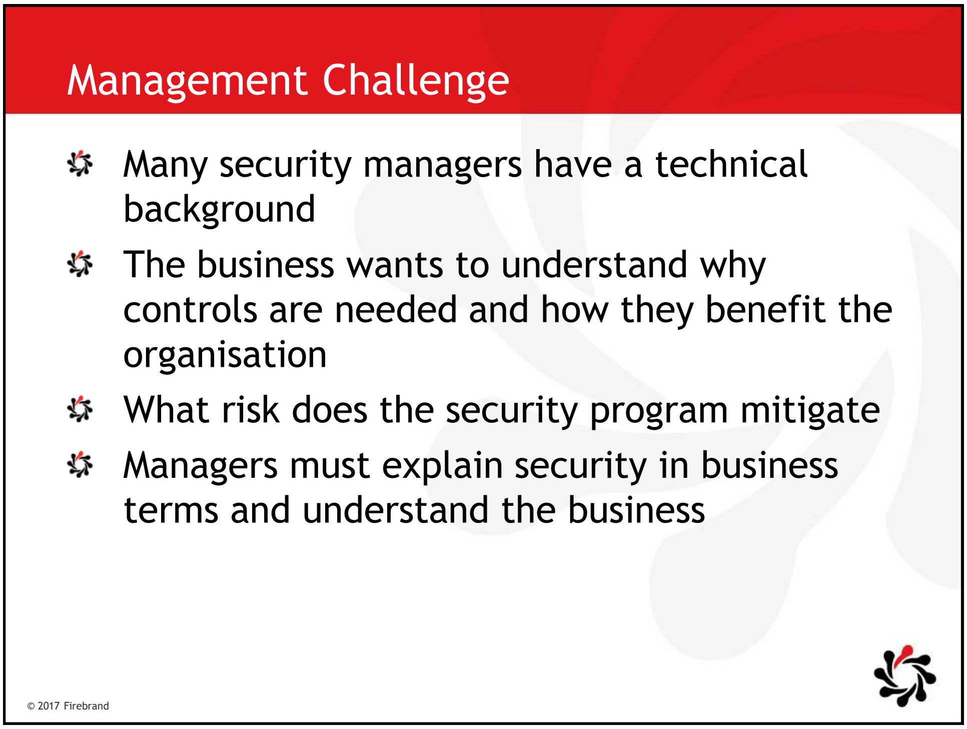
- Administrative controls (standards)
- Security awareness
- Risk Management
- Third party management
- Effective metrics and monitoring
- Reporting



## Overview

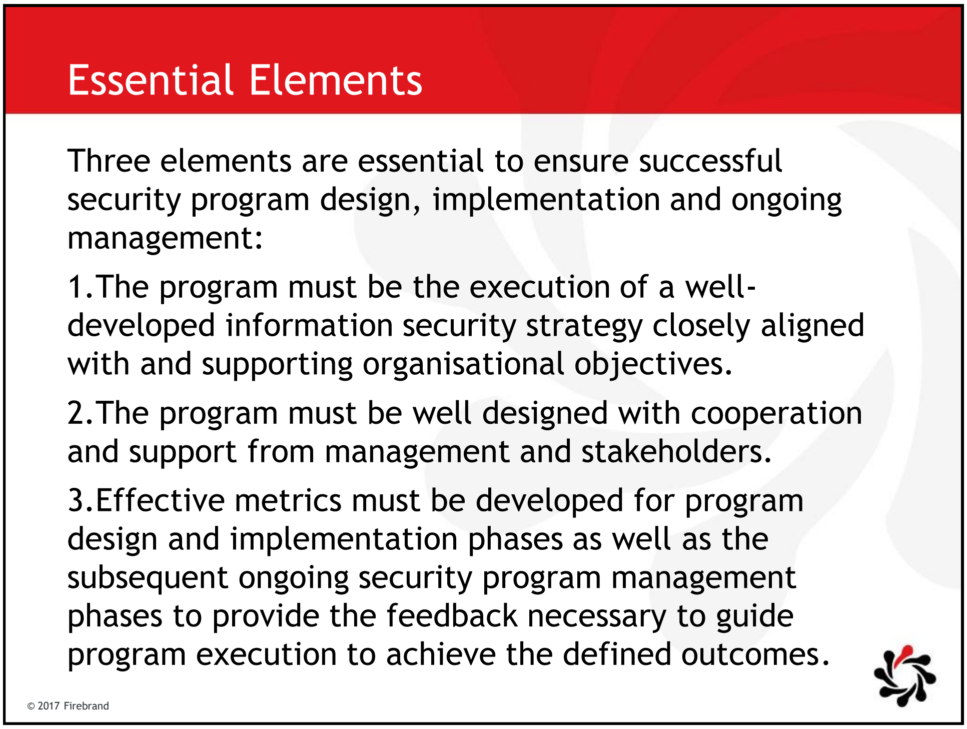
- Primary program activities:
  - Design
  - Development
  - Integration

  Of enterprise-wide controls
- Ongoing administration and management of controls



## Management Challenge

- Many security managers have a technical background
- The business wants to understand why controls are needed and how they benefit the organisation
- What risk does the security program mitigate
- Managers must explain security in business terms and understand the business



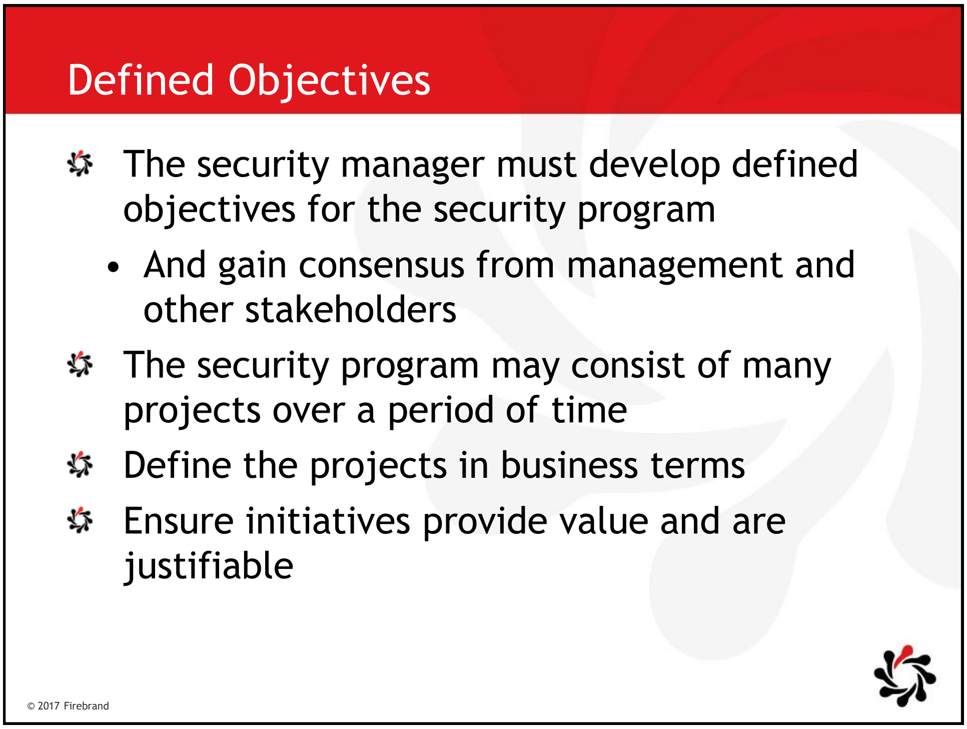
## Essential Elements

Three elements are essential to ensure successful security program design, implementation and ongoing management:

1.The program must be the execution of a well-developed information security strategy closely aligned with and supporting organisational objectives.

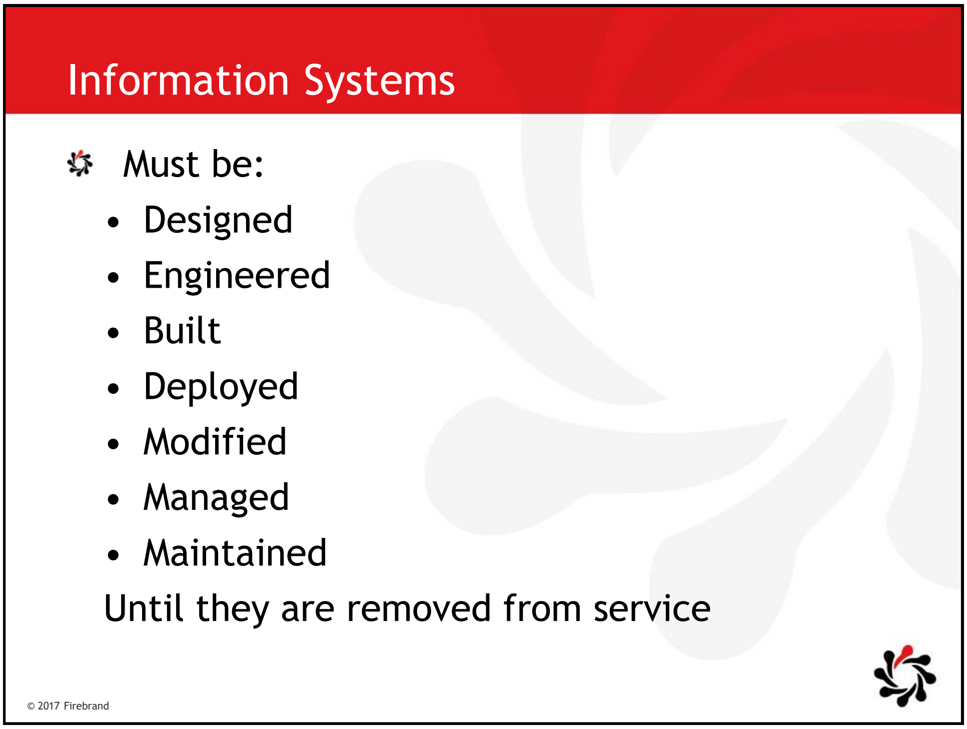
2.The program must be well designed with cooperation and support from management and stakeholders.

3.Effective metrics must be developed for program design and implementation phases as well as the subsequent ongoing security program management phases to provide the feedback necessary to guide program execution to achieve the defined outcomes.



## Defined Objectives

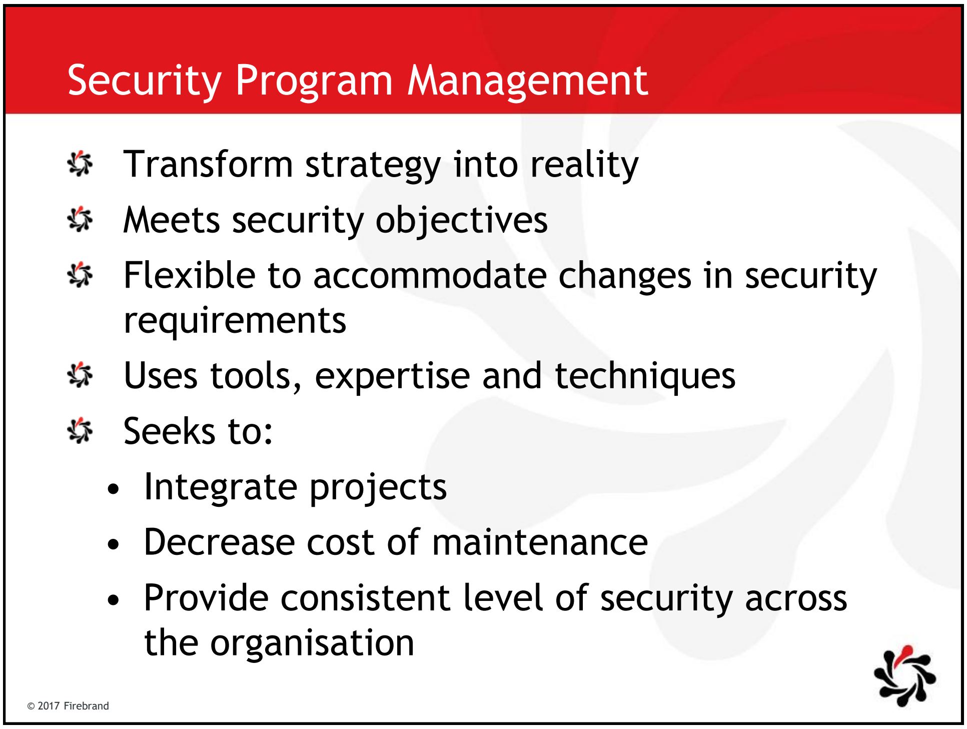
- The security manager must develop defined objectives for the security program
  - And gain consensus from management and other stakeholders
- The security program may consist of many projects over a period of time
- Define the projects in business terms
- Ensure initiatives provide value and are justifiable



## Information Systems

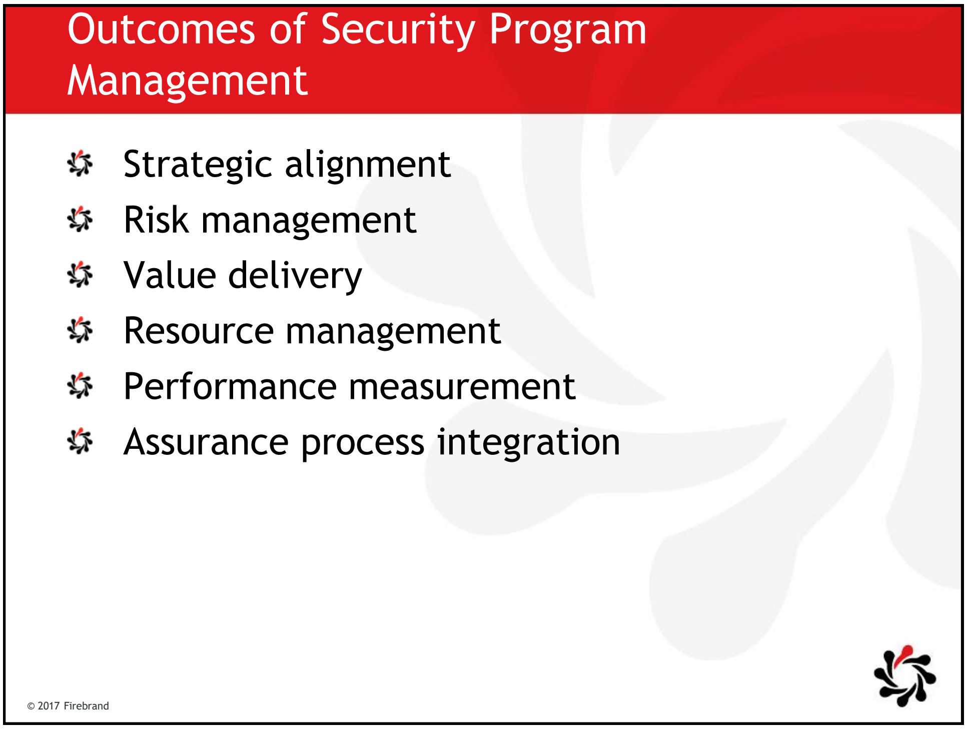
- Must be:
  - Designed
  - Engineered
  - Built
  - Deployed
  - Modified
  - Managed
  - Maintained

Until they are removed from service



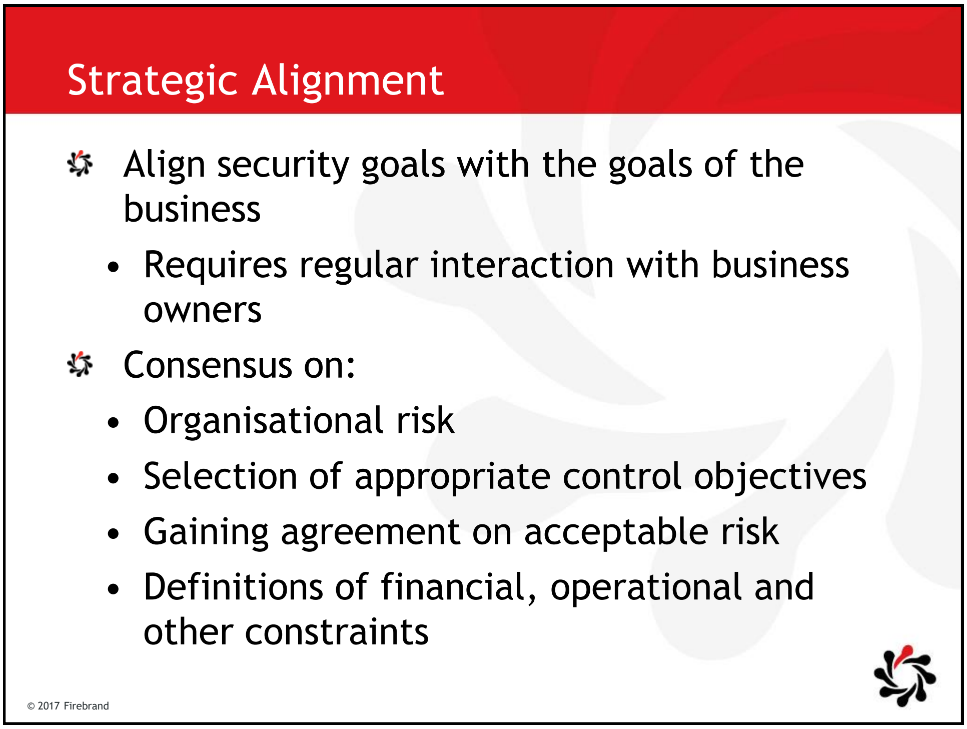
## Security Program Management

- Transform strategy into reality
- Meets security objectives
- Flexible to accommodate changes in security requirements
- Uses tools, expertise and techniques
- Seeks to:
  - Integrate projects
  - Decrease cost of maintenance
  - Provide consistent level of security across the organisation



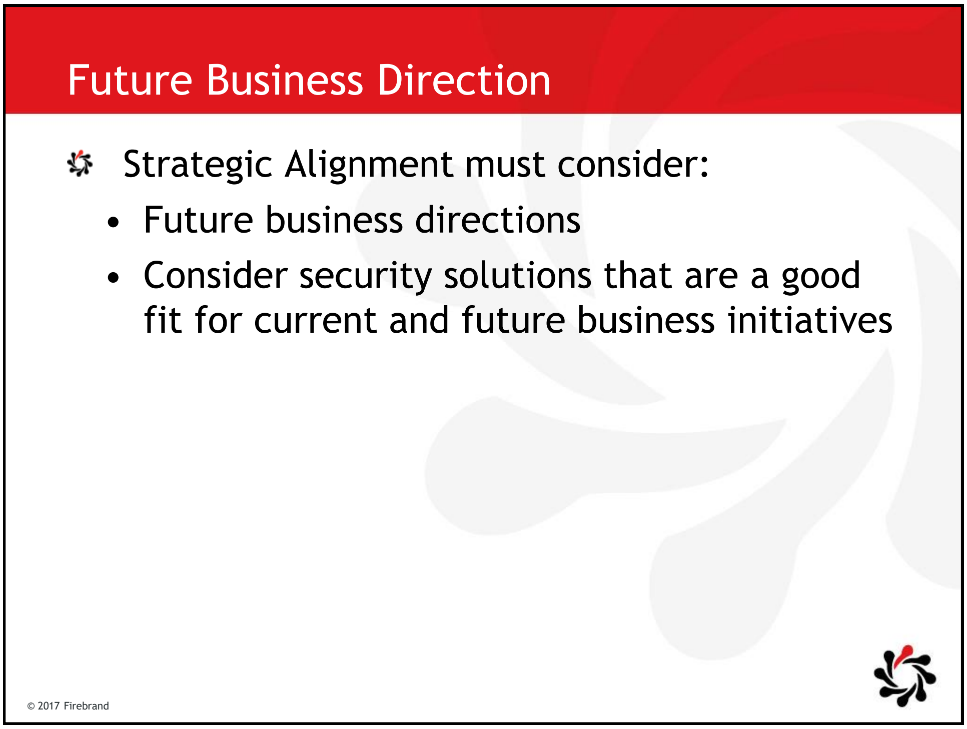
## Outcomes of Security Program Management

- Strategic alignment
- Risk management
- Value delivery
- Resource management
- Performance measurement
- Assurance process integration



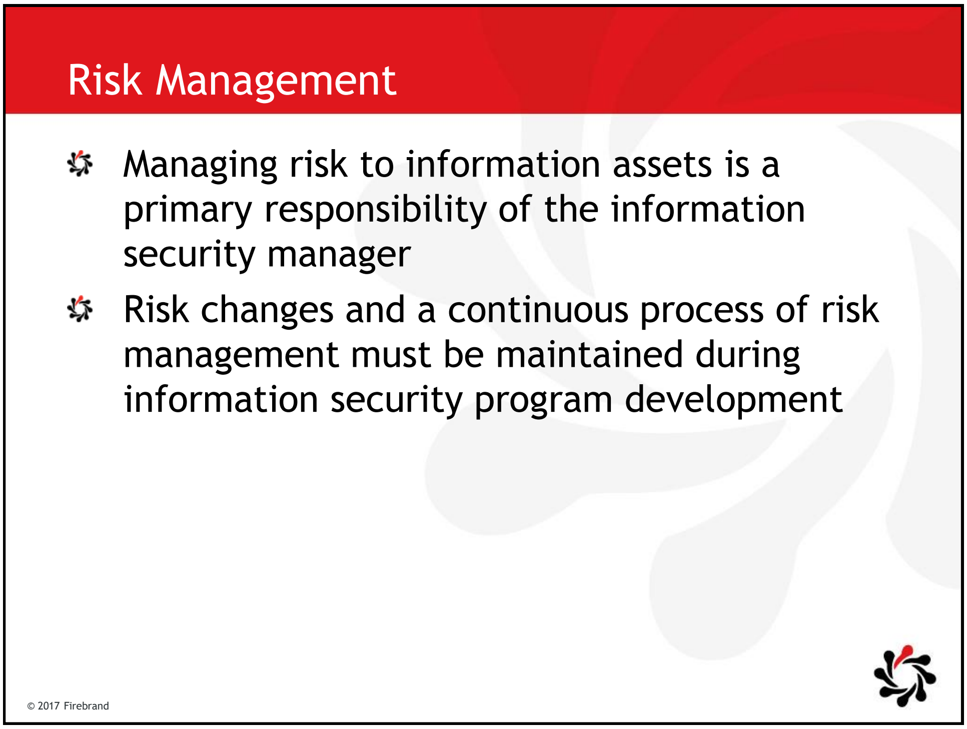
## Strategic Alignment

- Align security goals with the goals of the business
  - Requires regular interaction with business owners
- Consensus on:
  - Organisational risk
  - Selection of appropriate control objectives
  - Gaining agreement on acceptable risk
  - Definitions of financial, operational and other constraints



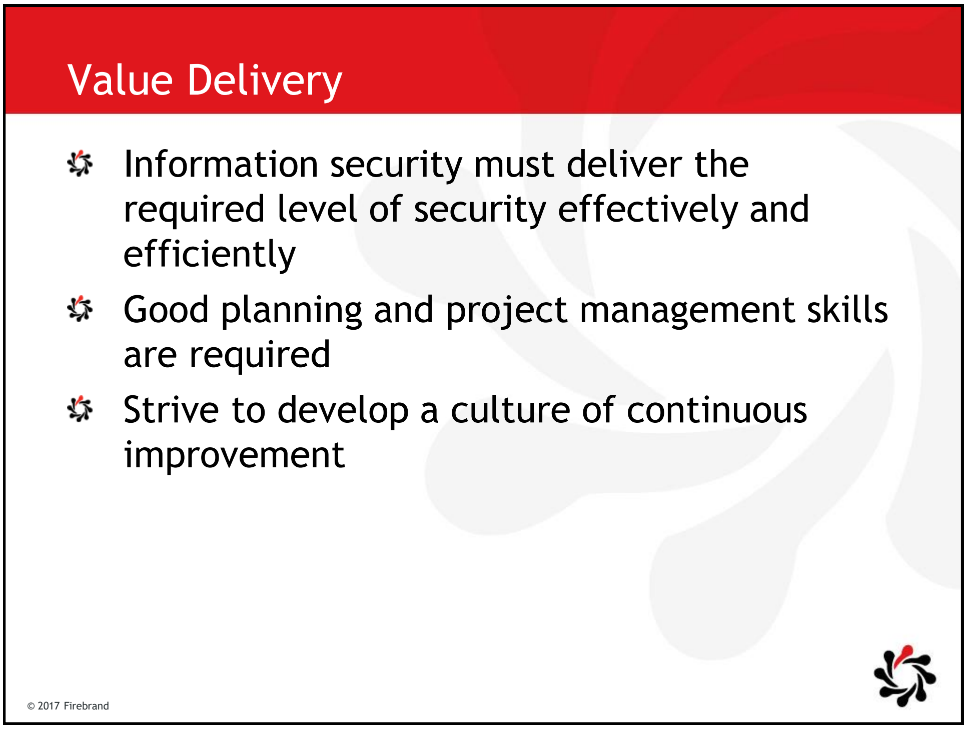
## Future Business Direction

- Strategic Alignment must consider:
  - Future business directions
  - Consider security solutions that are a good fit for current and future business initiatives



## Risk Management

- Managing risk to information assets is a primary responsibility of the information security manager
- Risk changes and a continuous process of risk management must be maintained during information security program development

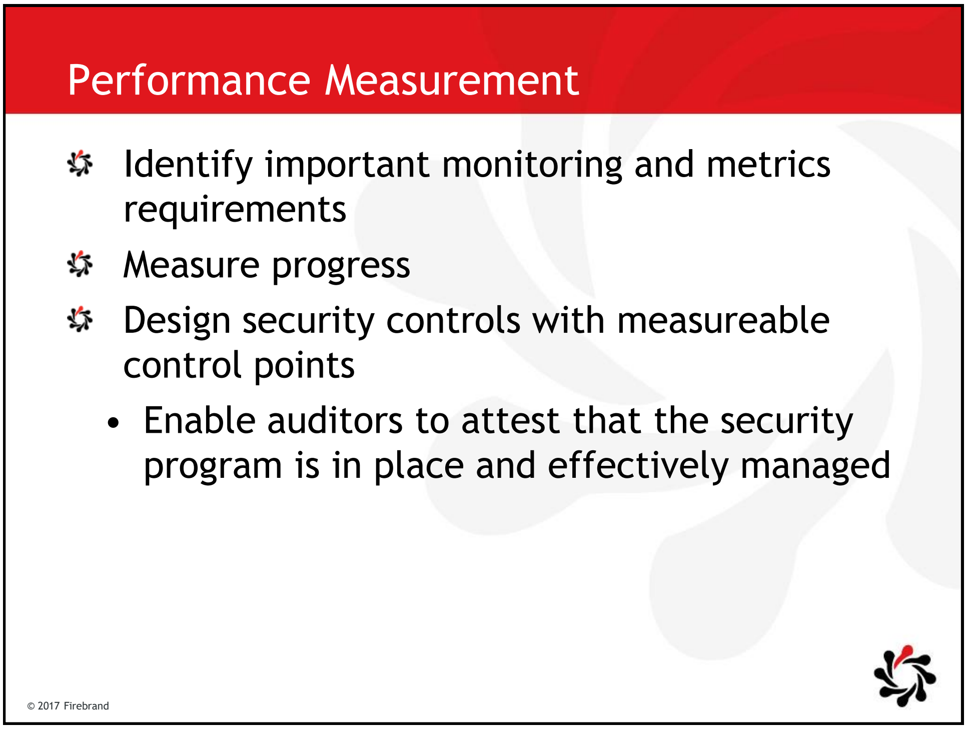


## Value Delivery

- Information security must deliver the required level of security effectively and efficiently
- Good planning and project management skills are required
- Strive to develop a culture of continuous improvement

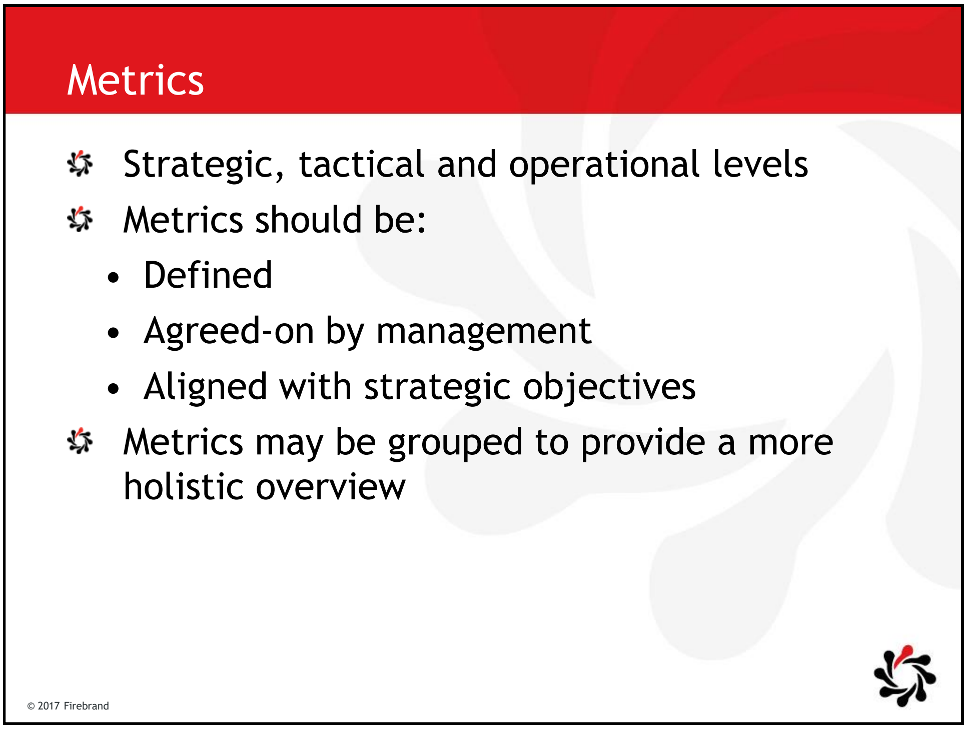
## Resource Management

- Developing and managing a security program requires:
  - People
  - Technology
  - Processes
- Use resources efficiently and effectively:
  - Human
  - Financial
  - Technical
  - Knowledge



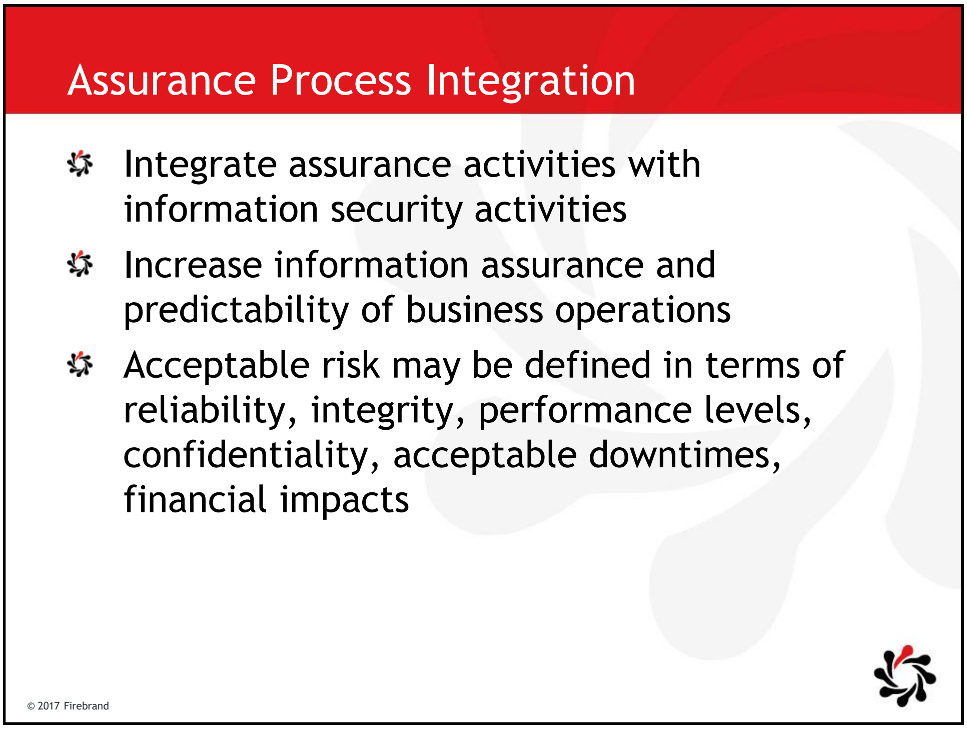
## Performance Measurement

- Identify important monitoring and metrics requirements
- Measure progress
- Design security controls with measureable control points
  - Enable auditors to attest that the security program is in place and effectively managed



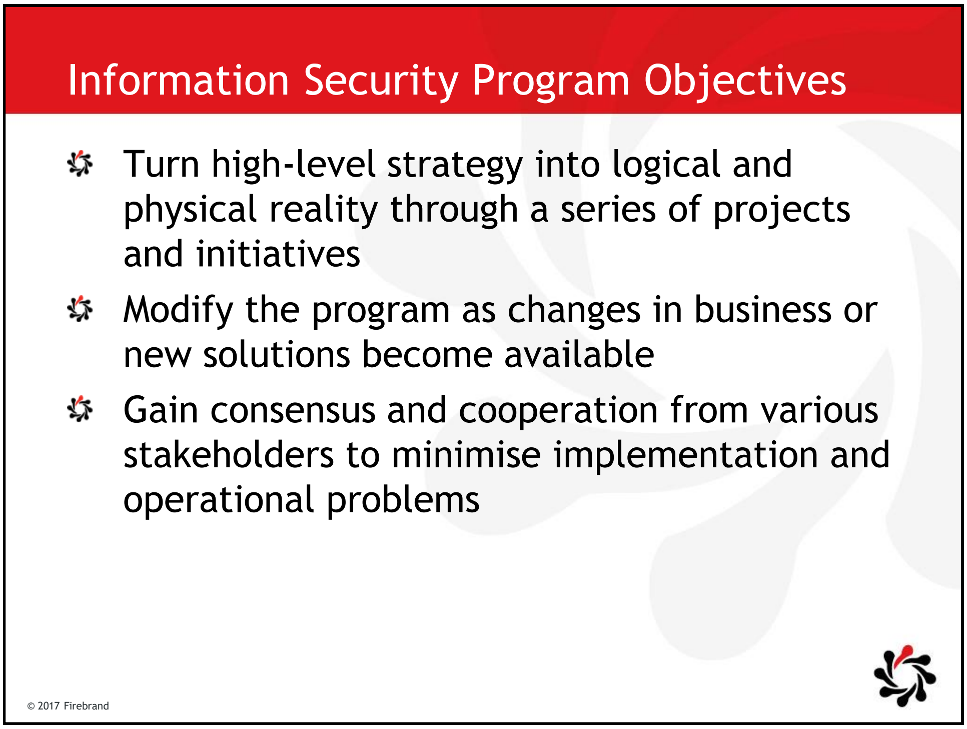
## Metrics

- Strategic, tactical and operational levels
- Metrics should be:
  - Defined
  - Agreed-on by management
  - Aligned with strategic objectives
- Metrics may be grouped to provide a more holistic overview



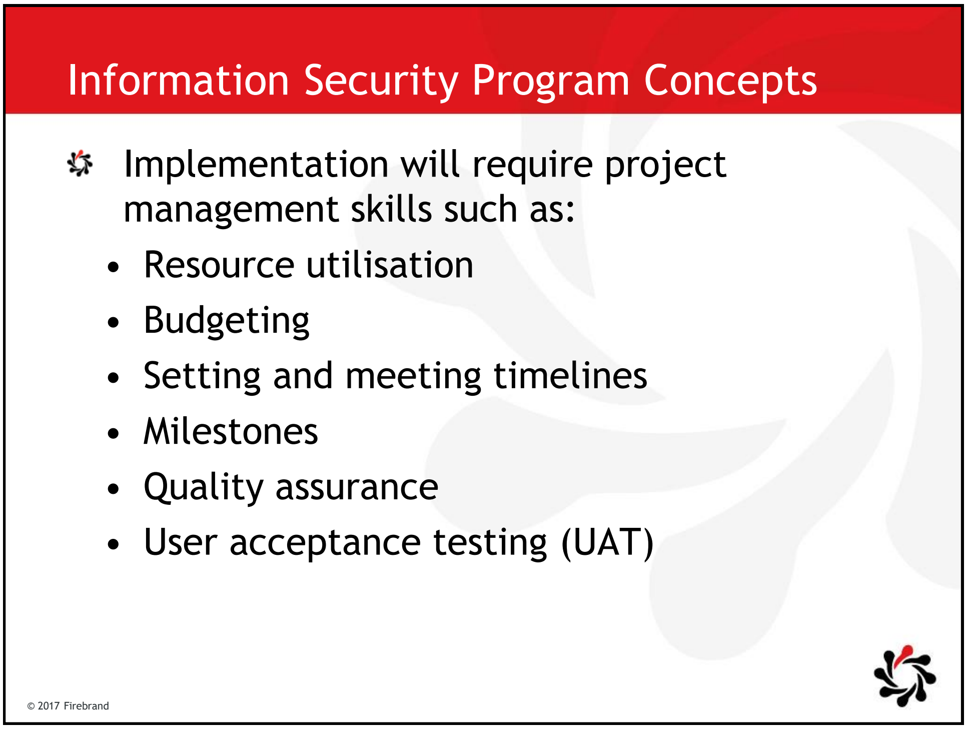
## Assurance Process Integration

- Integrate assurance activities with information security activities
- Increase information assurance and predictability of business operations
- Acceptable risk may be defined in terms of reliability, integrity, performance levels, confidentiality, acceptable downtimes, financial impacts



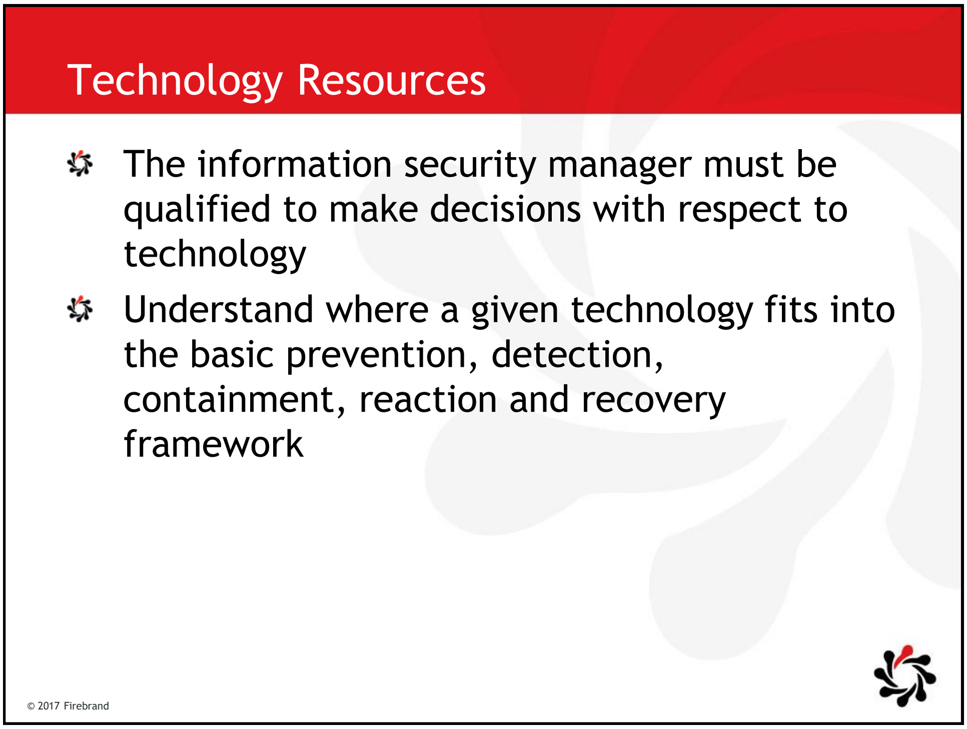
## Information Security Program Objectives

- Turn high-level strategy into logical and physical reality through a series of projects and initiatives
- Modify the program as changes in business or new solutions become available
- Gain consensus and cooperation from various stakeholders to minimise implementation and operational problems



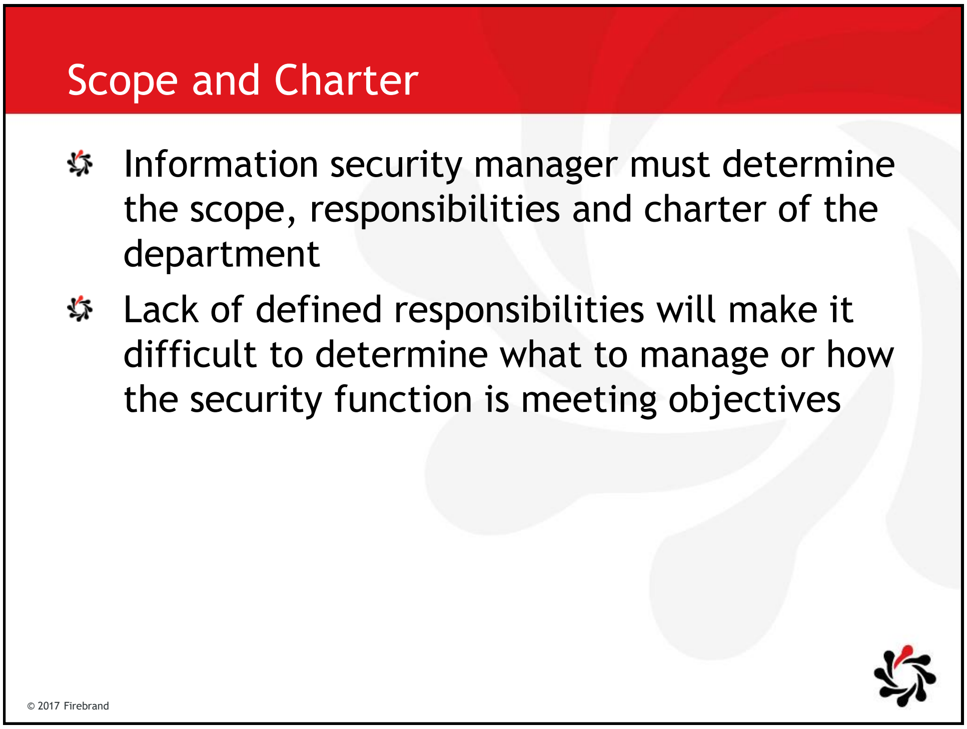
## Information Security Program Concepts

- Implementation will require project management skills such as:
  - Resource utilisation
  - Budgeting
  - Setting and meeting timelines
  - Milestones
  - Quality assurance
  - User acceptance testing (UAT)



## Technology Resources

- The information security manager must be qualified to make decisions with respect to technology
- Understand where a given technology fits into the basic prevention, detection, containment, reaction and recovery framework



## Scope and Charter

- Information security manager must determine the scope, responsibilities and charter of the department
- Lack of defined responsibilities will make it difficult to determine what to manage or how the security function is meeting objectives

## Chain of Command

- Where should security fit into the organisation?
  - Avoid conflicts of interest
  - Security is primarily an internal regulatory function – and should not report to the entities that it is supposed to regulate
- Understand current state of the security function in the organisation
  - Review audits, incidents and other reports

## Scope

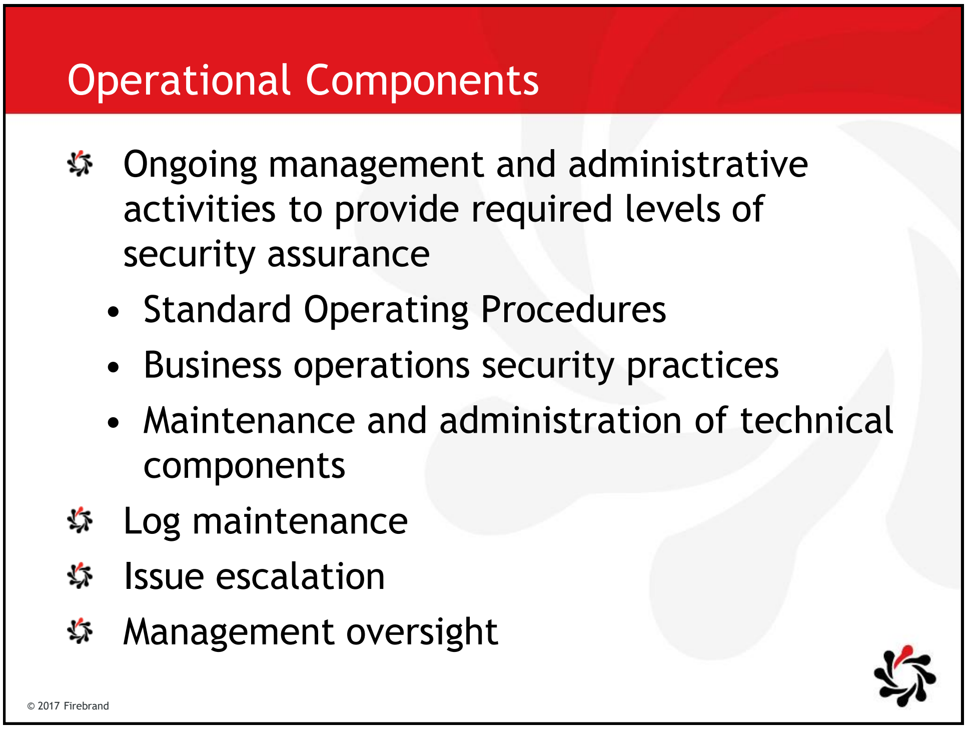
- Established through the development of a strategy in combination with risk management
- Management support and risk management determine the charter
- Security will impact the organisation’s established way of doing things
  - Integrate security into existing processes
  - Will result in some resistance to security

## Information Security Management Framework

- Conceptual representation of the security management structure
- Defines the components of the structure:
  - Technical
  - Operational
  - Managerial
  - Administrative
  - Educational

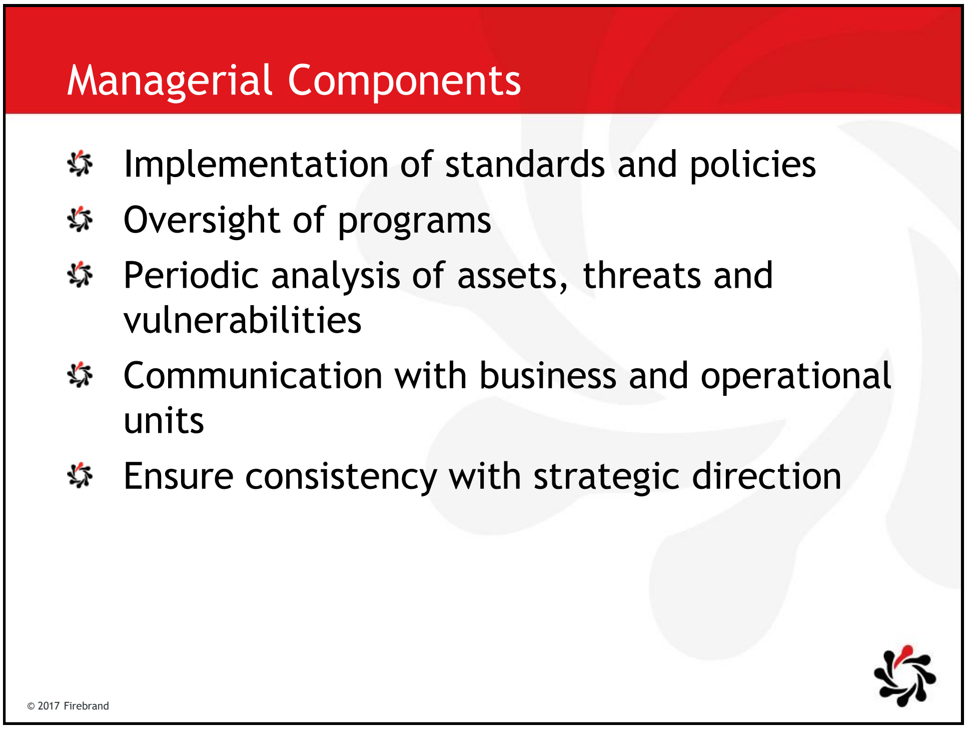
## Technical Components

- Configuration
- Monitoring
- Maintenance
- Operation
- All technical components must have an identified owner for responsibility and accountability



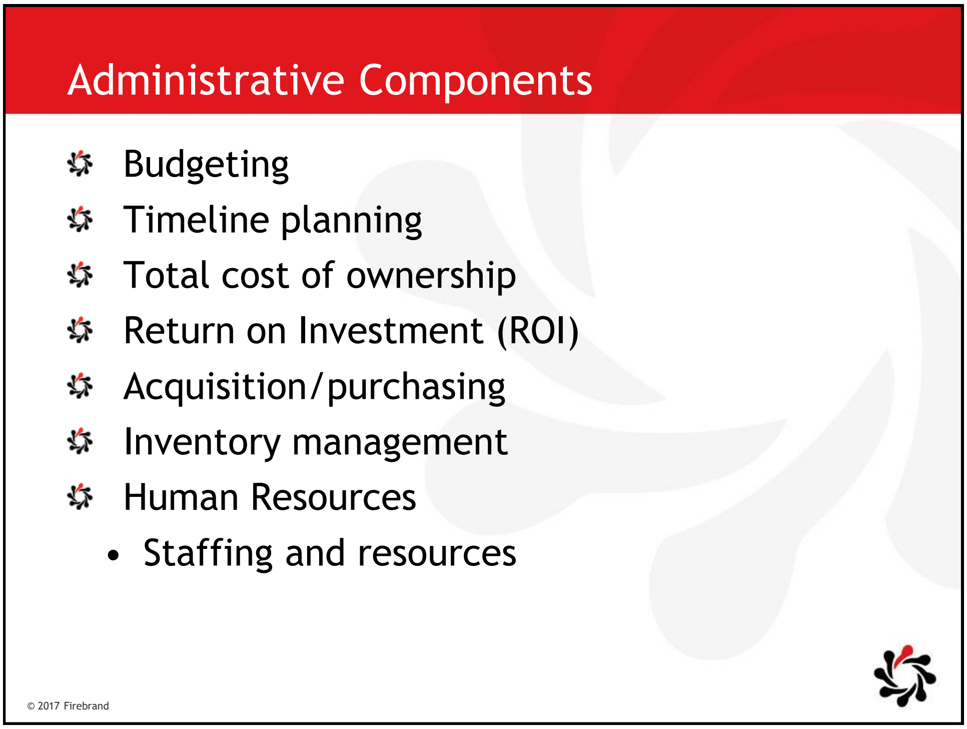
## Operational Components

- Ongoing management and administrative activities to provide required levels of security assurance
  - Standard Operating Procedures
  - Business operations security practices
  - Maintenance and administration of technical components
- Log maintenance
- Issue escalation
- Management oversight



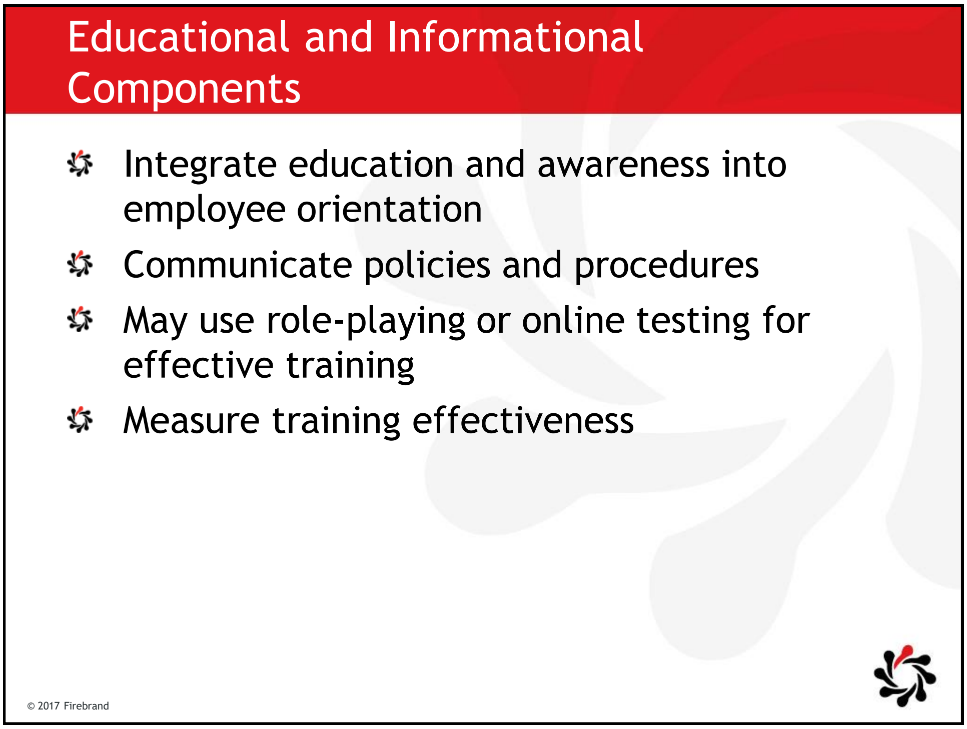
## Managerial Components

- Implementation of standards and policies
- Oversight of programs
- Periodic analysis of assets, threats and vulnerabilities
- Communication with business and operational units
- Ensure consistency with strategic direction



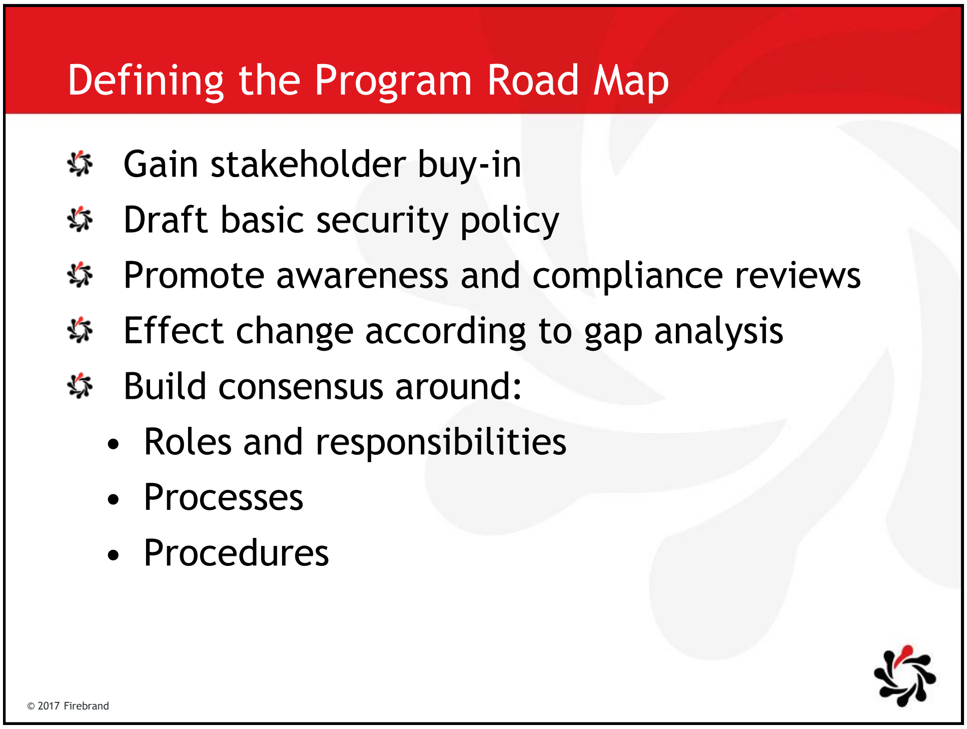
## Administrative Components

- Budgeting
- Timeline planning
- Total cost of ownership
- Return on Investment (ROI)
- Acquisition/purchasing
- Inventory management
- Human Resources
  - Staffing and resources



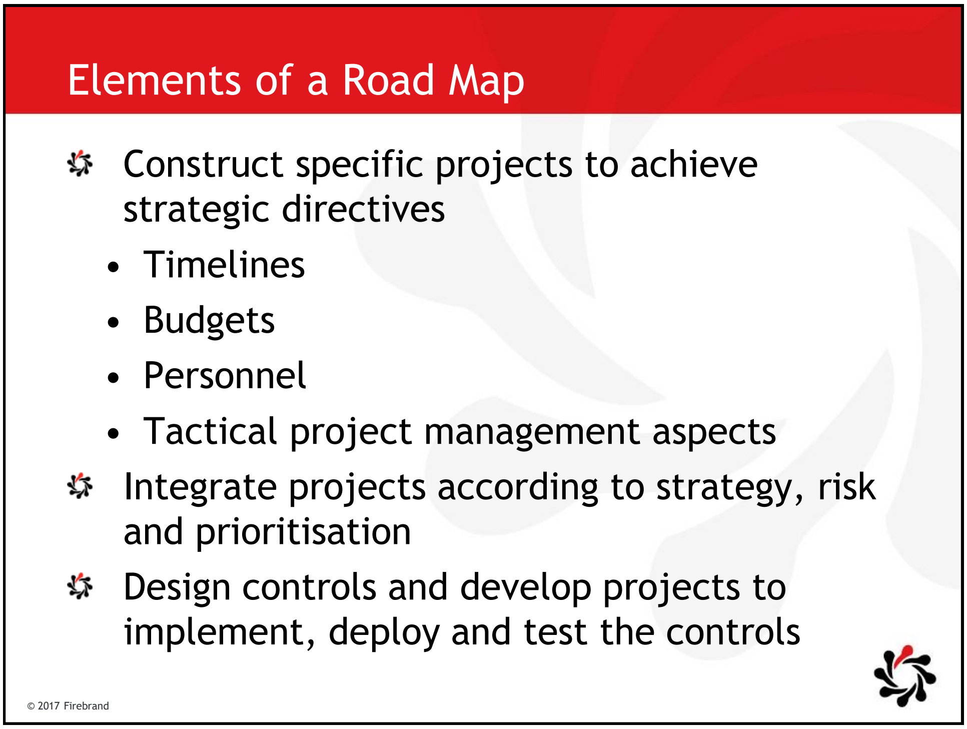
## Educational and Informational Components

- Integrate education and awareness into employee orientation
- Communicate policies and procedures
- May use role-playing or online testing for effective training
- Measure training effectiveness



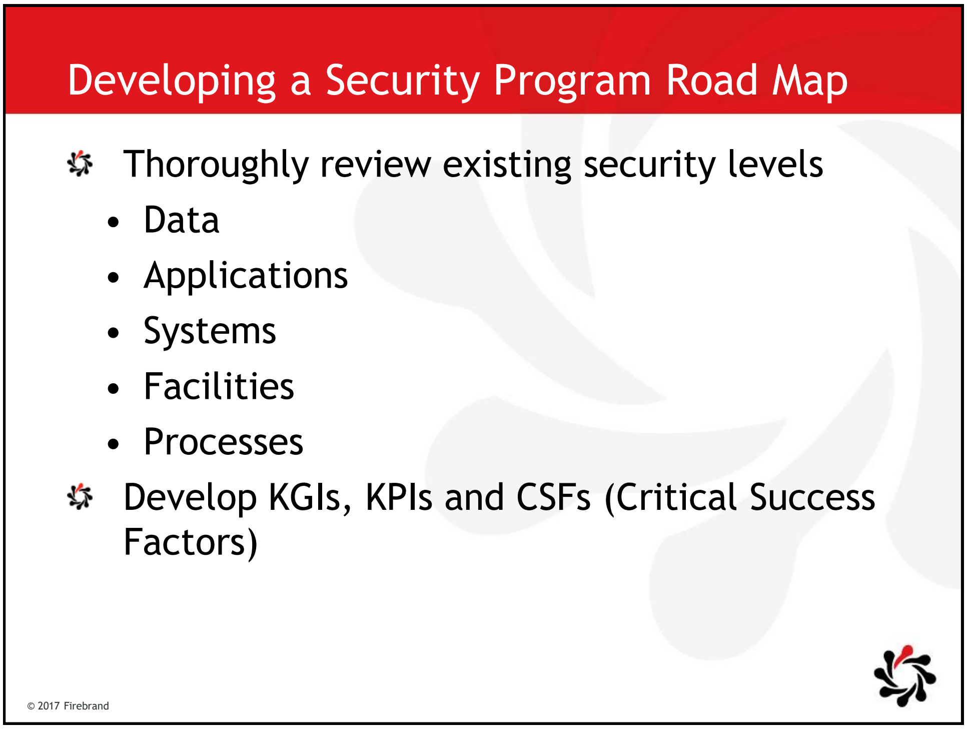
## Defining the Program Road Map

- Gain stakeholder buy-in
- Draft basic security policy
- Promote awareness and compliance reviews
- Effect change according to gap analysis
- Build consensus around:
  - Roles and responsibilities
  - Processes
  - Procedures



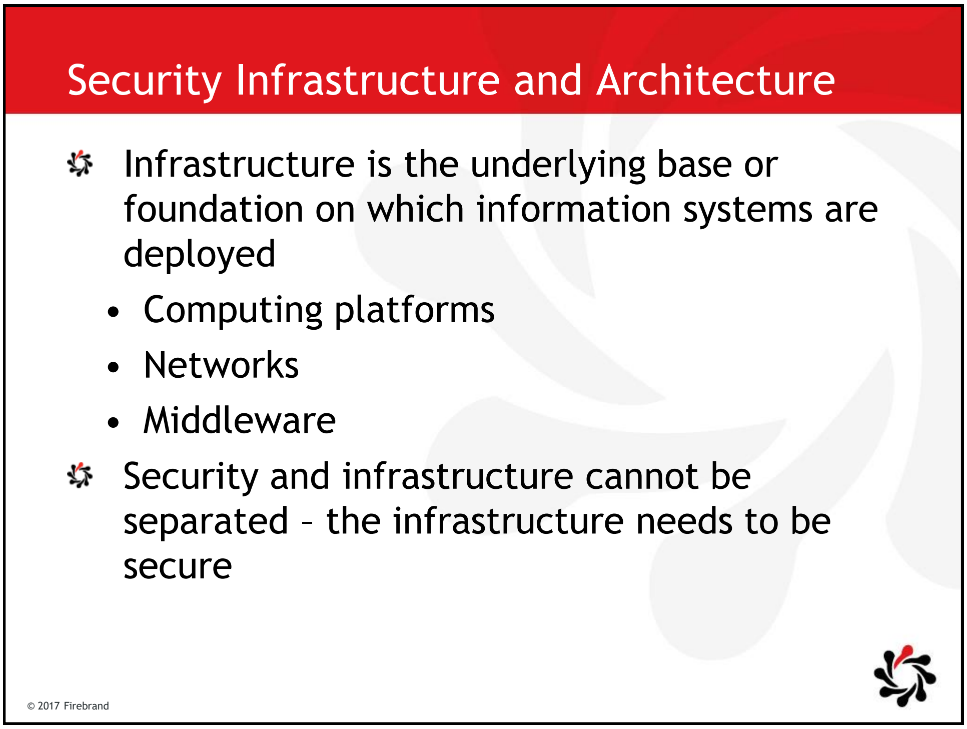
## Elements of a Road Map

- Construct specific projects to achieve strategic directives
  - Timelines
  - Budgets
  - Personnel
  - Tactical project management aspects
- Integrate projects according to strategy, risk and prioritisation
- Design controls and develop projects to implement, deploy and test the controls



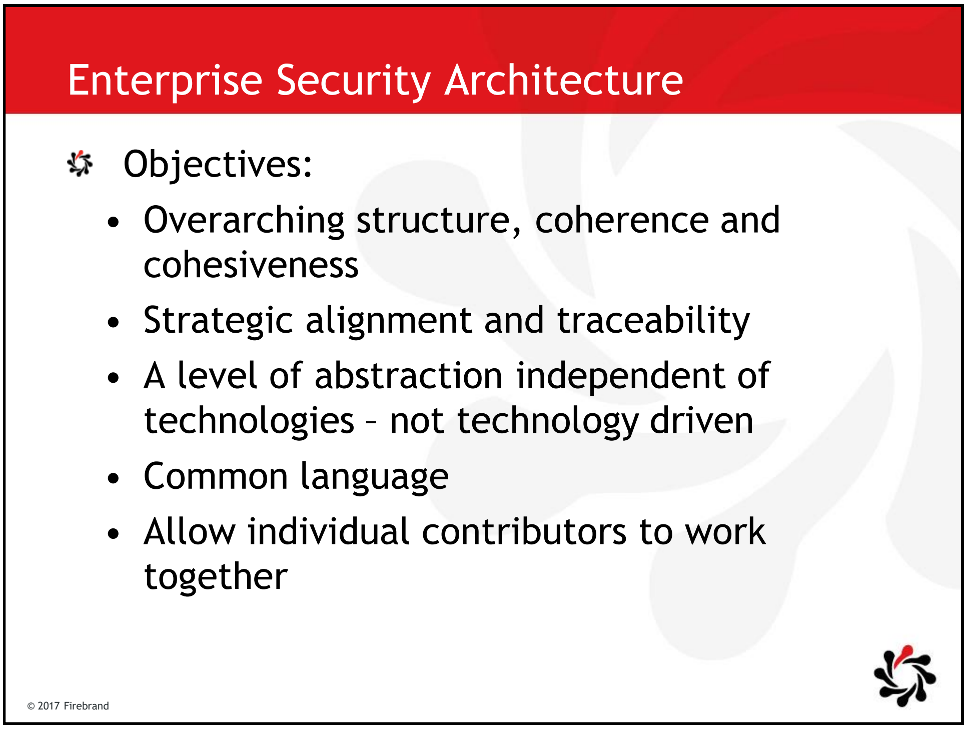
## Developing a Security Program Road Map

- Thoroughly review existing security levels
  - Data
  - Applications
  - Systems
  - Facilities
  - Processes
- Develop KGIs, KPIs and CSFs (Critical Success Factors)



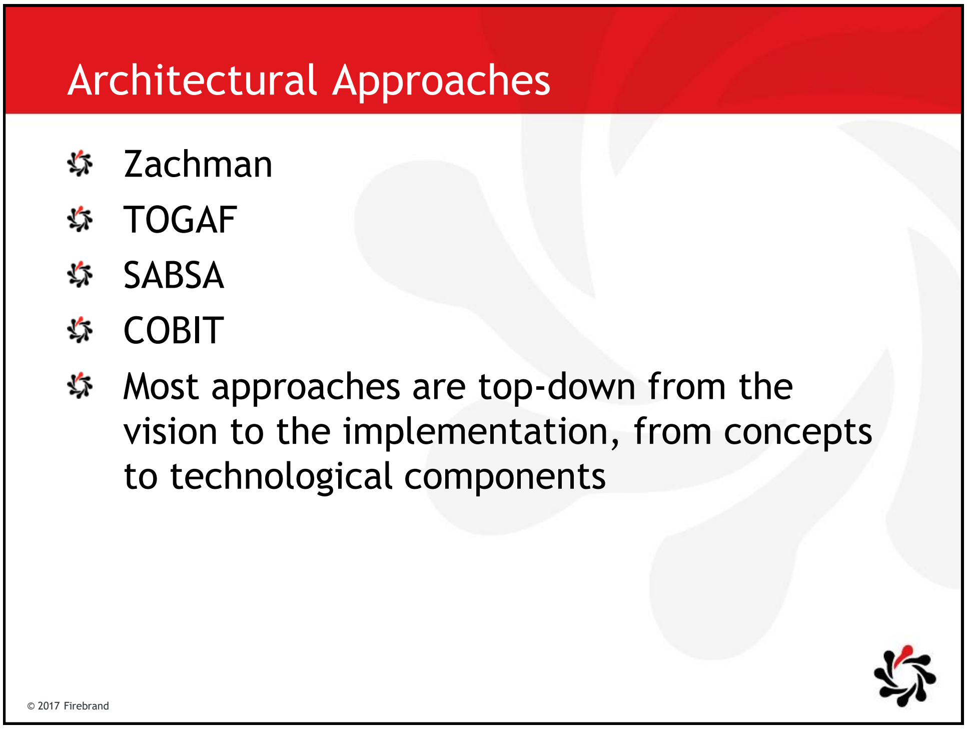
## Security Infrastructure and Architecture

- Infrastructure is the underlying base or foundation on which information systems are deployed
  - Computing platforms
  - Networks
  - Middleware
- Security and infrastructure cannot be separated – the infrastructure needs to be secure



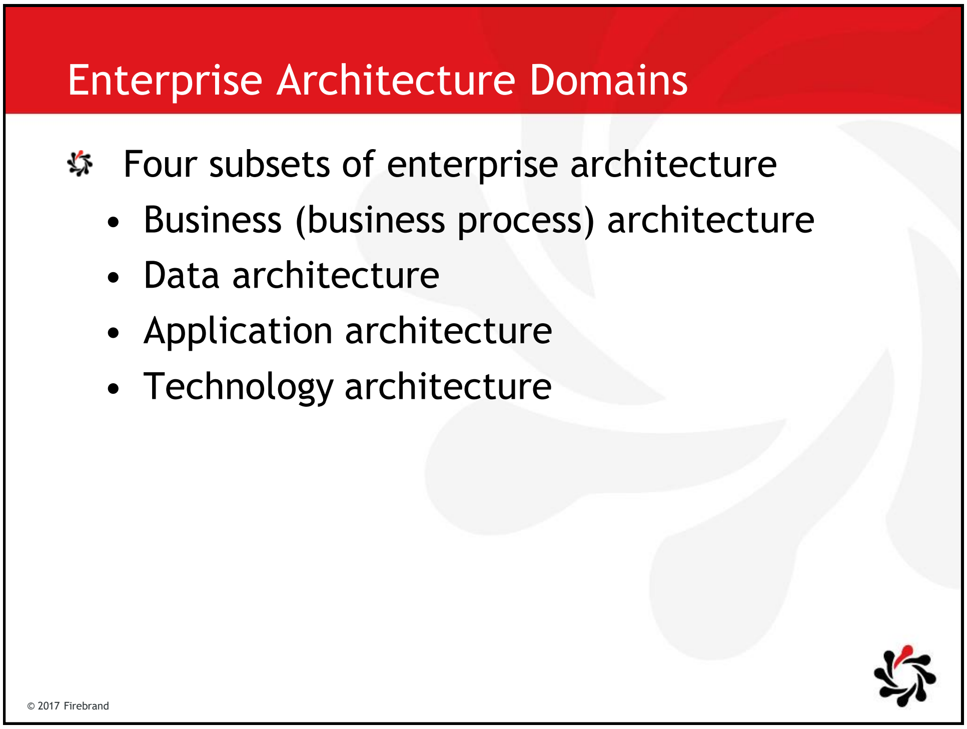
## Enterprise Security Architecture

- Objectives:
  - Overarching structure, coherence and cohesiveness
  - Strategic alignment and traceability
  - A level of abstraction independent of technologies – not technology driven
  - Common language
  - Allow individual contributors to work together



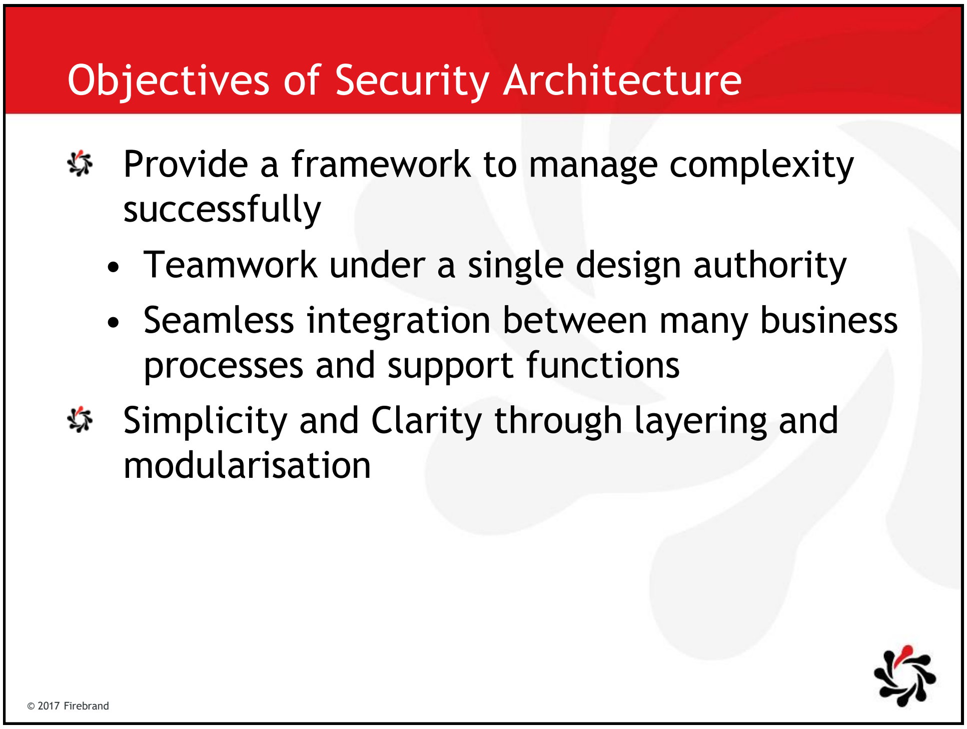
## Architectural Approaches

- Zachman
- TOGAF
- SABSA
- COBIT
- Most approaches are top-down from the vision to the implementation, from concepts to technological components



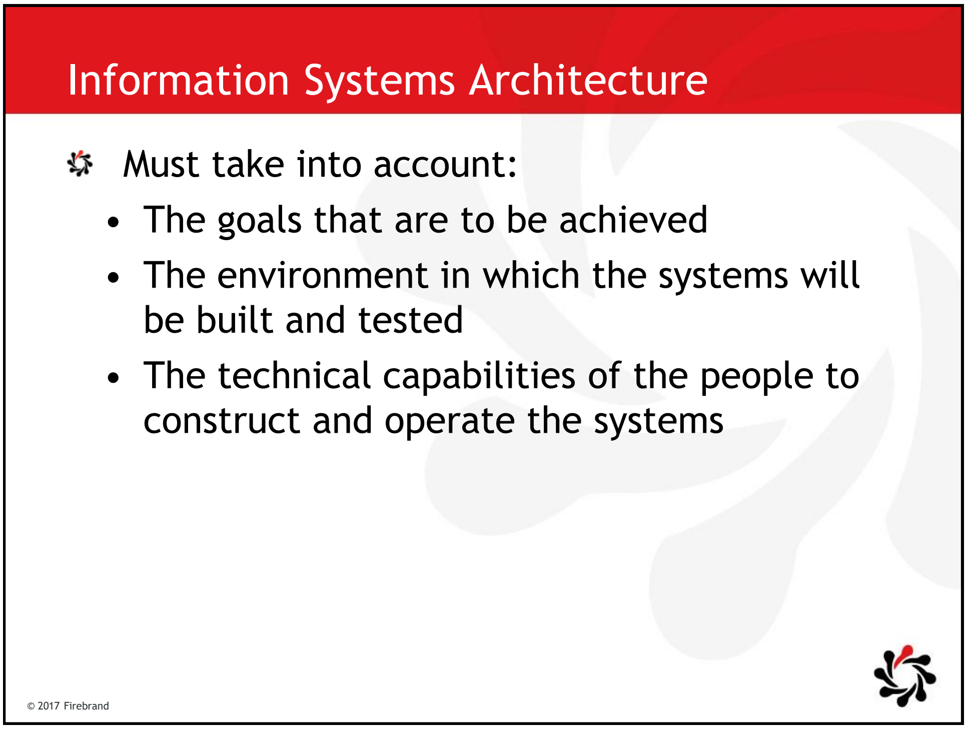
## Enterprise Architecture Domains

- Four subsets of enterprise architecture
  - Business (business process) architecture
  - Data architecture
  - Application architecture
  - Technology architecture



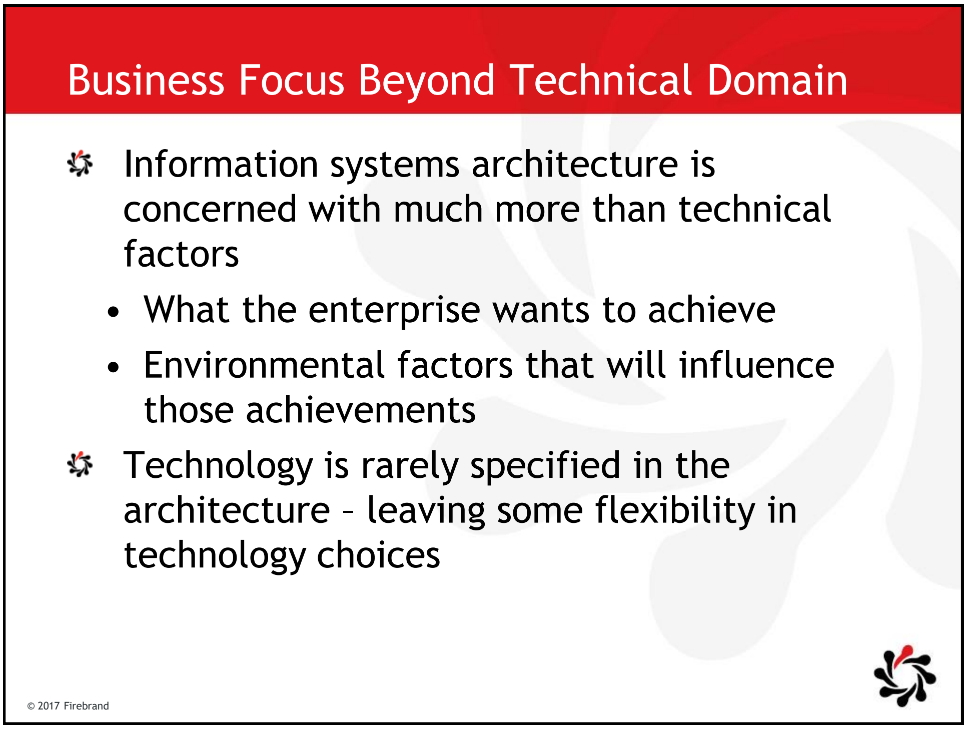
## Objectives of Security Architecture

- Provide a framework to manage complexity successfully
  - Teamwork under a single design authority
  - Seamless integration between many business processes and support functions
- Simplicity and Clarity through layering and modularisation



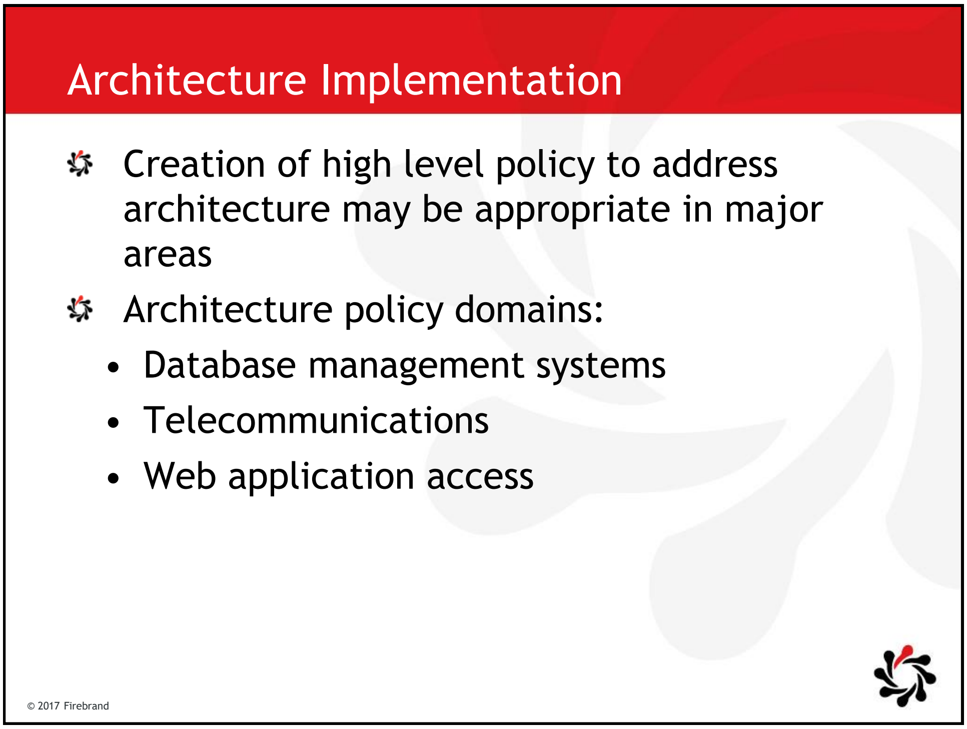
## Information Systems Architecture

- Must take into account:
  - The goals that are to be achieved
  - The environment in which the systems will be built and tested
  - The technical capabilities of the people to construct and operate the systems



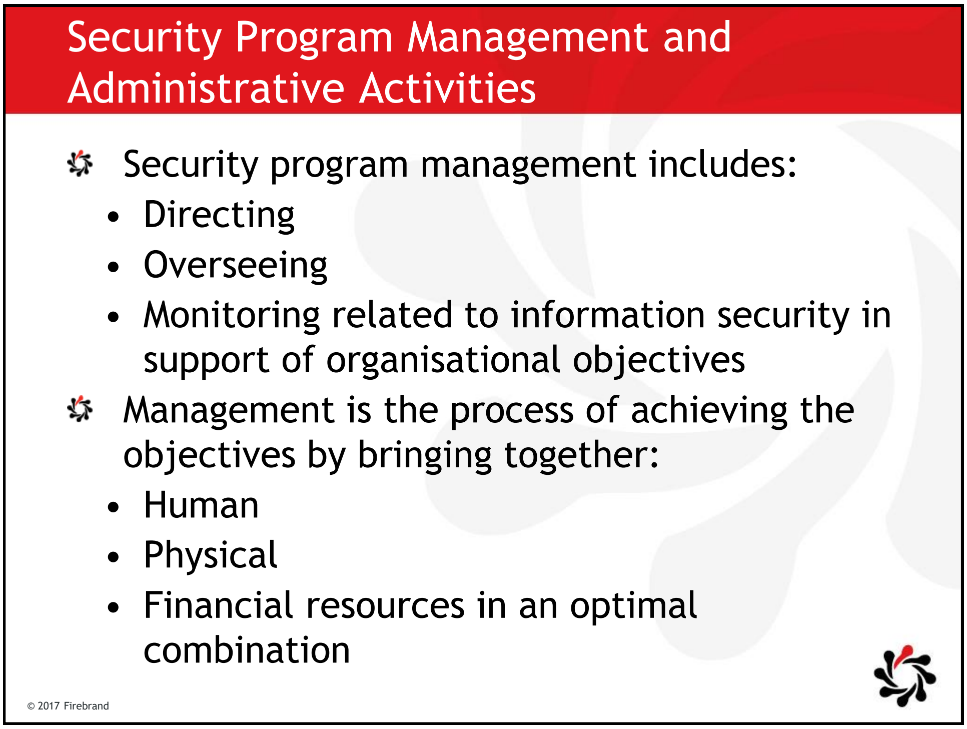
## Business Focus Beyond Technical Domain

- Information systems architecture is concerned with much more than technical factors
  - What the enterprise wants to achieve
  - Environmental factors that will influence those achievements
- Technology is rarely specified in the architecture – leaving some flexibility in technology choices



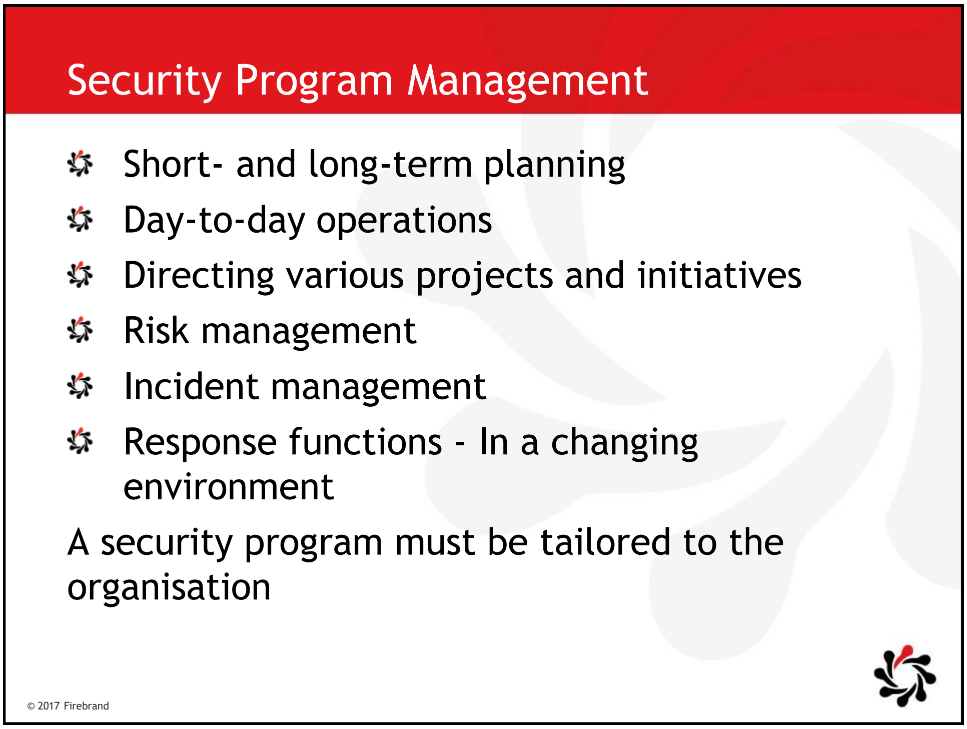
## Architecture Implementation

- Creation of high level policy to address architecture may be appropriate in major areas
- Architecture policy domains:
  - Database management systems
  - Telecommunications
  - Web application access



## Security Program Management and Administrative Activities

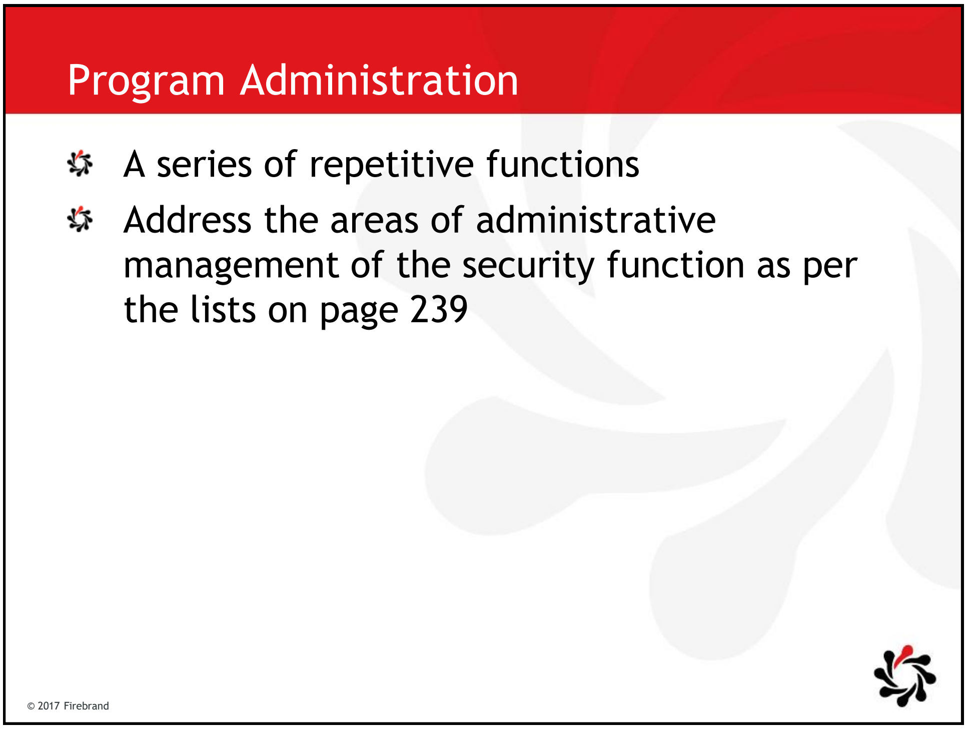
- Security program management includes:
  - Directing
  - Overseeing
  - Monitoring related to information security in support of organisational objectives
- Management is the process of achieving the objectives by bringing together:
  - Human
  - Physical
  - Financial resources in an optimal combination



## Security Program Management

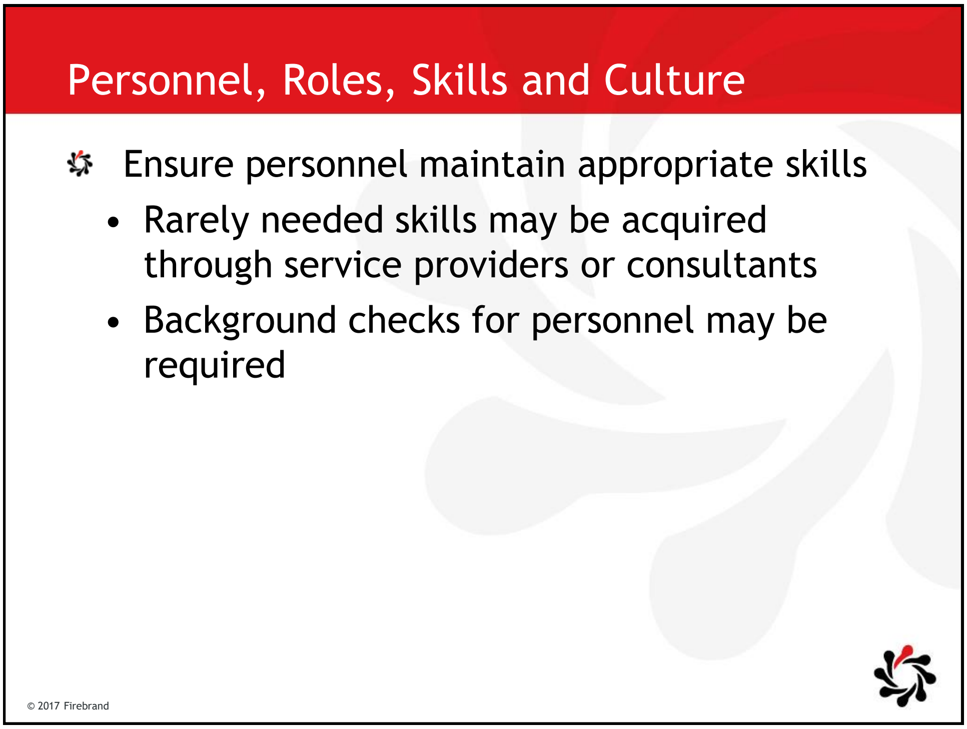
- Short- and long-term planning
- Day-to-day operations
- Directing various projects and initiatives
- Risk management
- Incident management
- Response functions - In a changing environment

A security program must be tailored to the organisation



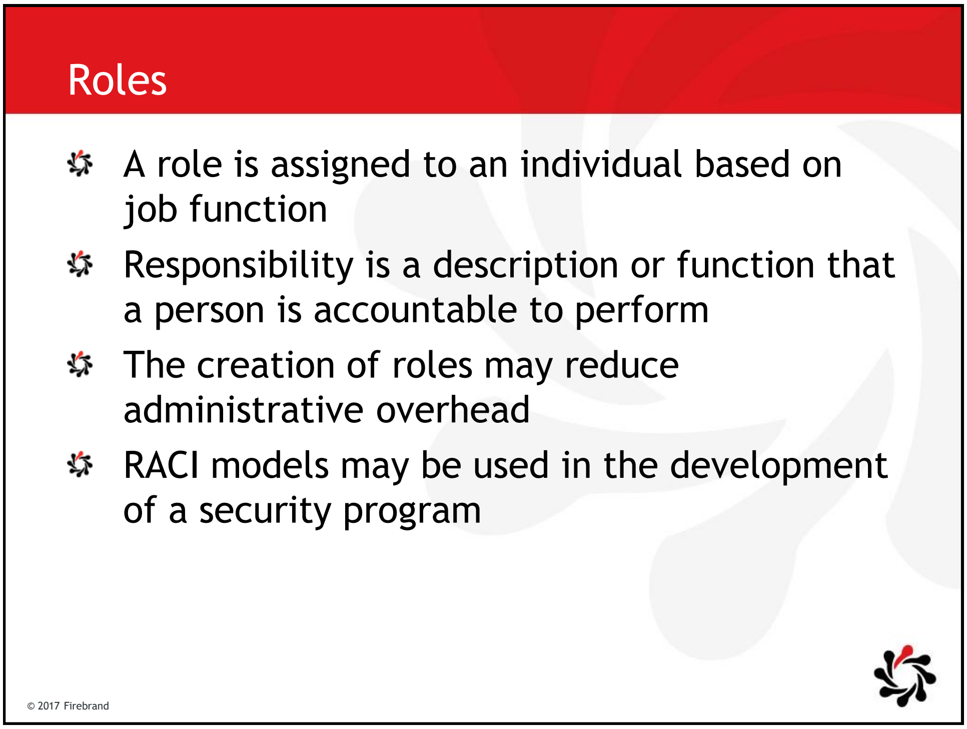
## Program Administration

- A series of repetitive functions
- Address the areas of administrative management of the security function as per the lists on page 239



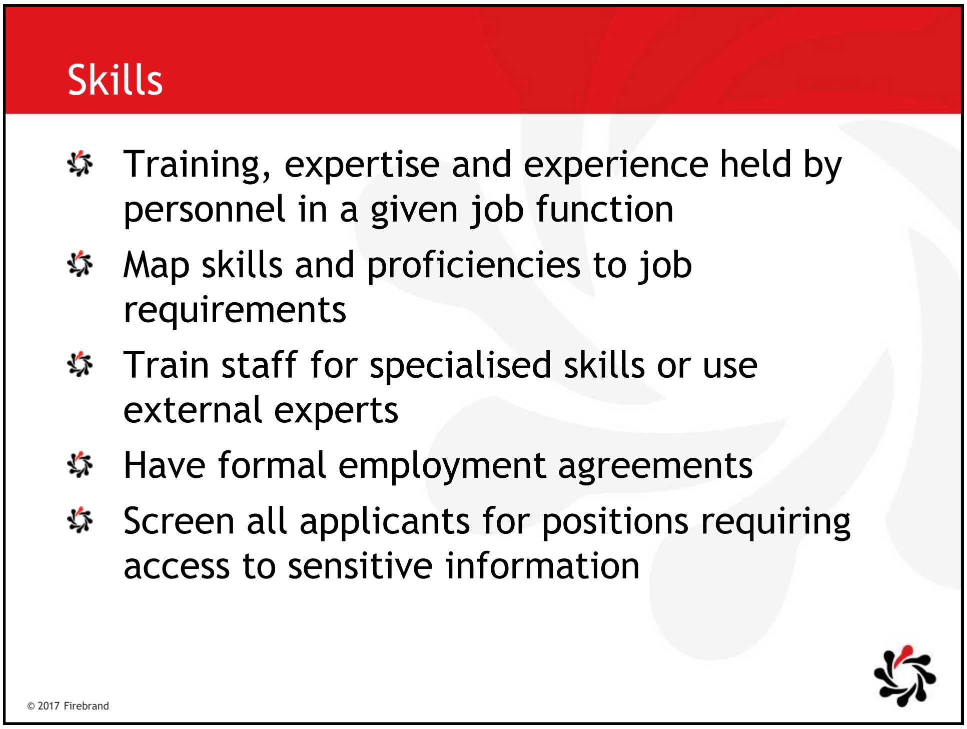
## Personnel, Roles, Skills and Culture

- Ensure personnel maintain appropriate skills
  - Rarely needed skills may be acquired through service providers or consultants
  - Background checks for personnel may be required



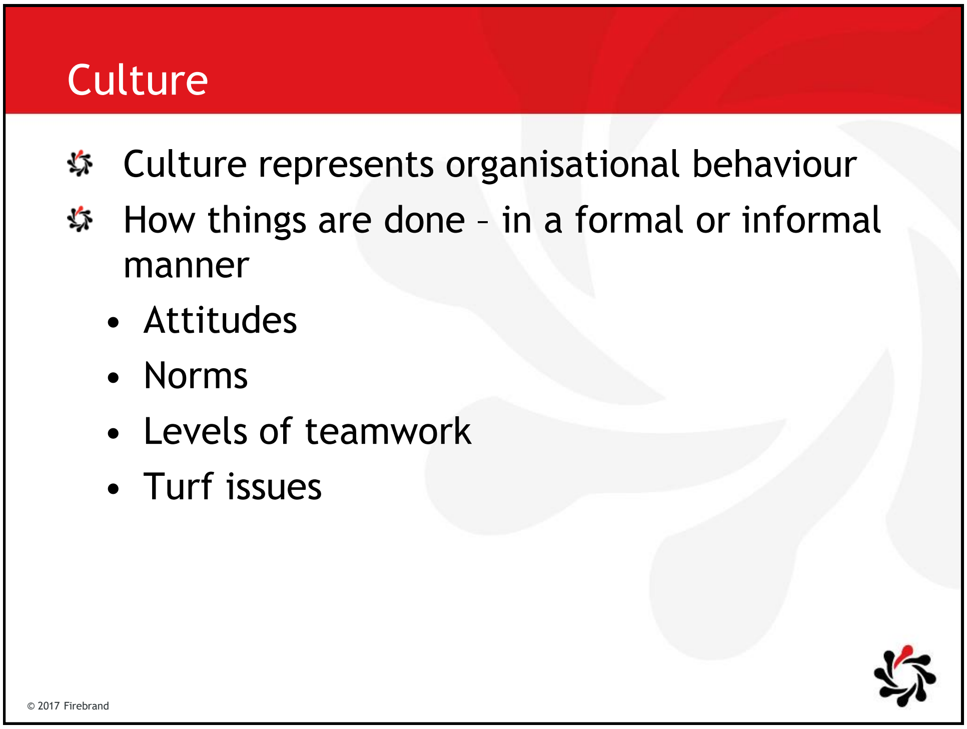
## Roles

- A role is assigned to an individual based on job function
- Responsibility is a description or function that a person is accountable to perform
- The creation of roles may reduce administrative overhead
- RACI models may be used in the development of a security program



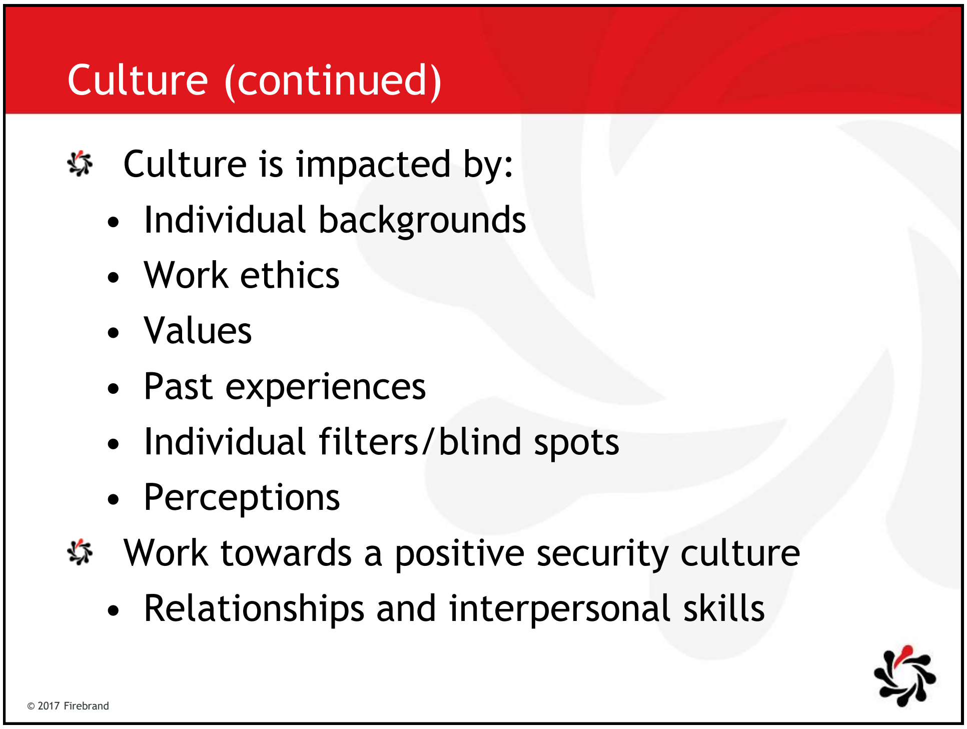
## Skills

- Training, expertise and experience held by personnel in a given job function
- Map skills and proficiencies to job requirements
- Train staff for specialised skills or use external experts
- Have formal employment agreements
- Screen all applicants for positions requiring access to sensitive information



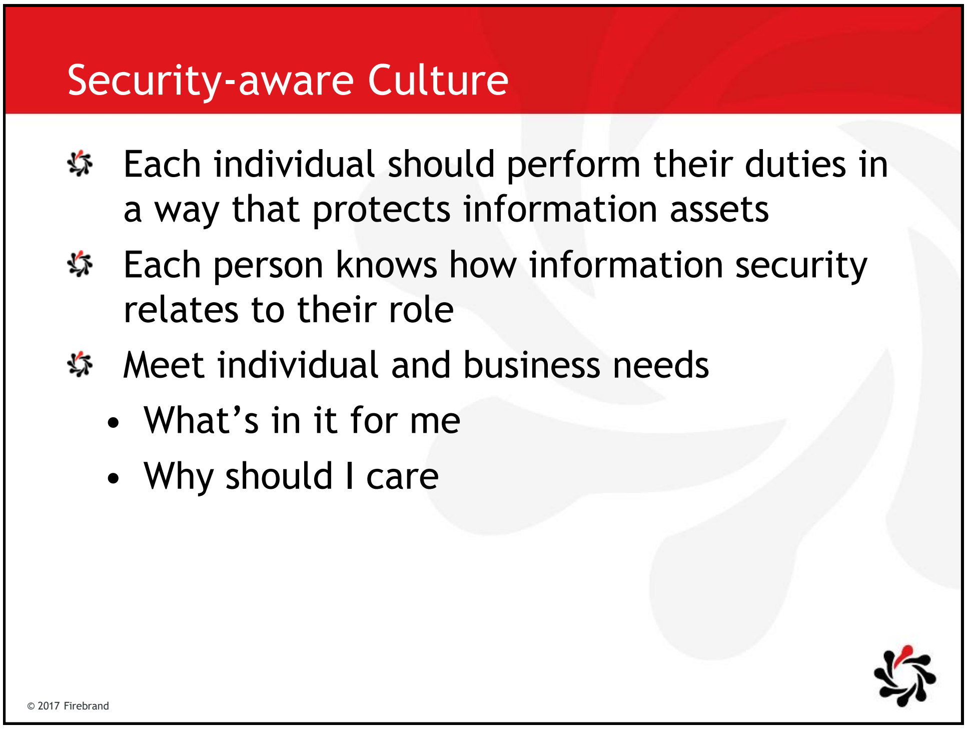
## Culture

- Culture represents organisational behaviour
- How things are done – in a formal or informal manner
  - Attitudes
  - Norms
  - Levels of teamwork
  - Turf issues



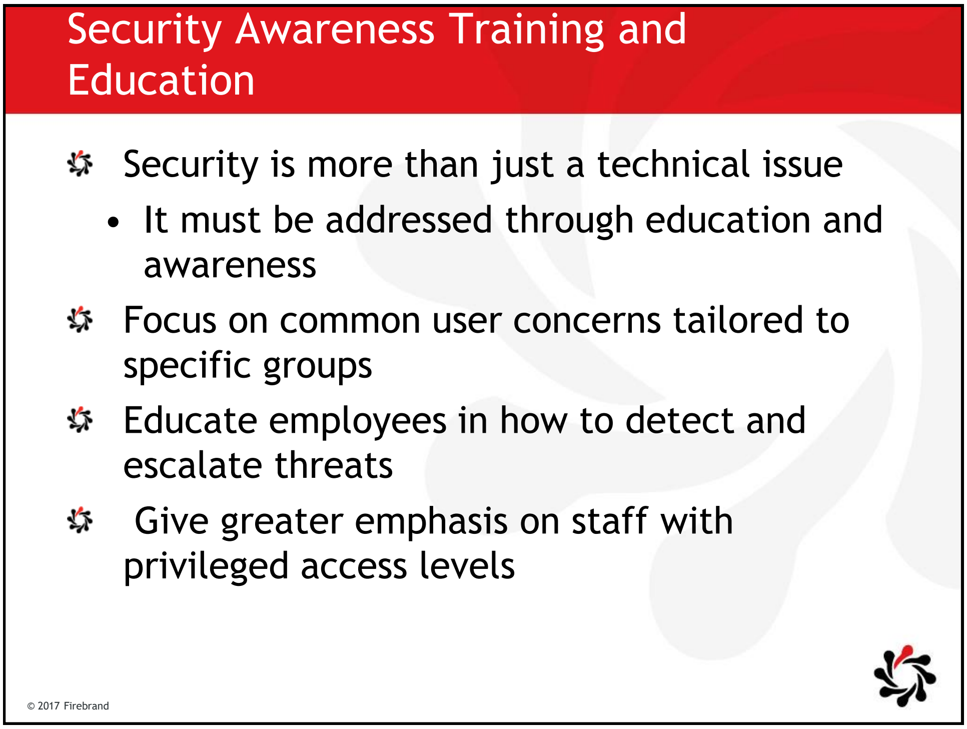
## Culture (continued)

- Culture is impacted by:
  - Individual backgrounds
  - Work ethics
  - Values
  - Past experiences
  - Individual filters/blind spots
  - Perceptions
- Work towards a positive security culture
  - Relationships and interpersonal skills



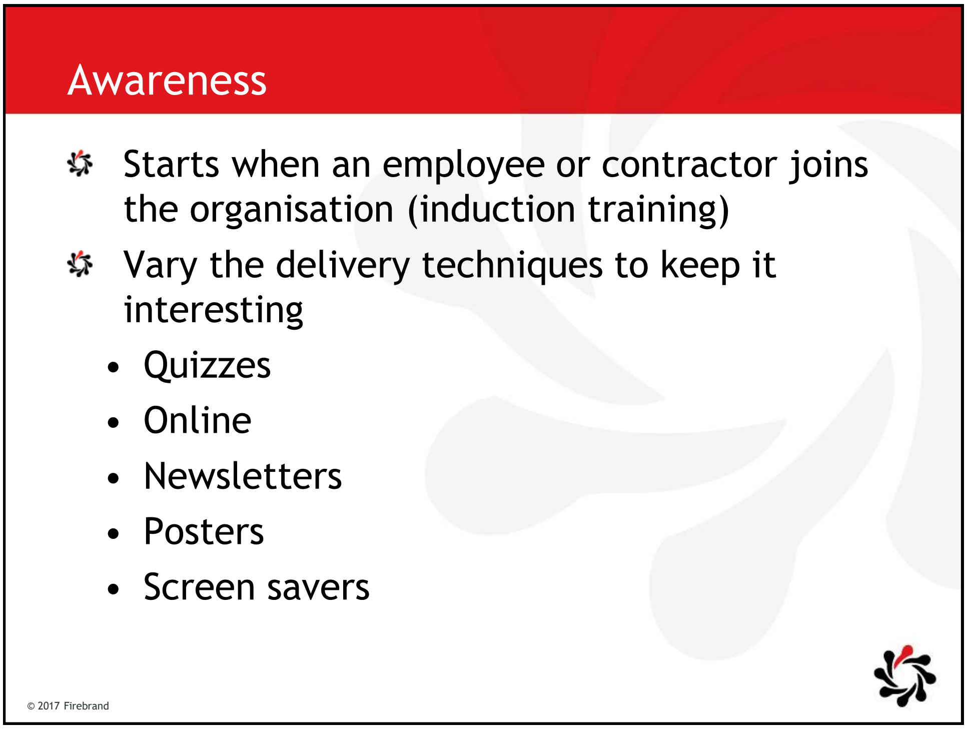
## Security-aware Culture

- Each individual should perform their duties in a way that protects information assets
- Each person knows how information security relates to their role
- Meet individual and business needs
  - What’s in it for me
  - Why should I care



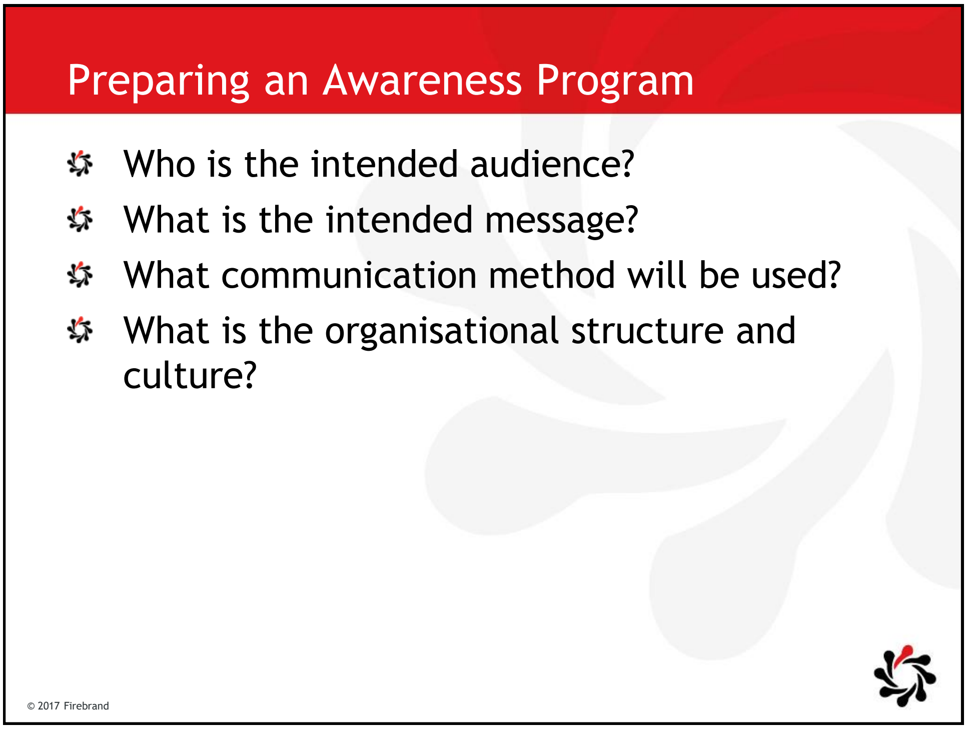
## Security Awareness Training and Education

- Security is more than just a technical issue
  - It must be addressed through education and awareness
- Focus on common user concerns tailored to specific groups
- Educate employees in how to detect and escalate threats
- Give greater emphasis on staff with privileged access levels



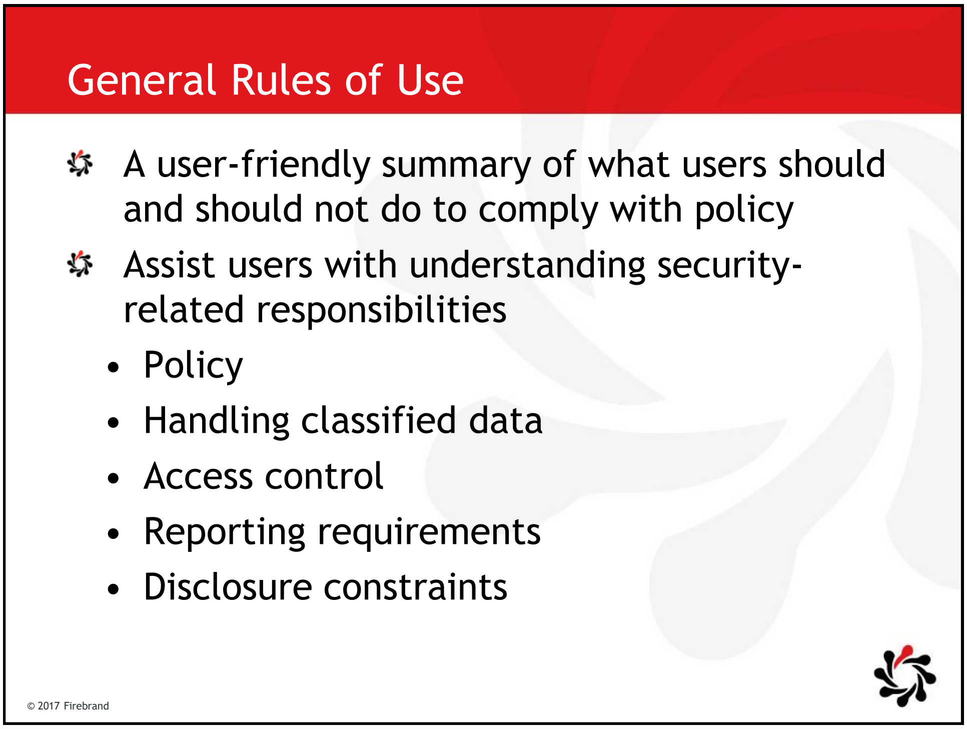
## Awareness

- Starts when an employee or contractor joins the organisation (induction training)
- Vary the delivery techniques to keep it interesting
  - Quizzes
  - Online
  - Newsletters
  - Posters
  - Screen savers



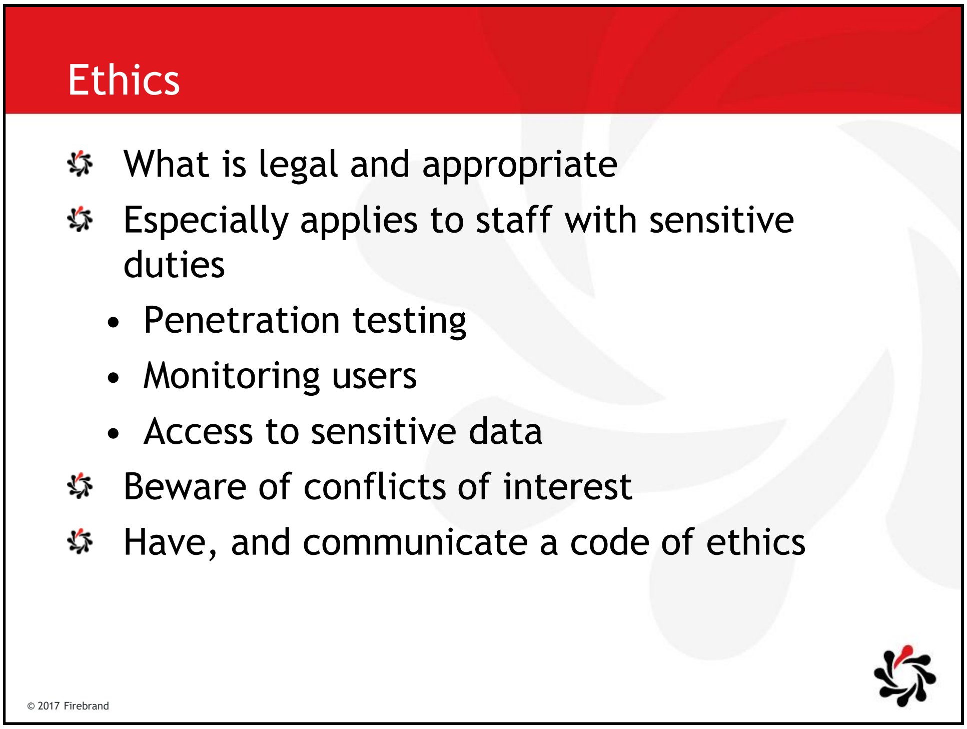
## Preparing an Awareness Program

- Who is the intended audience?
- What is the intended message?
- What communication method will be used?
- What is the organisational structure and culture?



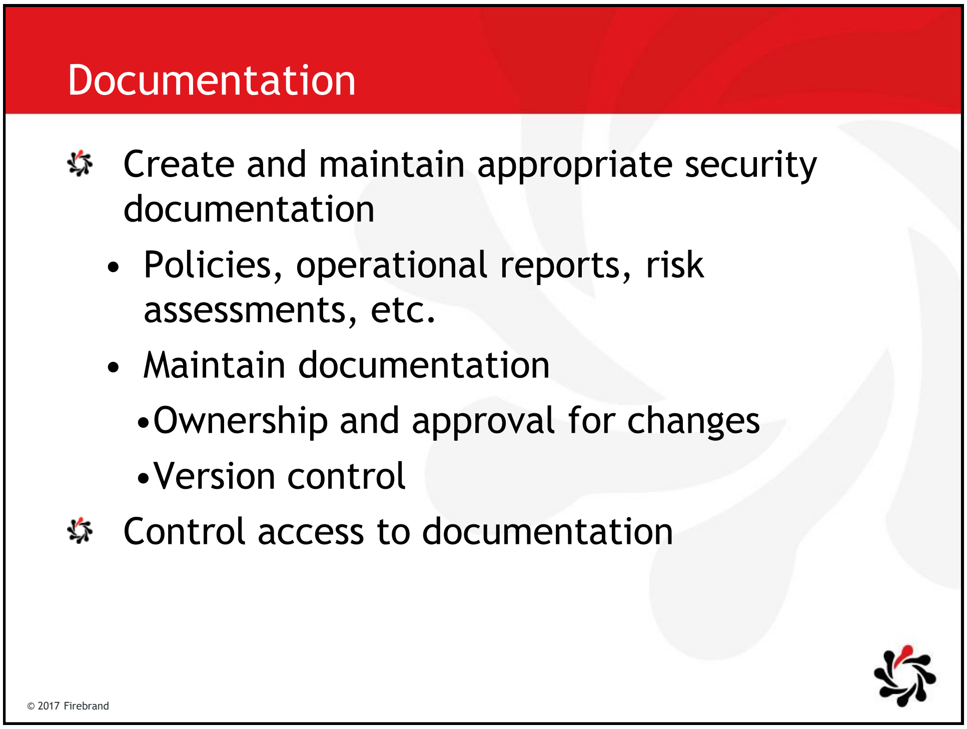
## General Rules of Use

- A user-friendly summary of what users should and should not do to comply with policy
- Assist users with understanding security-related responsibilities
  - Policy
  - Handling classified data
  - Access control
  - Reporting requirements
  - Disclosure constraints



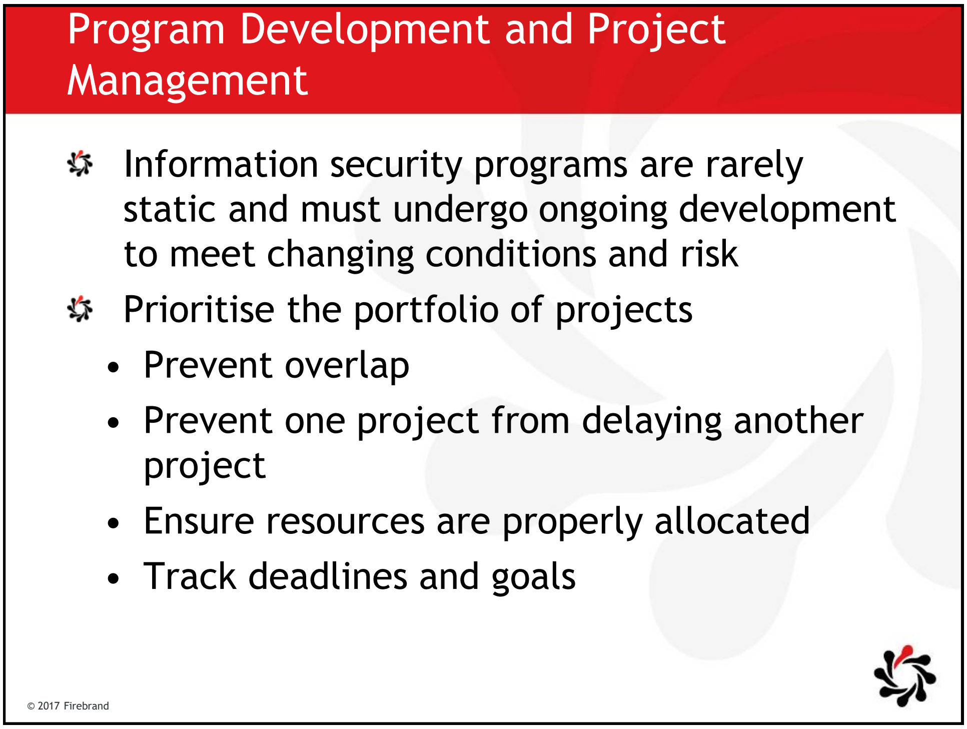
## Ethics

- What is legal and appropriate
- Especially applies to staff with sensitive duties
  - Penetration testing
  - Monitoring users
  - Access to sensitive data
- Beware of conflicts of interest
- Have, and communicate a code of ethics



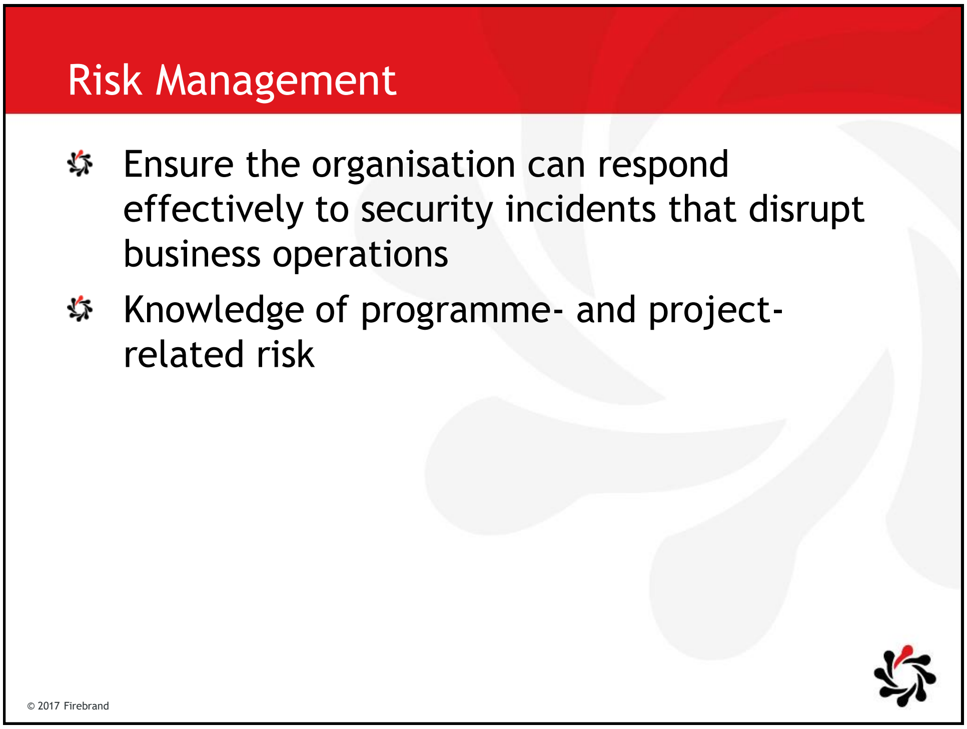
## Documentation

- Create and maintain appropriate security documentation
  - Policies, operational reports, risk assessments, etc.
  - Maintain documentation
    - Ownership and approval for changes
    - Version control
- Control access to documentation



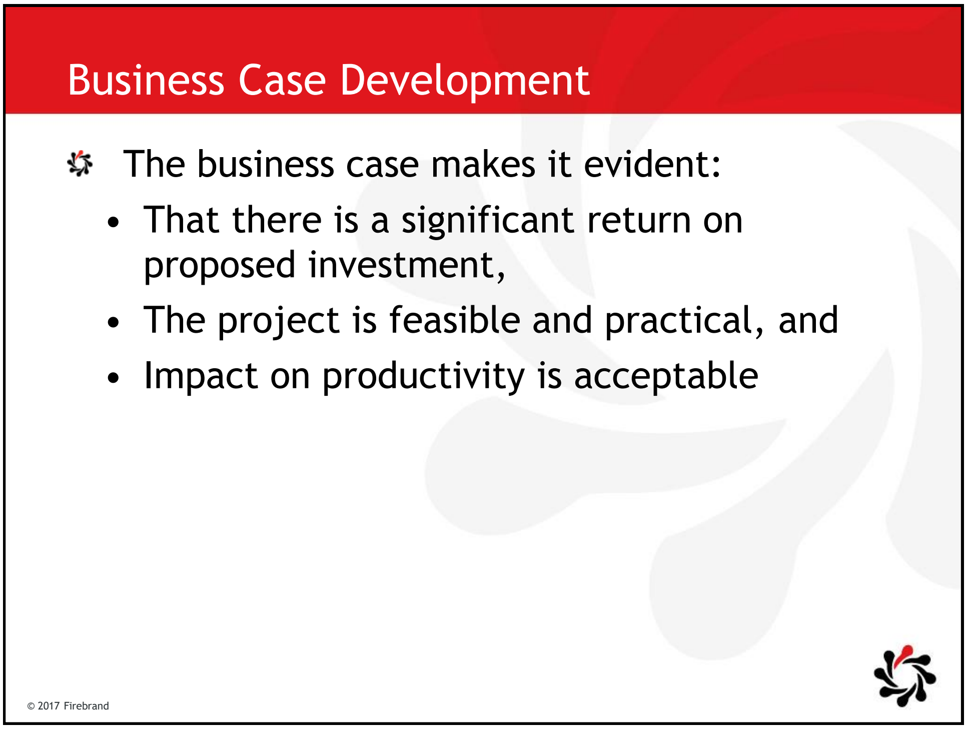
## Program Development and Project Management

- Information security programs are rarely static and must undergo ongoing development to meet changing conditions and risk
- Prioritise the portfolio of projects
  - Prevent overlap
  - Prevent one project from delaying another project
  - Ensure resources are properly allocated
  - Track deadlines and goals



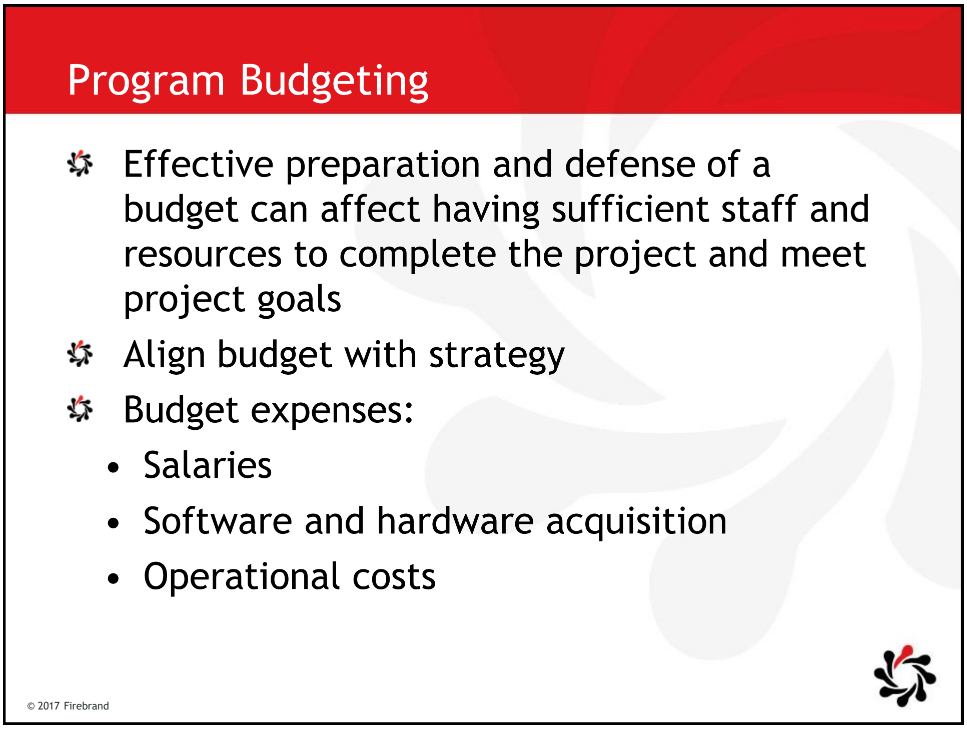
## Risk Management

- Ensure the organisation can respond effectively to security incidents that disrupt business operations
- Knowledge of programme- and project-related risk



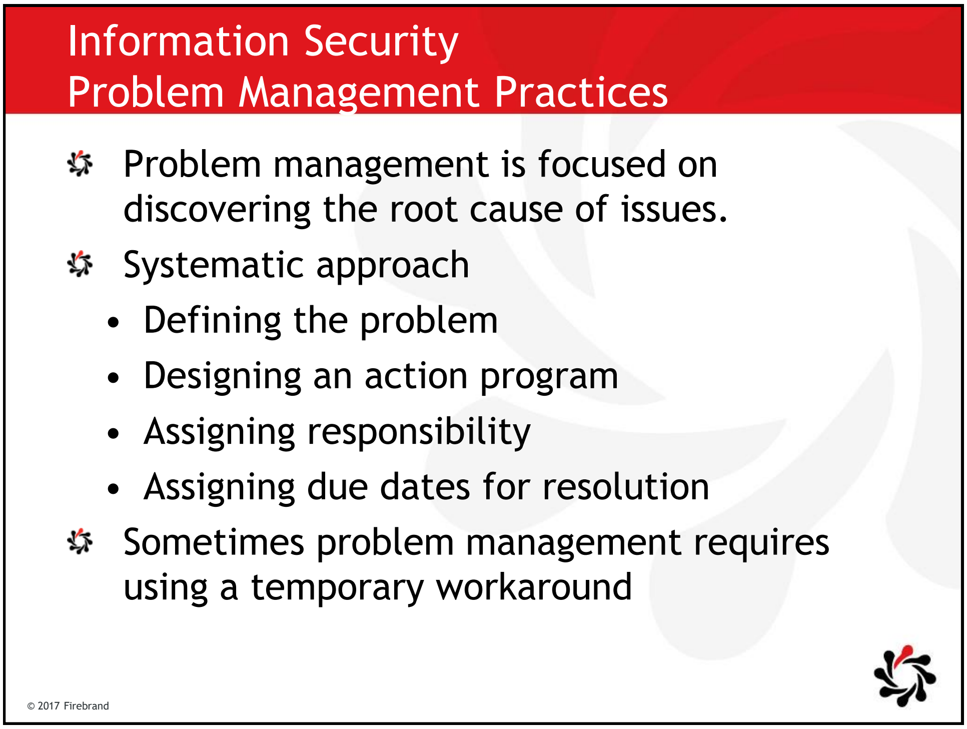
## Business Case Development

- The business case makes it evident:
  - That there is a significant return on proposed investment,
  - The project is feasible and practical, and
  - Impact on productivity is acceptable



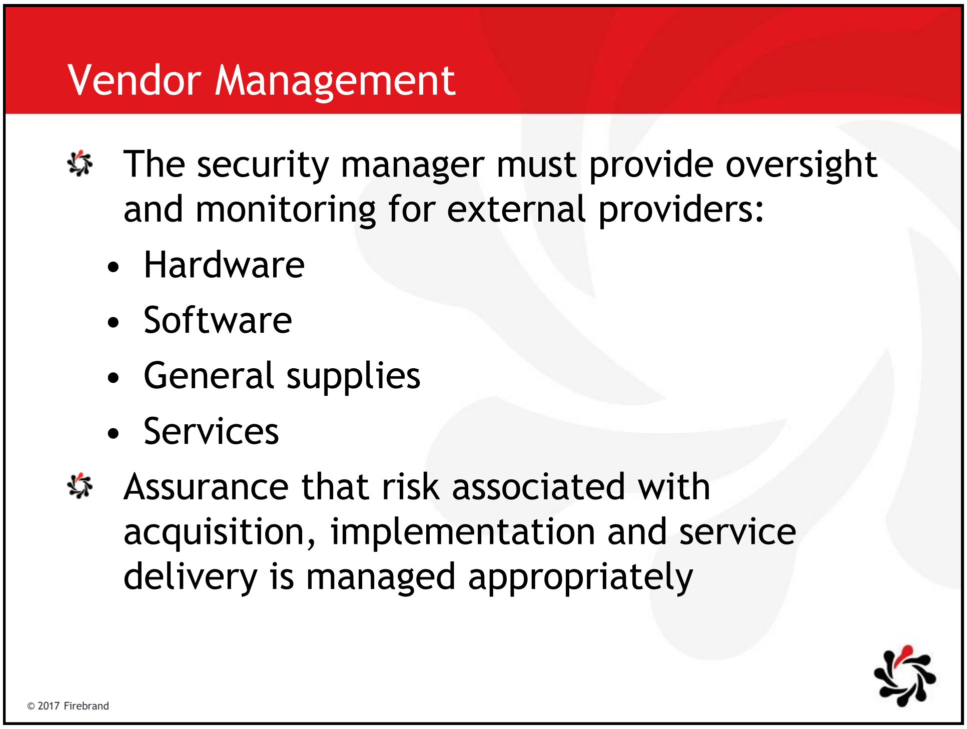
## Program Budgeting

- Effective preparation and defense of a budget can affect having sufficient staff and resources to complete the project and meet project goals
- Align budget with strategy
- Budget expenses:
  - Salaries
  - Software and hardware acquisition
  - Operational costs



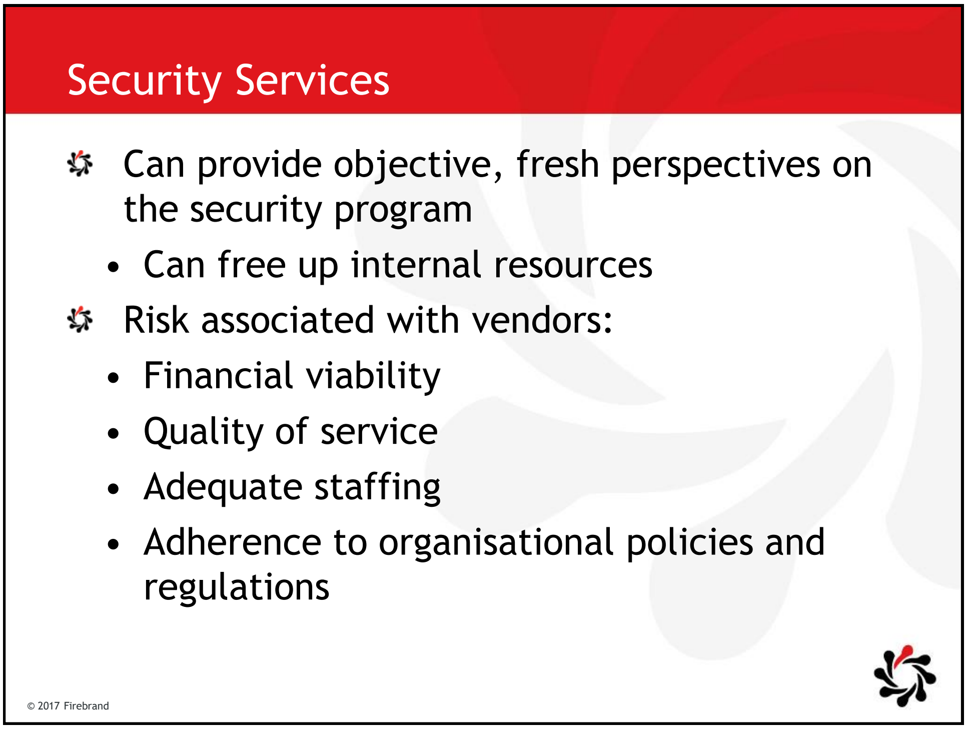
## Information Security Problem Management Practices

- Problem management is focused on discovering the root cause of issues.
- Systematic approach
  - Defining the problem
  - Designing an action program
  - Assigning responsibility
  - Assigning due dates for resolution
- Sometimes problem management requires using a temporary workaround



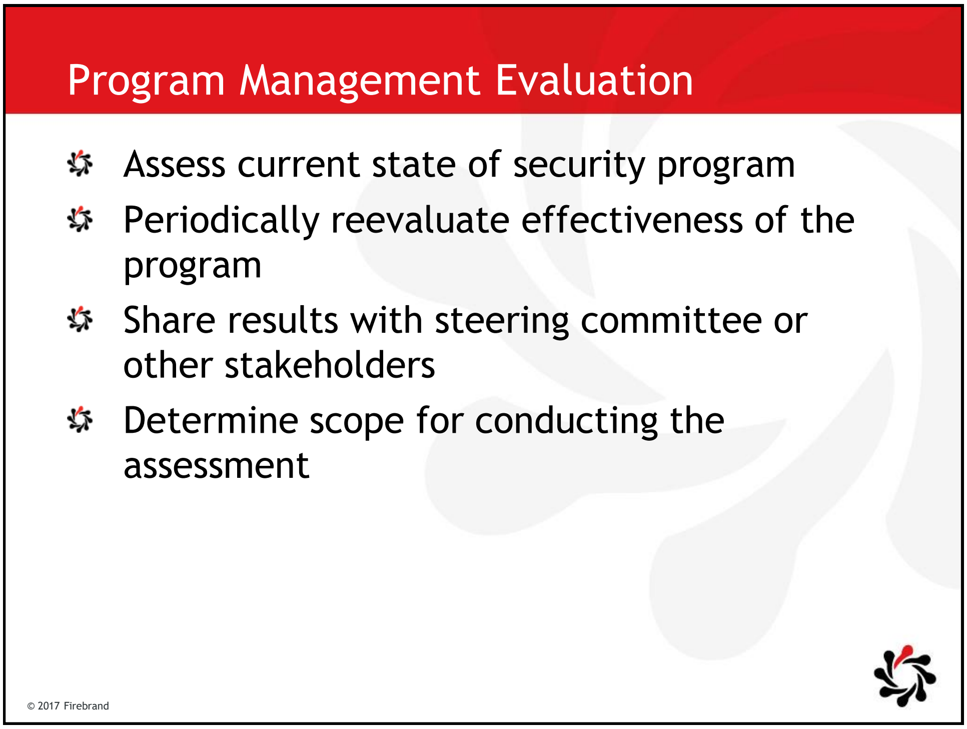
## Vendor Management

- The security manager must provide oversight and monitoring for external providers:
  - Hardware
  - Software
  - General supplies
  - Services
- Assurance that risk associated with acquisition, implementation and service delivery is managed appropriately



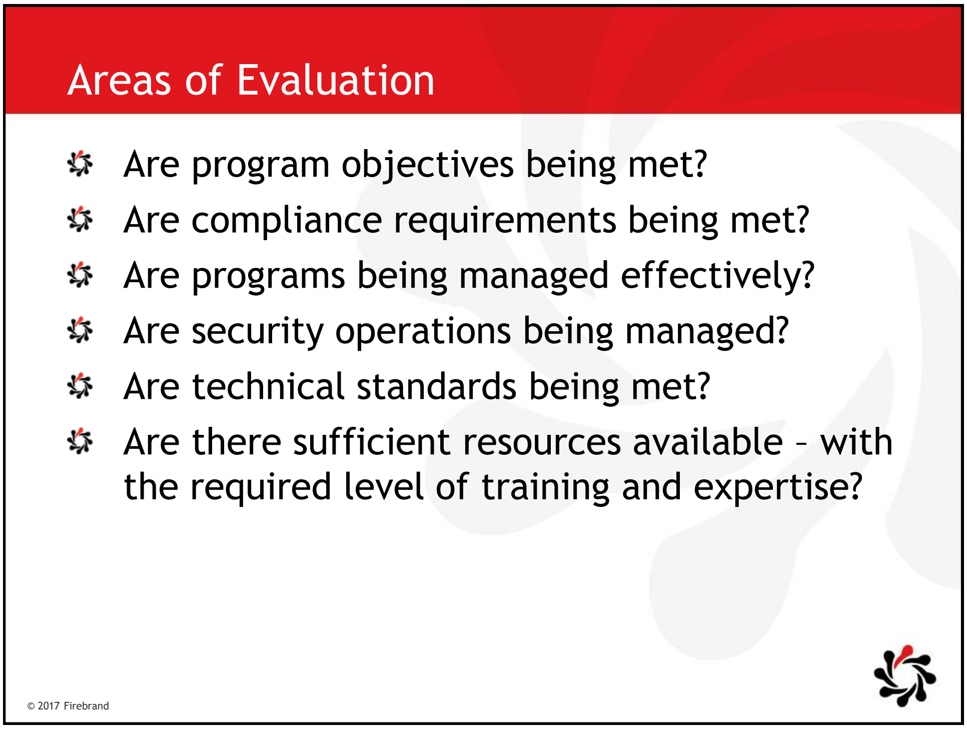
## Security Services

- Can provide objective, fresh perspectives on the security program
  - Can free up internal resources
- Risk associated with vendors:
  - Financial viability
  - Quality of service
  - Adequate staffing
  - Adherence to organisational policies and regulations



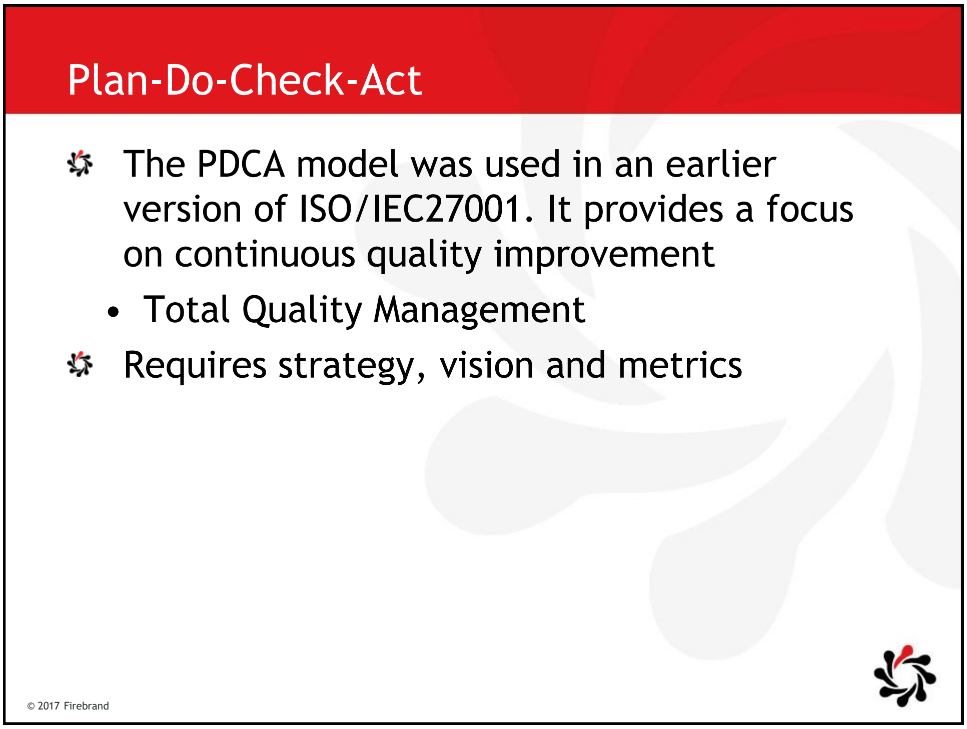
## Program Management Evaluation

- Assess current state of security program
- Periodically reevaluate effectiveness of the program
- Share results with steering committee or other stakeholders
- Determine scope for conducting the assessment



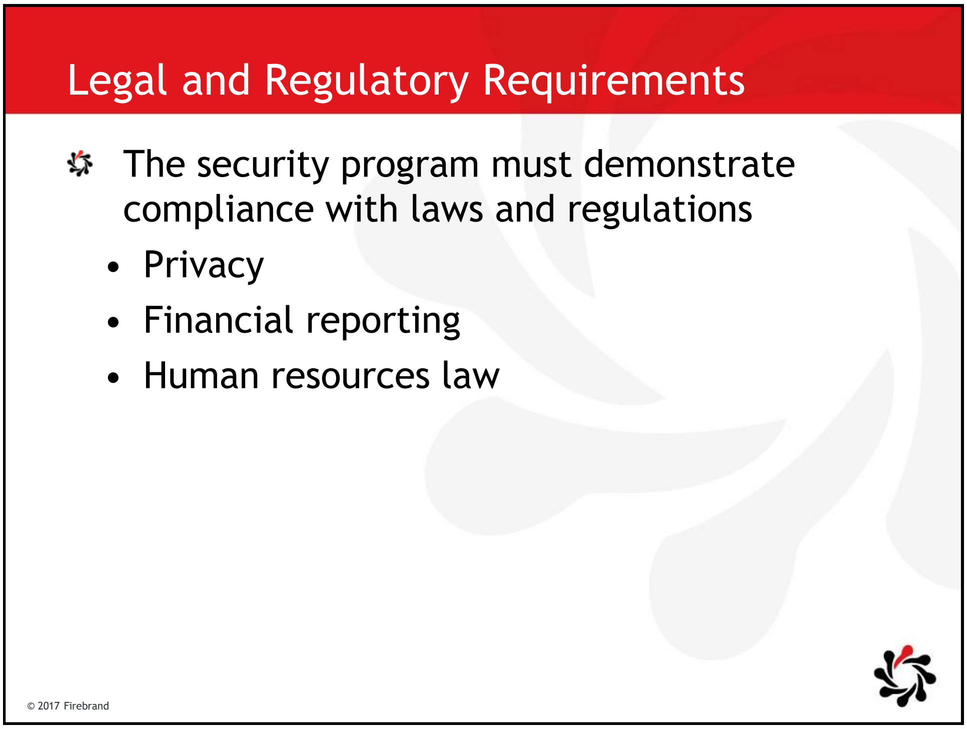
## Areas of Evaluation

- Are program objectives being met?
- Are compliance requirements being met?
- Are programs being managed effectively?
- Are security operations being managed?
- Are technical standards being met?
- Are there sufficient resources available – with the required level of training and expertise?



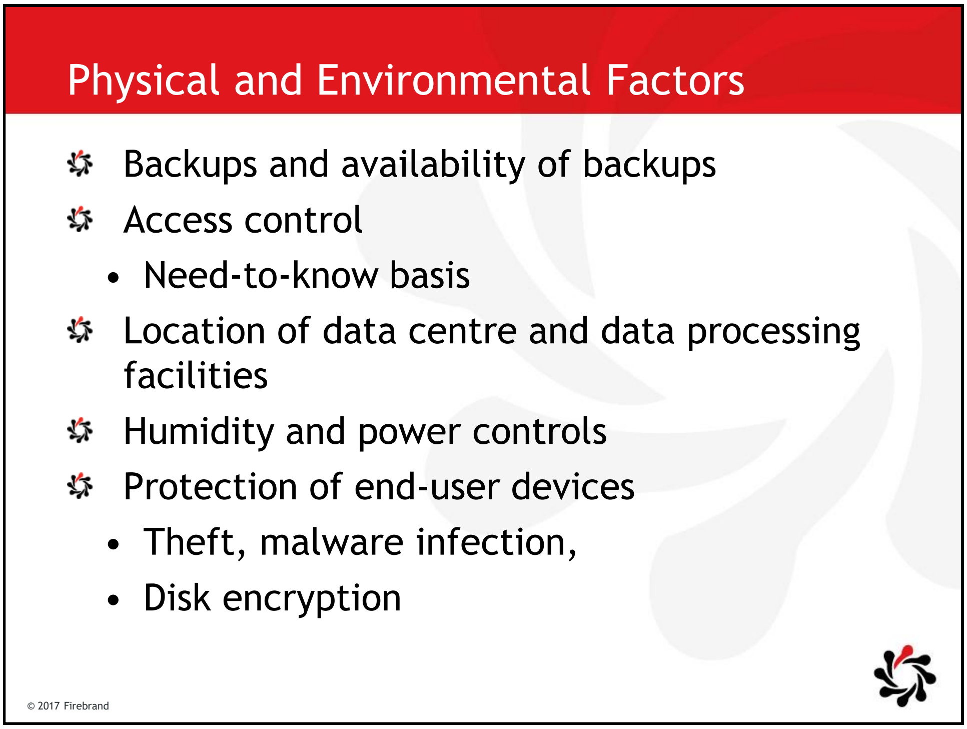
## Plan-Do-Check-Act

- The PDCA model was used in an earlier version of ISO/IEC27001. It provides a focus on continuous quality improvement
  - Total Quality Management
- Requires strategy, vision and metrics



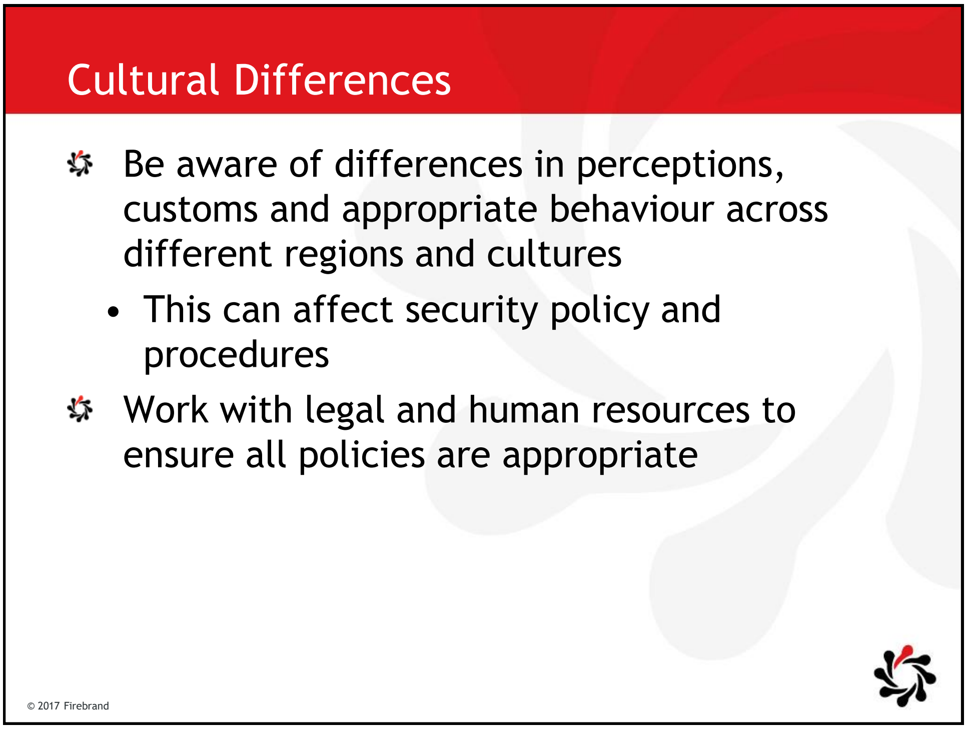
## Legal and Regulatory Requirements

- The security program must demonstrate compliance with laws and regulations
  - Privacy
  - Financial reporting
  - Human resources law



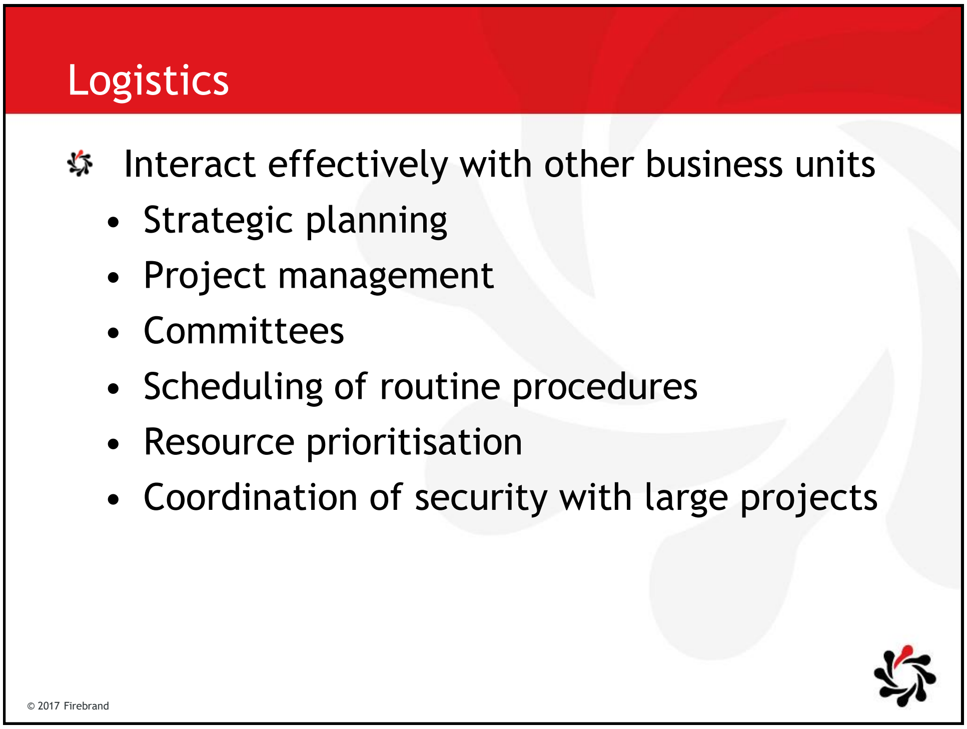
## Physical and Environmental Factors

- Backups and availability of backups
- Access control
  - Need-to-know basis
- Location of data centre and data processing facilities
- Humidity and power controls
- Protection of end-user devices
  - Theft, malware infection,
  - Disk encryption



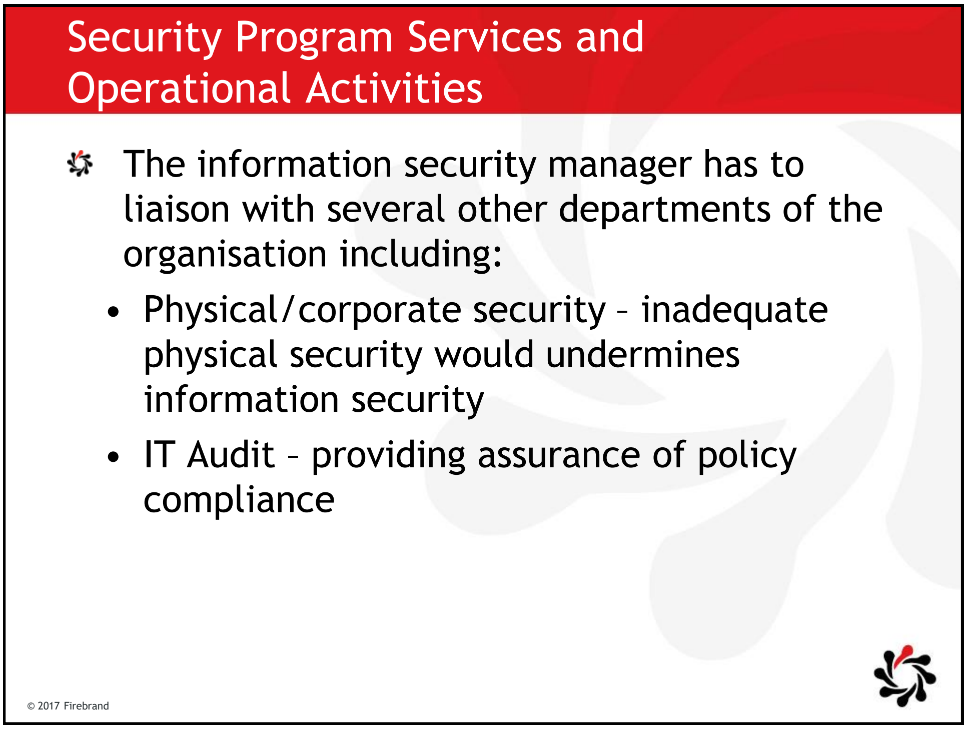
## Cultural Differences

- Be aware of differences in perceptions, customs and appropriate behaviour across different regions and cultures
  - This can affect security policy and procedures
- Work with legal and human resources to ensure all policies are appropriate



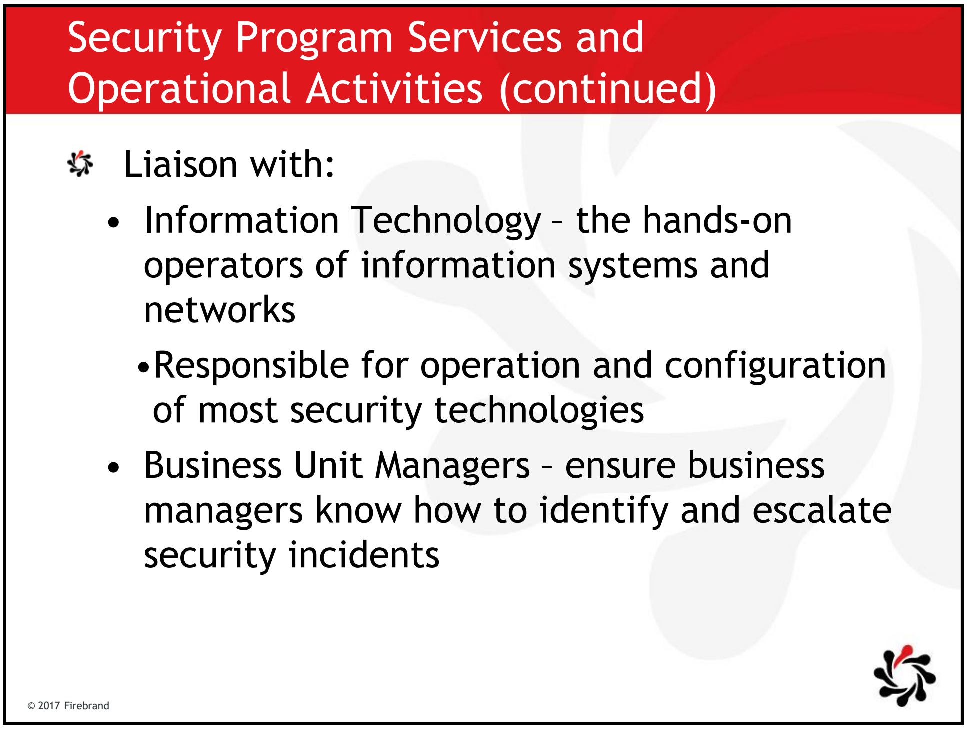
## Logistics

- Interact effectively with other business units
  - Strategic planning
  - Project management
  - Committees
  - Scheduling of routine procedures
  - Resource prioritisation
  - Coordination of security with large projects



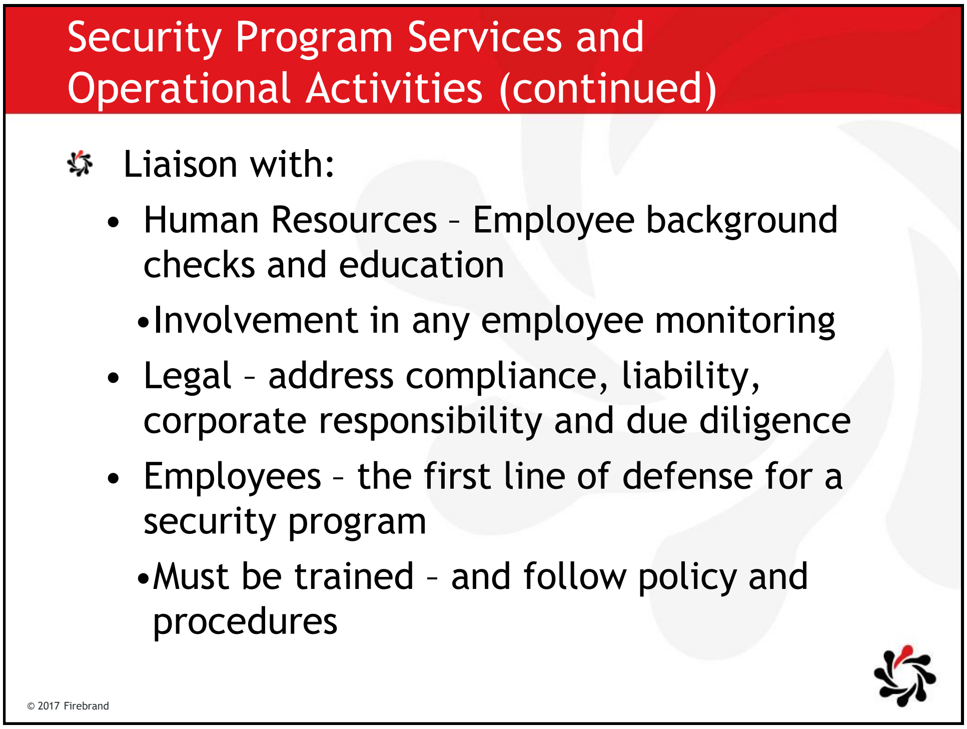
## Security Program Services and Operational Activities

- The information security manager has to liaison with several other departments of the organisation including:
  - Physical/corporate security – inadequate physical security would undermines information security
  - IT Audit – providing assurance of policy compliance



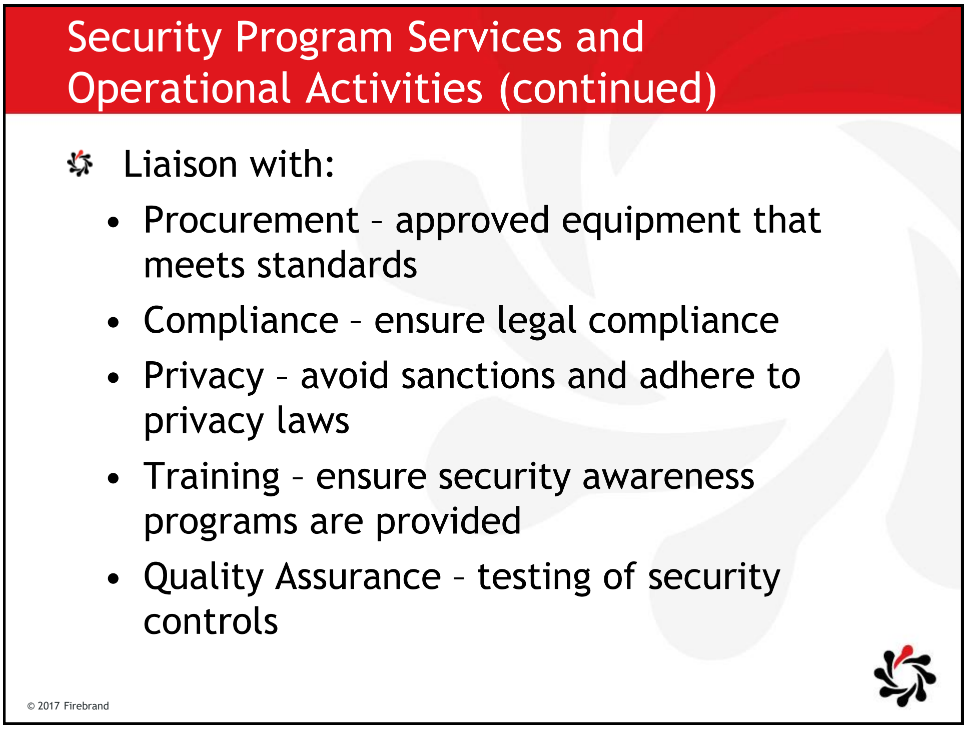
## Security Program Services and Operational Activities (continued)

- Liaison with:
  - Information Technology – the hands-on operators of information systems and networks
    - Responsible for operation and configuration of most security technologies
  - Business Unit Managers – ensure business managers know how to identify and escalate security incidents



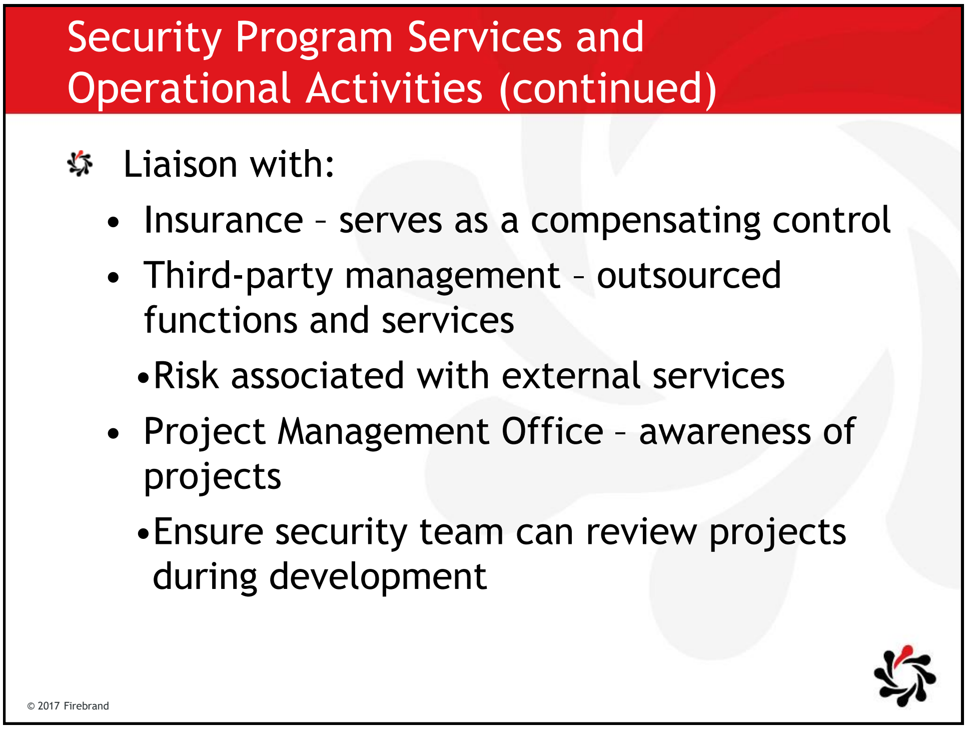
## Security Program Services and Operational Activities (continued)

- Liaison with:
  - Human Resources – Employee background checks and education
    - Involvement in any employee monitoring
  - Legal – address compliance, liability, corporate responsibility and due diligence
  - Employees – the first line of defense for a security program
    - Must be trained – and follow policy and procedures



## Security Program Services and Operational Activities (continued)

- Liaison with:
  - Procurement – approved equipment that meets standards
  - Compliance – ensure legal compliance
  - Privacy – avoid sanctions and adhere to privacy laws
  - Training – ensure security awareness programs are provided
  - Quality Assurance – testing of security controls

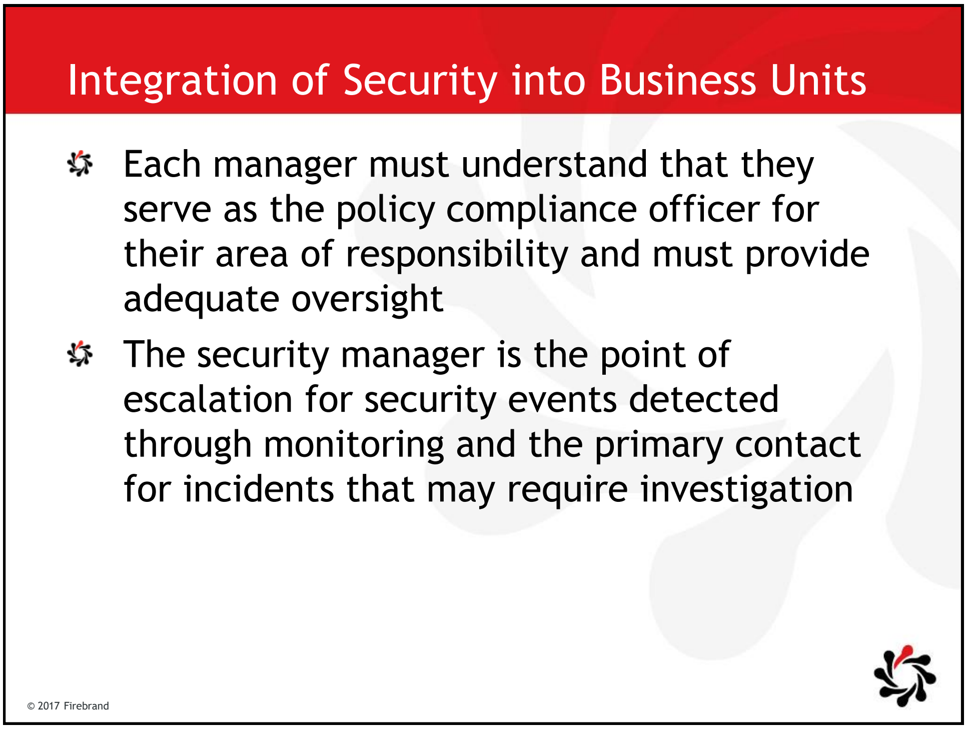


## Security Program Services and Operational Activities (continued)

- Liaison with:
  - Insurance – serves as a compensating control
  - Third-party management – outsourced functions and services
    - Risk associated with external services
  - Project Management Office – awareness of projects
    - Ensure security team can review projects during development

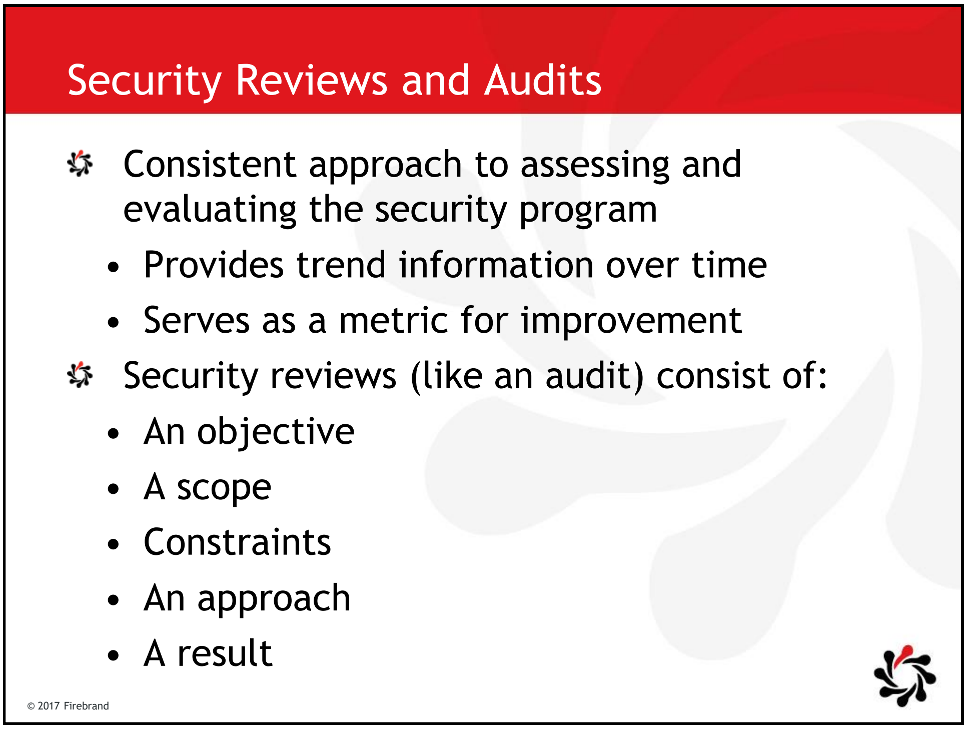
## Cross-Organisational Responsibilities

- Separation of duties (SoD) is an important element of a security program
  - Compensating controls should be in place where there is insufficient SoD
- Coordinated activities across departments and management tiers through communications and relationship building
- Each department must understand the requirement to support and implement the security program



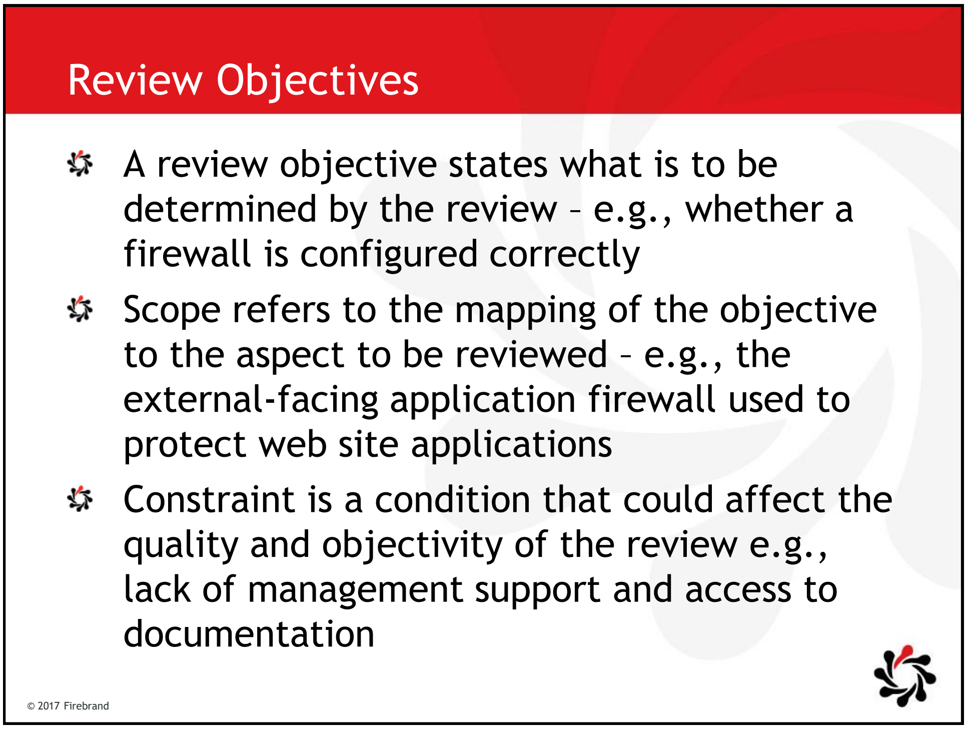
## Integration of Security into Business Units

- Each manager must understand that they serve as the policy compliance officer for their area of responsibility and must provide adequate oversight
- The security manager is the point of escalation for security events detected through monitoring and the primary contact for incidents that may require investigation



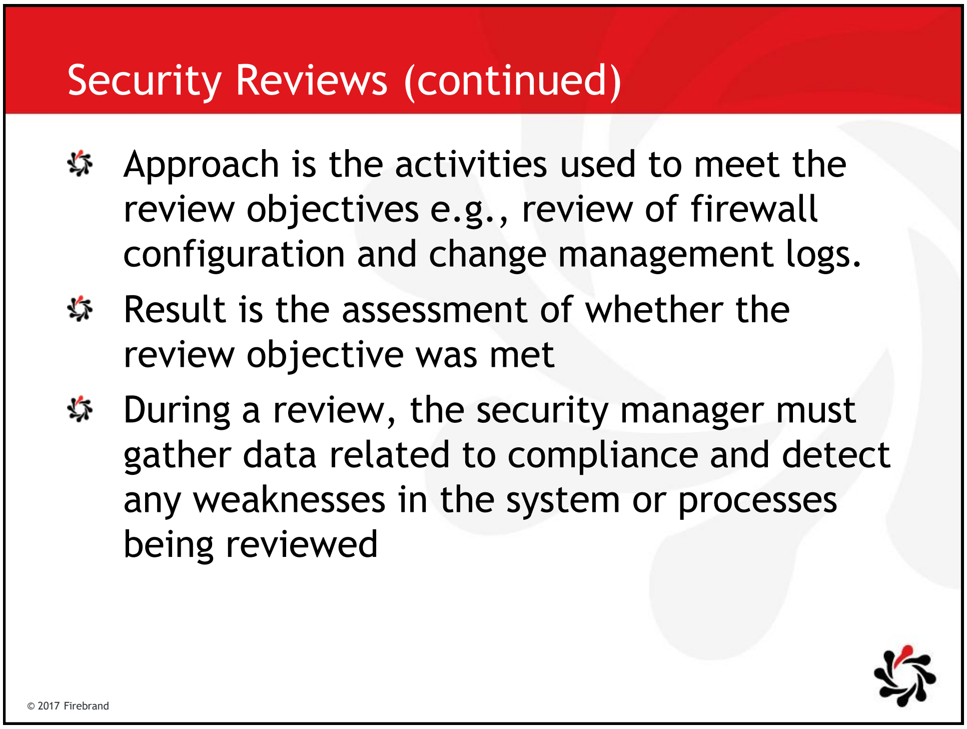
## Security Reviews and Audits

- Consistent approach to assessing and evaluating the security program
  - Provides trend information over time
  - Serves as a metric for improvement
- Security reviews (like an audit) consist of:
  - An objective
  - A scope
  - Constraints
  - An approach
  - A result



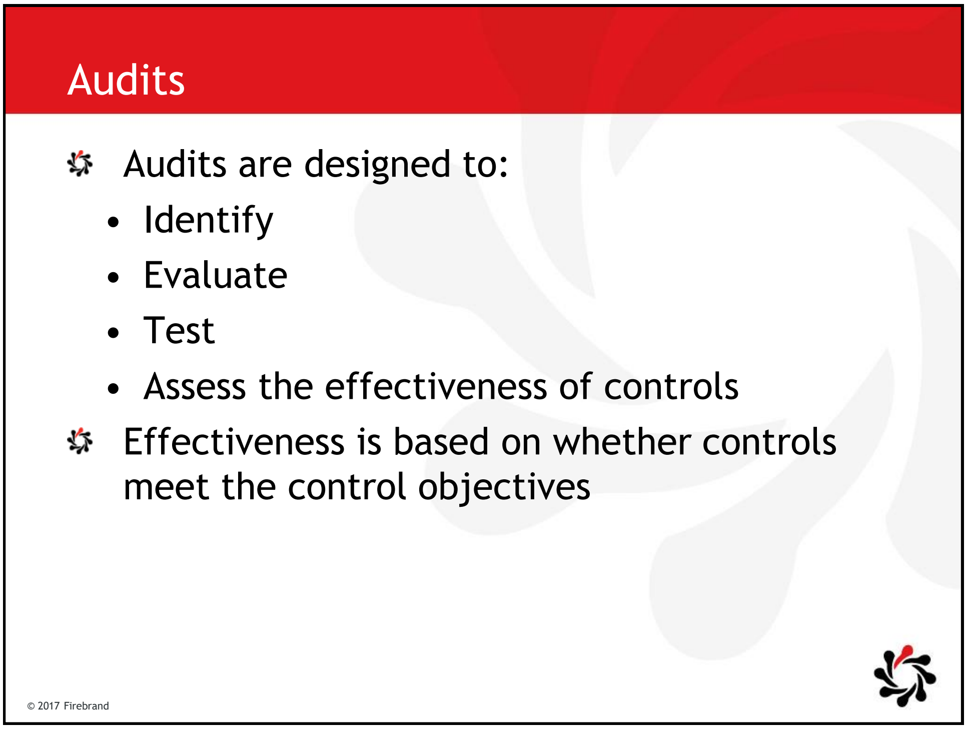
## Review Objectives

- A review objective states what is to be determined by the review – e.g., whether a firewall is configured correctly
- Scope refers to the mapping of the objective to the aspect to be reviewed – e.g., the external-facing application firewall used to protect web site applications
- Constraint is a condition that could affect the quality and objectivity of the review e.g., lack of management support and access to documentation



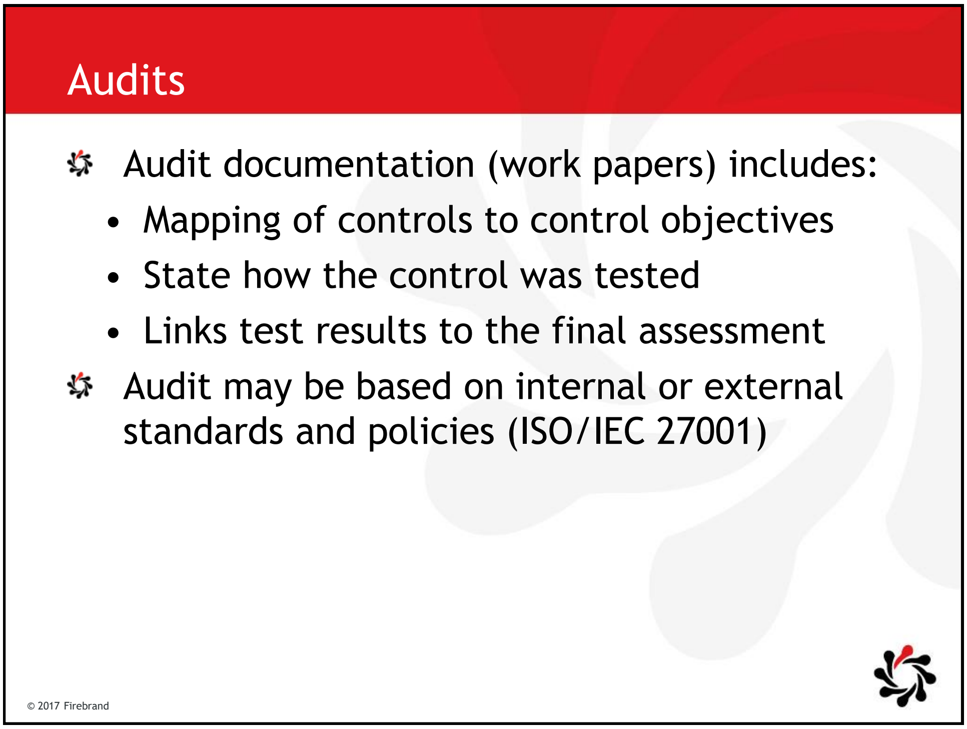
## Security Reviews (continued)

- Approach is the activities used to meet the review objectives e.g., review of firewall configuration and change management logs.
- Result is the assessment of whether the review objective was met
- During a review, the security manager must gather data related to compliance and detect any weaknesses in the system or processes being reviewed



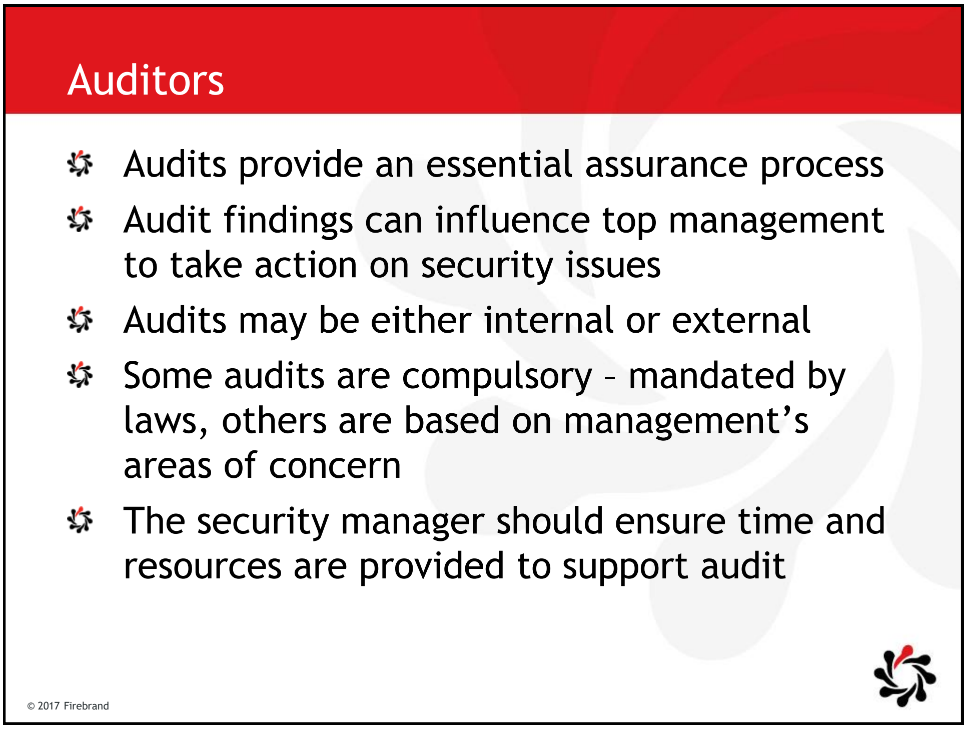
## Audits

- Audits are designed to:
  - Identify
  - Evaluate
  - Test
  - Assess the effectiveness of controls
- Effectiveness is based on whether controls meet the control objectives



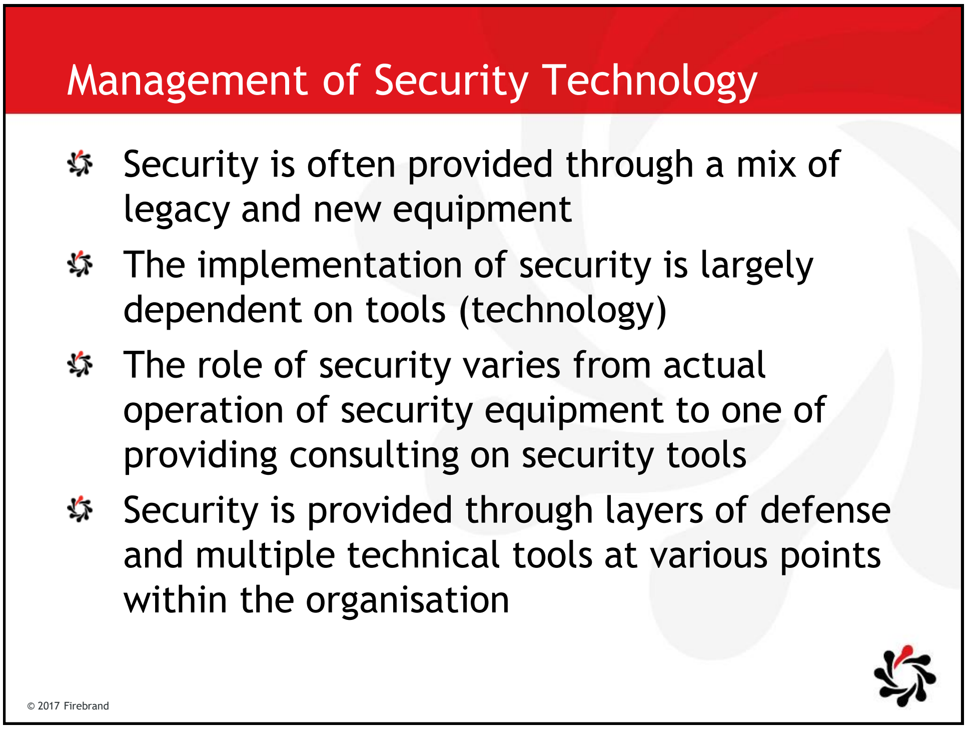
## Audits

- Audit documentation (work papers) includes:
  - Mapping of controls to control objectives
  - State how the control was tested
  - Links test results to the final assessment
- Audit may be based on internal or external standards and policies (ISO/IEC 27001)



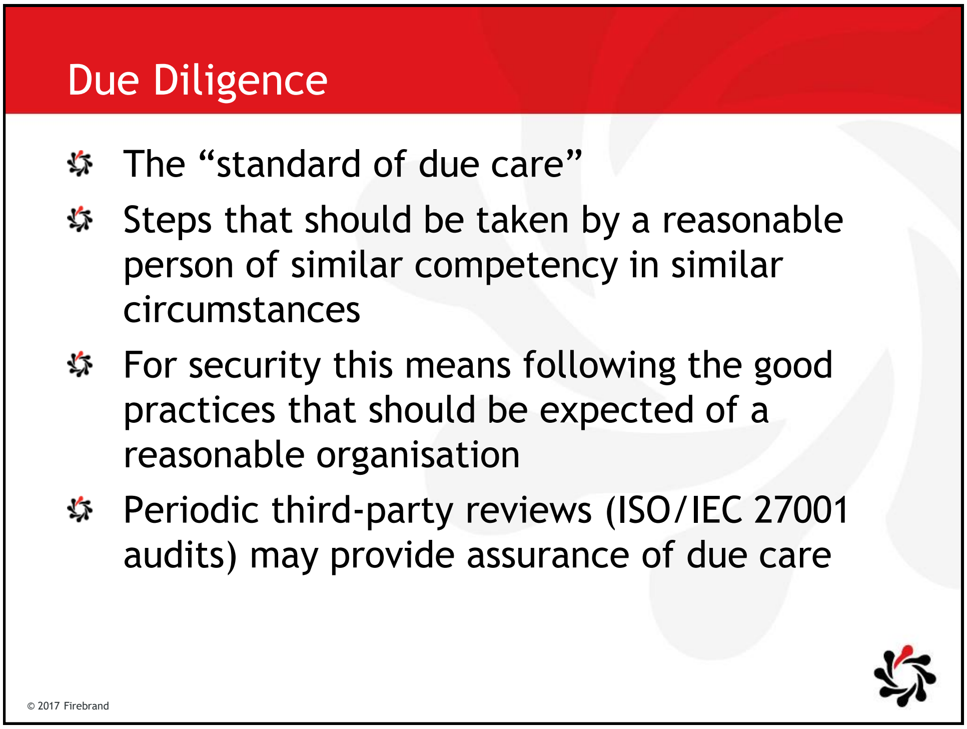
## Auditors

- Audits provide an essential assurance process
- Audit findings can influence top management to take action on security issues
- Audits may be either internal or external
- Some audits are compulsory – mandated by laws, others are based on management’s areas of concern
- The security manager should ensure time and resources are provided to support audit



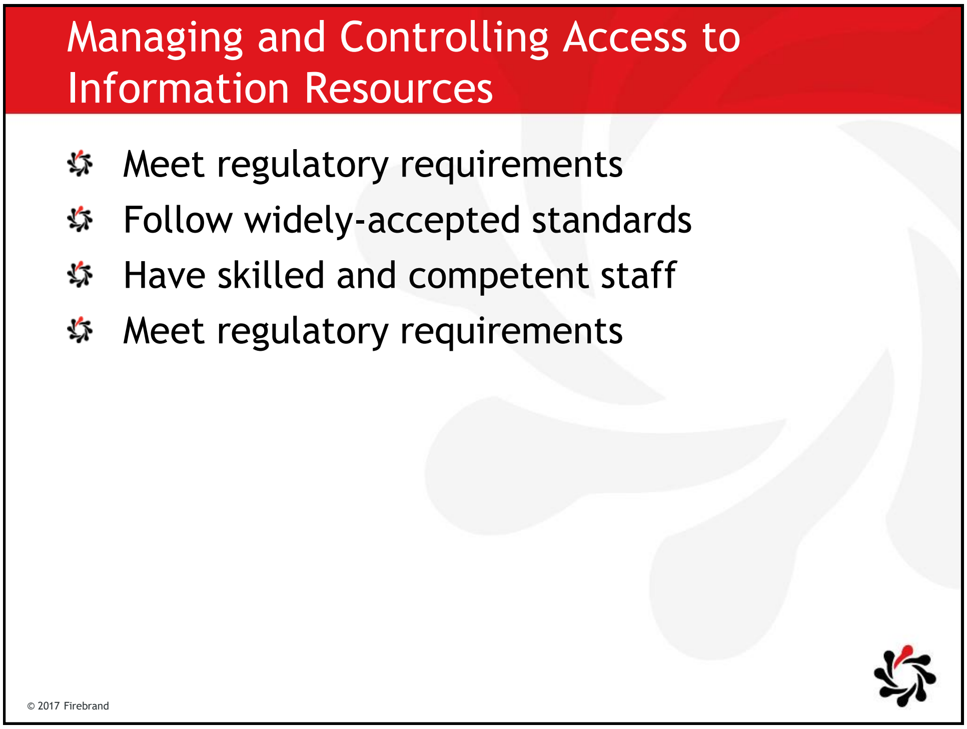
## Management of Security Technology

- Security is often provided through a mix of legacy and new equipment
- The implementation of security is largely dependent on tools (technology)
- The role of security varies from actual operation of security equipment to one of providing consulting on security tools
- Security is provided through layers of defense and multiple technical tools at various points within the organisation



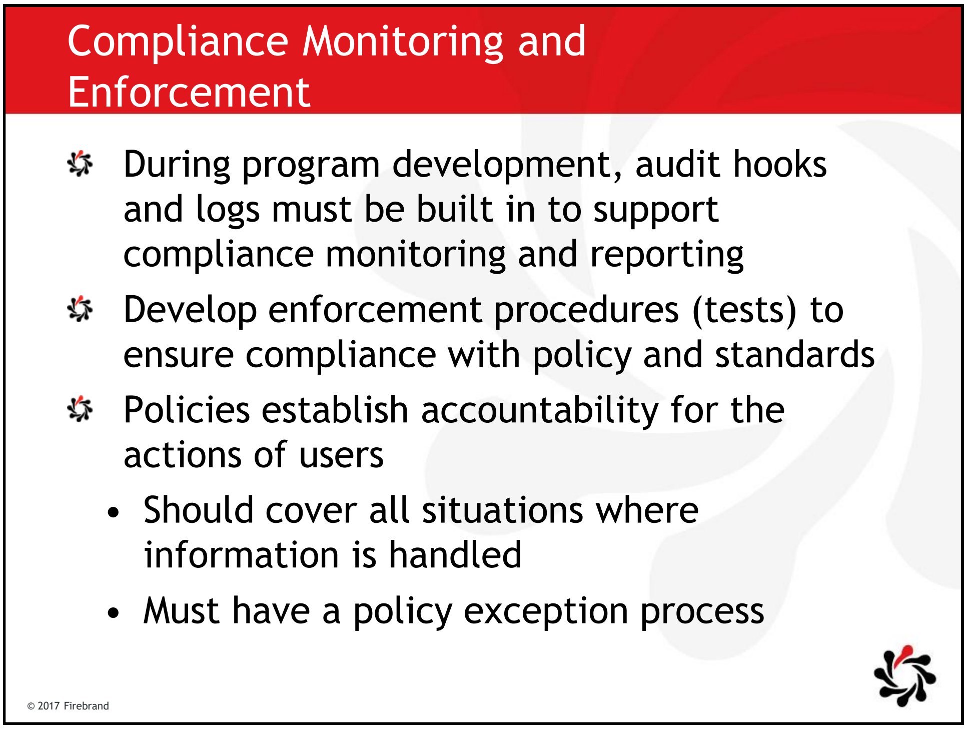
## Due Diligence

- The “standard of due care”
- Steps that should be taken by a reasonable person of similar competency in similar circumstances
- For security this means following the good practices that should be expected of a reasonable organisation
- Periodic third-party reviews (ISO/IEC 27001 audits) may provide assurance of due care



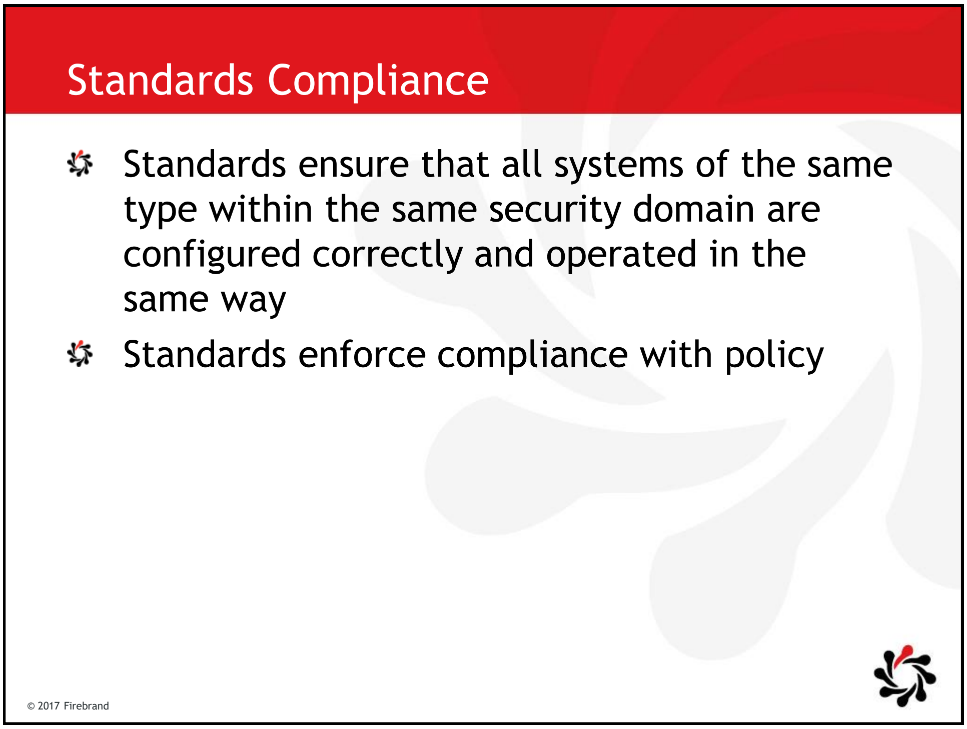
## Managing and Controlling Access to Information Resources

- Meet regulatory requirements
- Follow widely-accepted standards
- Have skilled and competent staff
- Meet regulatory requirements



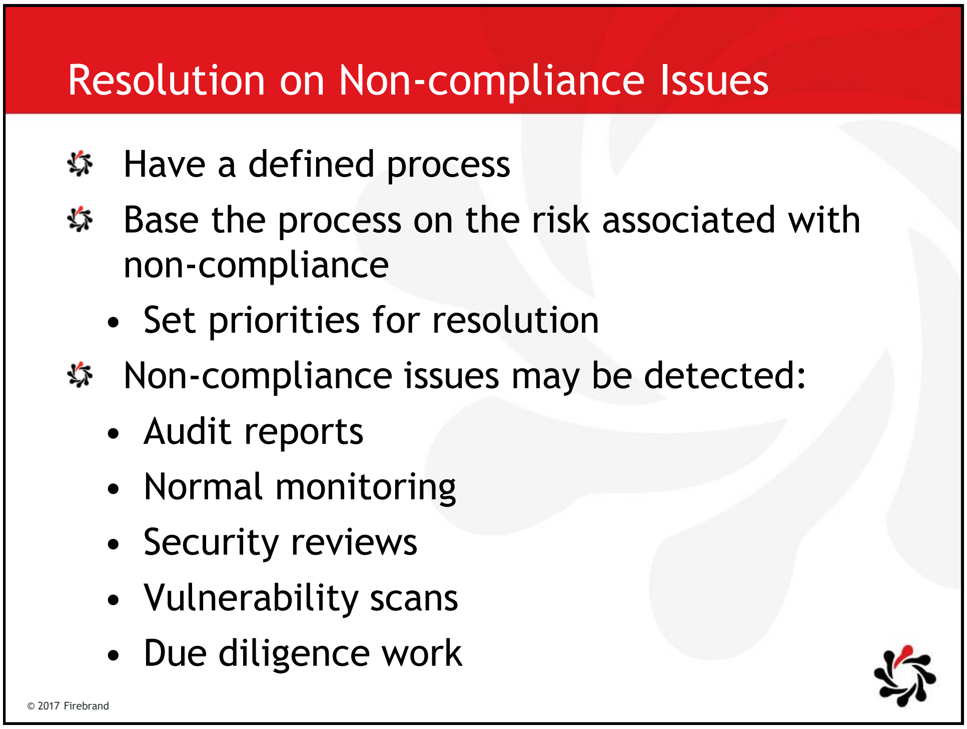
## Compliance Monitoring and Enforcement

- During program development, audit hooks and logs must be built in to support compliance monitoring and reporting
- Develop enforcement procedures (tests) to ensure compliance with policy and standards
- Policies establish accountability for the actions of users
  - Should cover all situations where information is handled
  - Must have a policy exception process



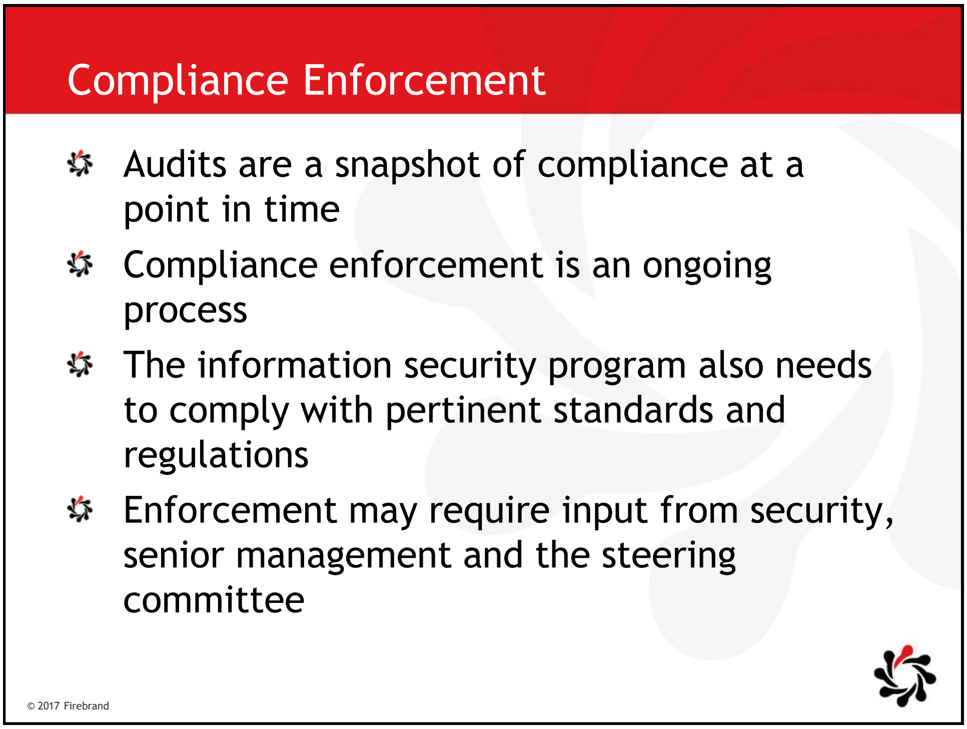
## Standards Compliance

- Standards ensure that all systems of the same type within the same security domain are configured correctly and operated in the same way
- Standards enforce compliance with policy



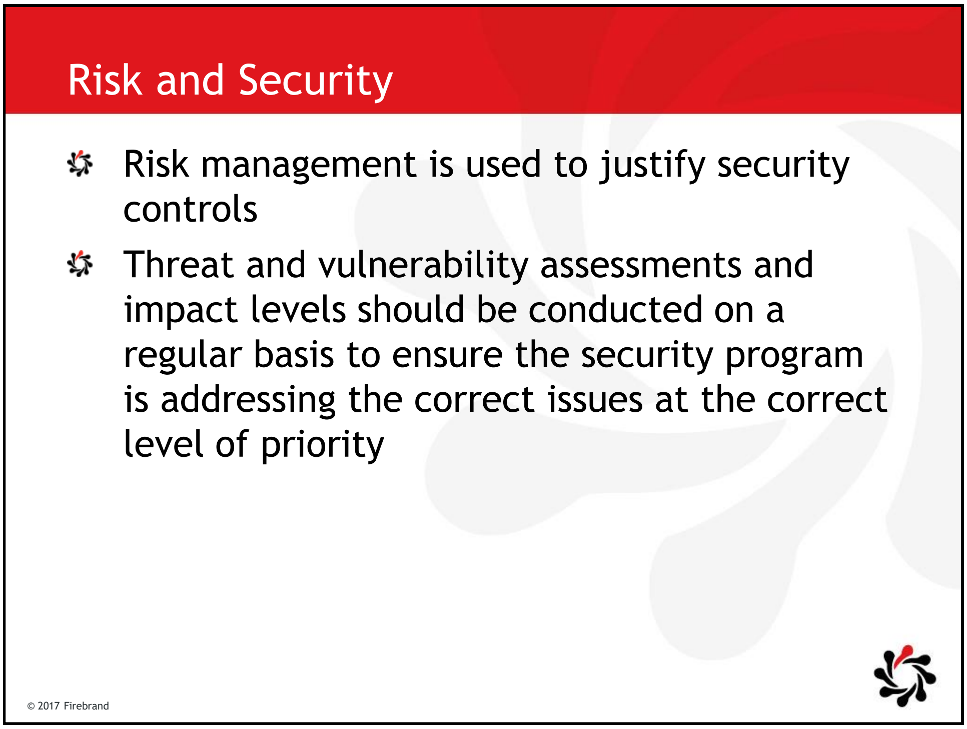
## Resolution on Non-compliance Issues

- Have a defined process
- Base the process on the risk associated with non-compliance
  - Set priorities for resolution
- Non-compliance issues may be detected:
  - Audit reports
  - Normal monitoring
  - Security reviews
  - Vulnerability scans
  - Due diligence work



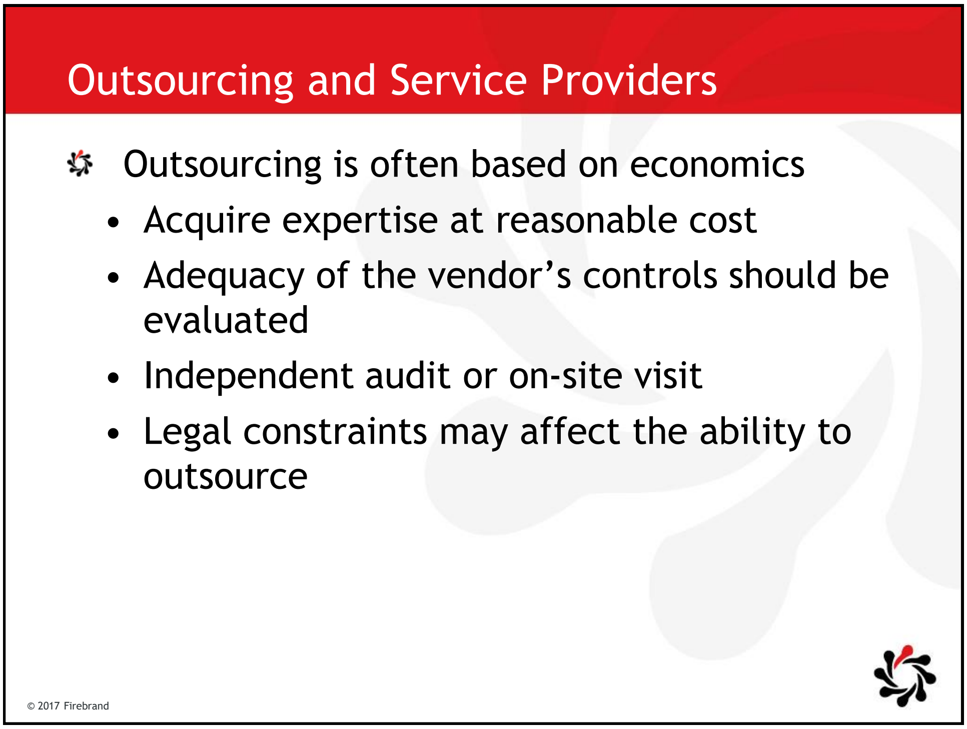
## Compliance Enforcement

- Audits are a snapshot of compliance at a point in time
- Compliance enforcement is an ongoing process
- The information security program also needs to comply with pertinent standards and regulations
- Enforcement may require input from security, senior management and the steering committee



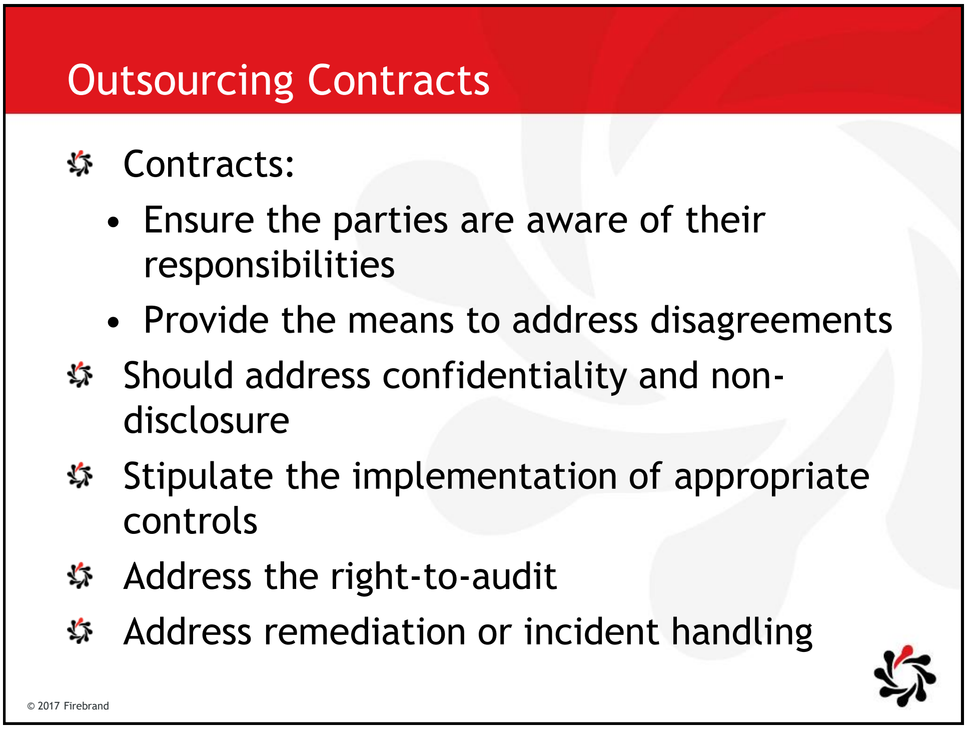
## Risk and Security

- Risk management is used to justify security controls
- Threat and vulnerability assessments and impact levels should be conducted on a regular basis to ensure the security program is addressing the correct issues at the correct level of priority



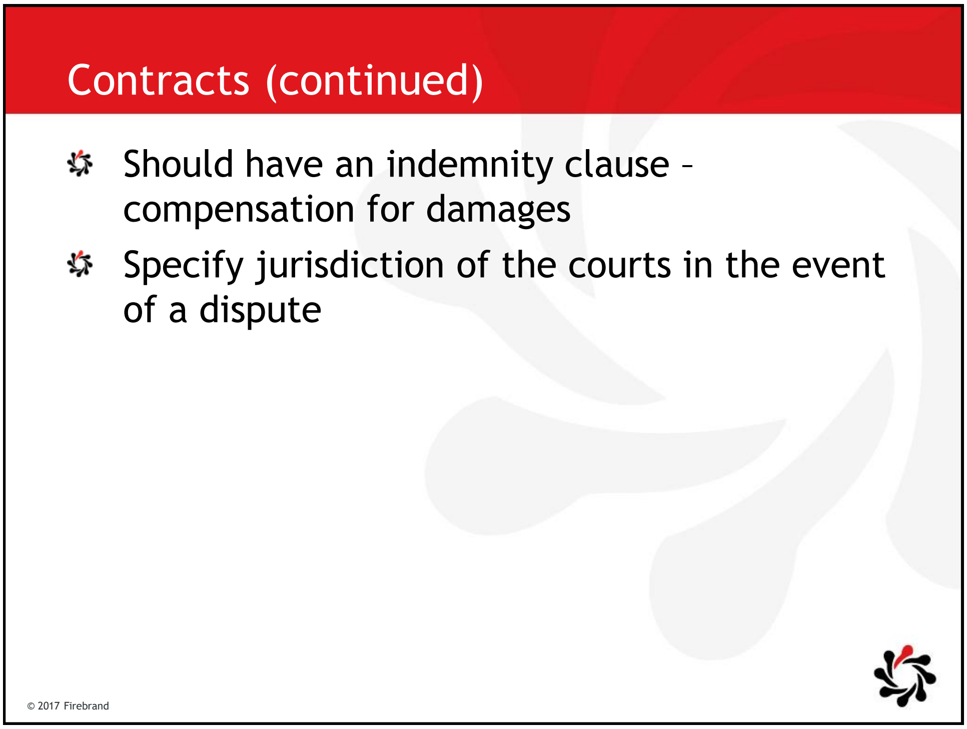
## Outsourcing and Service Providers

- Outsourcing is often based on economics
  - Acquire expertise at reasonable cost
  - Adequacy of the vendor’s controls should be evaluated
  - Independent audit or on-site visit
  - Legal constraints may affect the ability to outsource



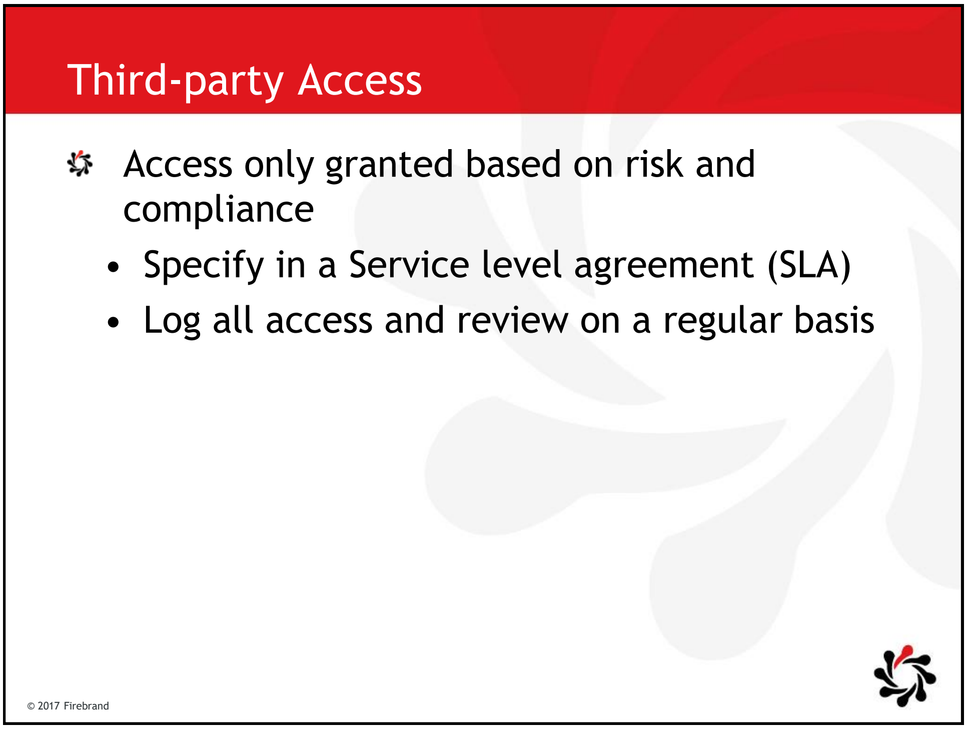
## Outsourcing Contracts

- Contracts:
  - Ensure the parties are aware of their responsibilities
  - Provide the means to address disagreements
- Should address confidentiality and non-disclosure
- Stipulate the implementation of appropriate controls
- Address the right-to-audit
- Address remediation or incident handling



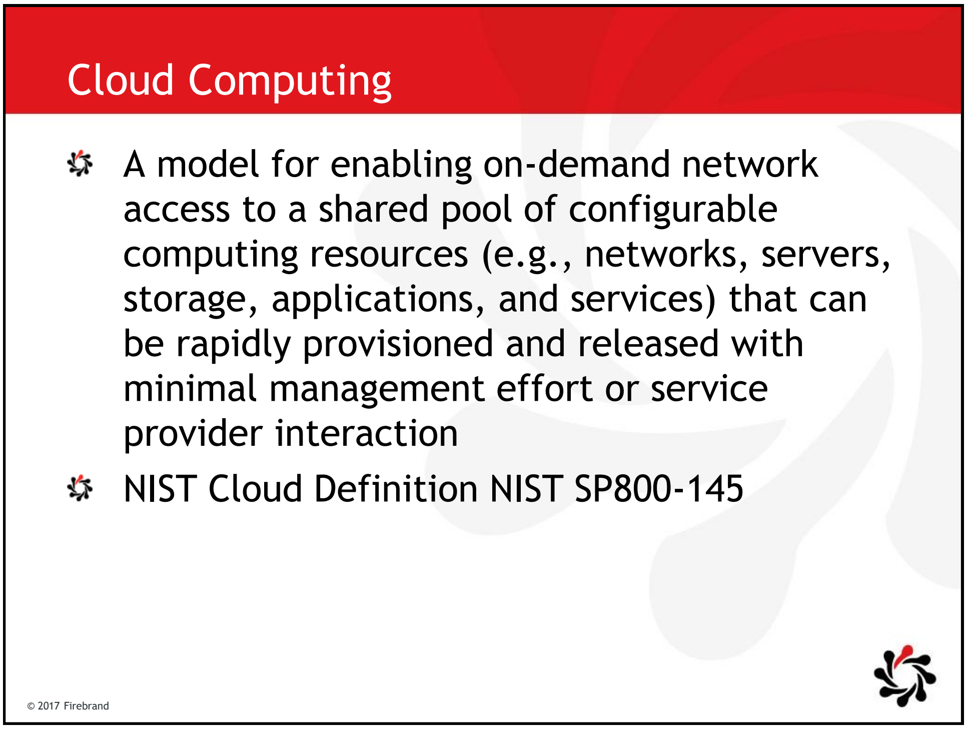
## Contracts (continued)

- Should have an indemnity clause – compensation for damages
- Specify jurisdiction of the courts in the event of a dispute



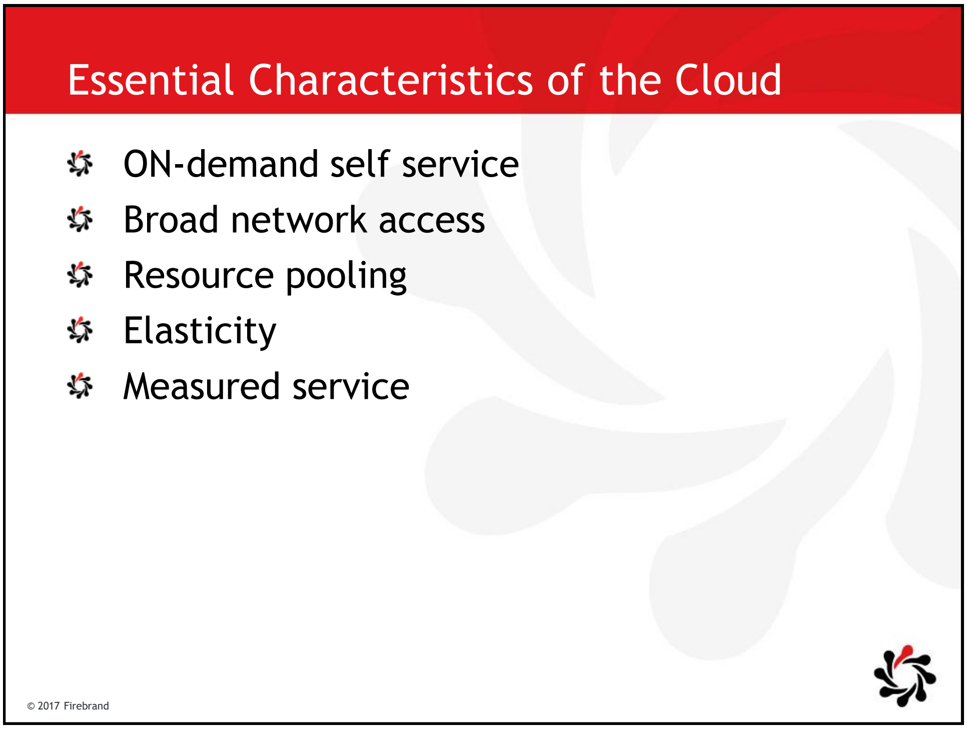
## Third-party Access

- Access only granted based on risk and compliance
  - Specify in a Service level agreement (SLA)
  - Log all access and review on a regular basis



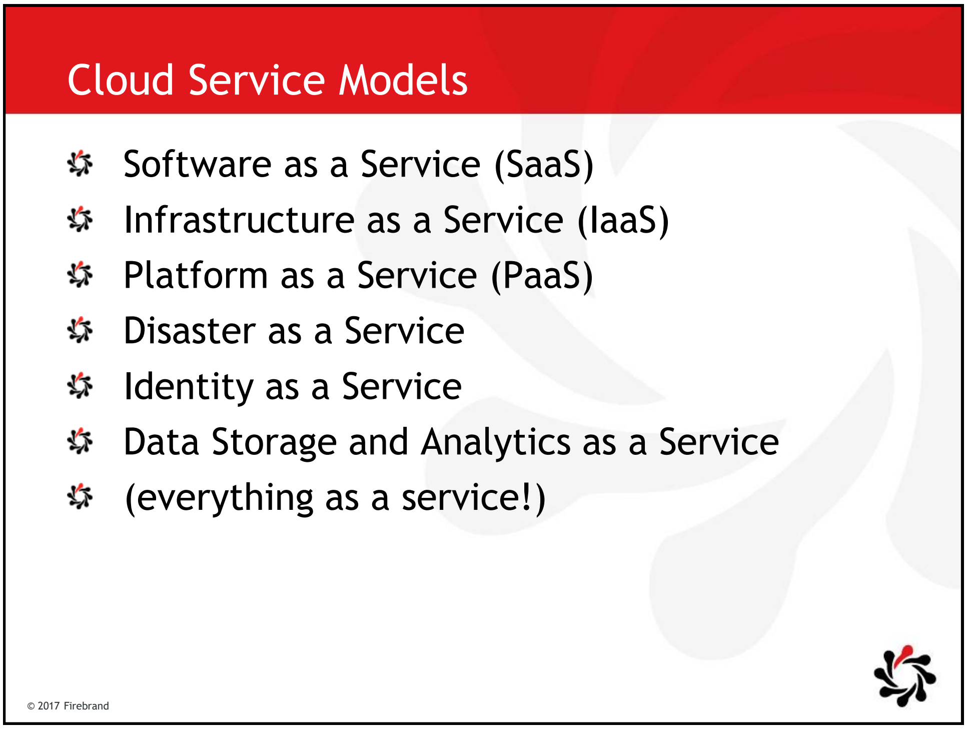
## Cloud Computing

- A model for enabling on-demand network access to a shared pool of configurable computing resources (e.g., networks, servers, storage, applications, and services) that can be rapidly provisioned and released with minimal management effort or service provider interaction
- NIST Cloud Definition NIST SP800-145



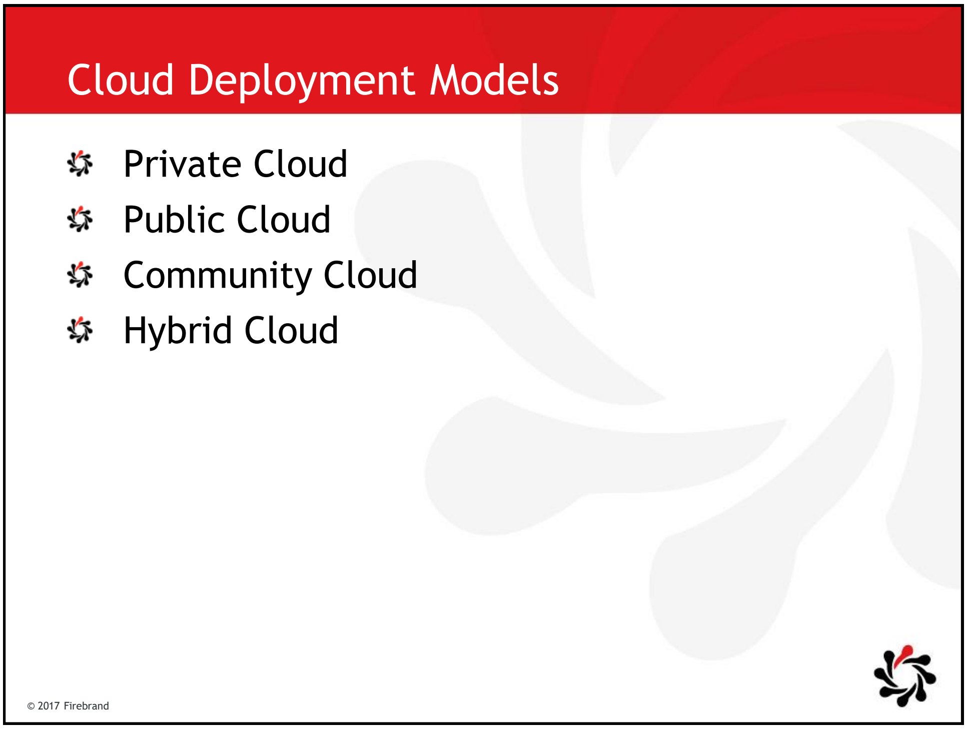
## Essential Characteristics of the Cloud

- ON-demand self service
- Broad network access
- Resource pooling
- Elasticity
- Measured service



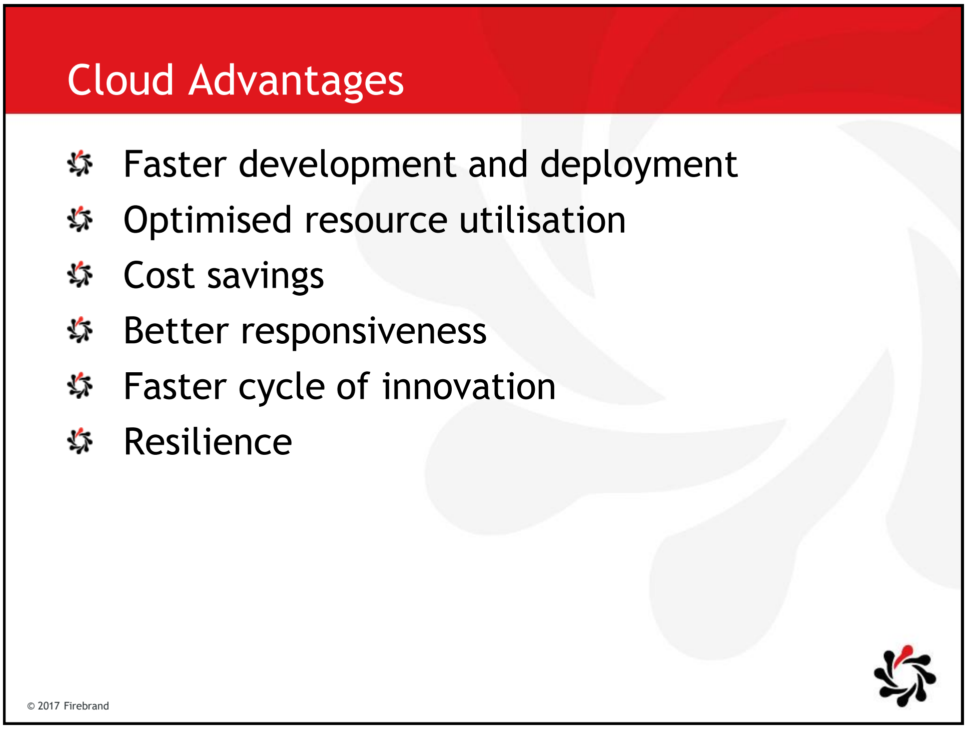
## Cloud Service Models

- Software as a Service (SaaS)
- Infrastructure as a Service (IaaS)
- Platform as a Service (PaaS)
- Disaster as a Service
- Identity as a Service
- Data Storage and Analytics as a Service
- (everything as a service!)



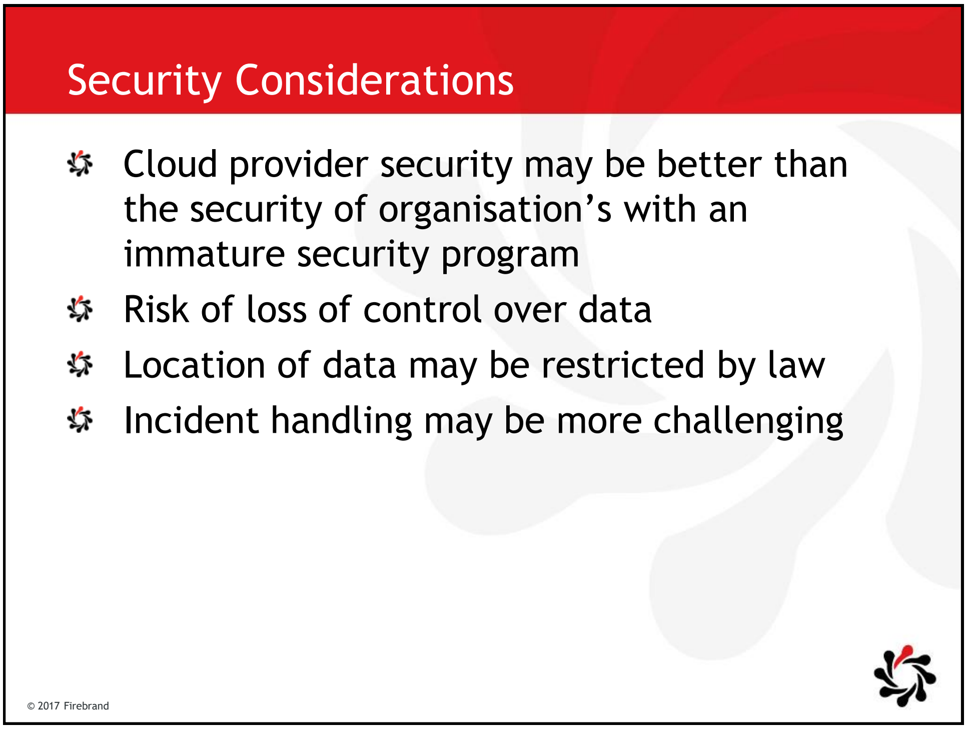
## Cloud Deployment Models

- Private Cloud
- Public Cloud
- Community Cloud
- Hybrid Cloud



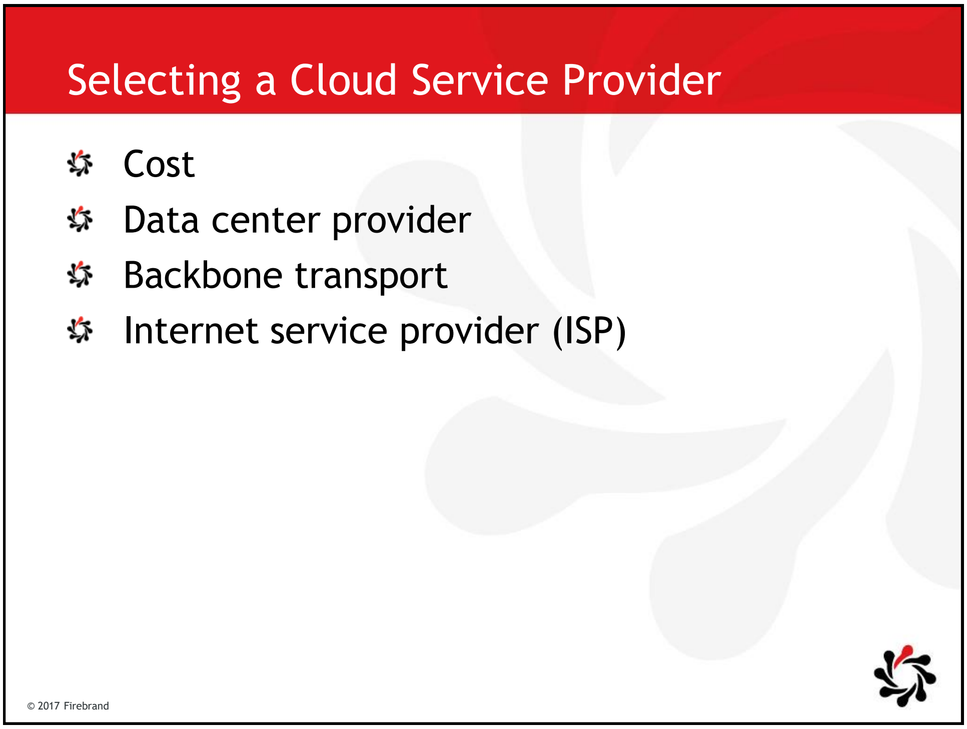
## Cloud Advantages

- Faster development and deployment
- Optimised resource utilisation
- Cost savings
- Better responsiveness
- Faster cycle of innovation
- Resilience



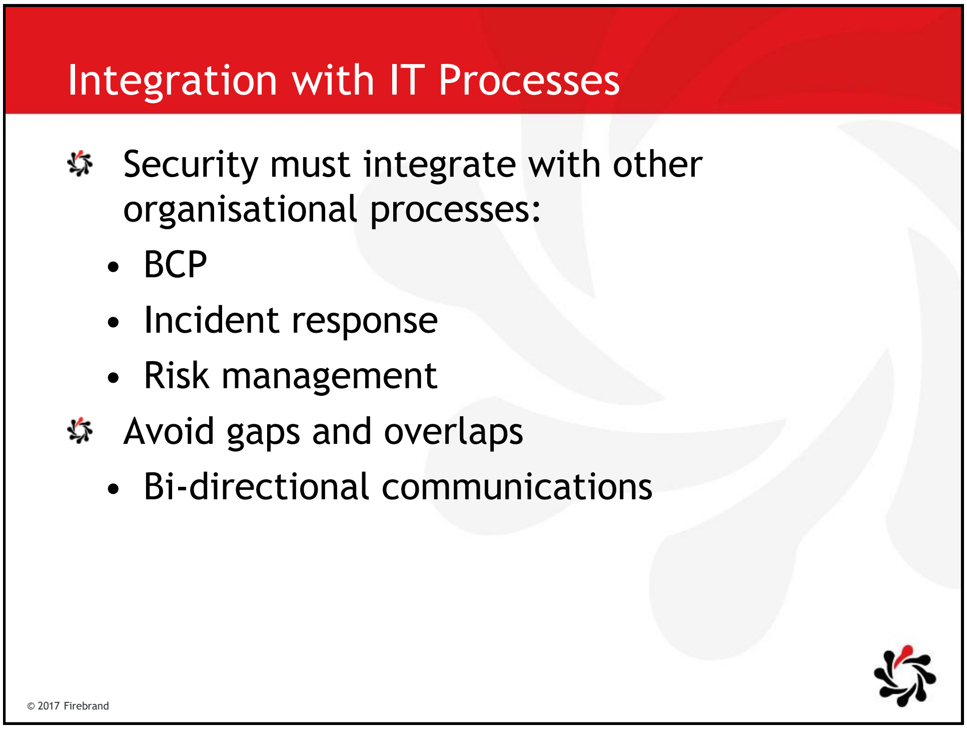
## Security Considerations

- Cloud provider security may be better than the security of organisation's with an immature security program
- Risk of loss of control over data
- Location of data may be restricted by law
- Incident handling may be more challenging



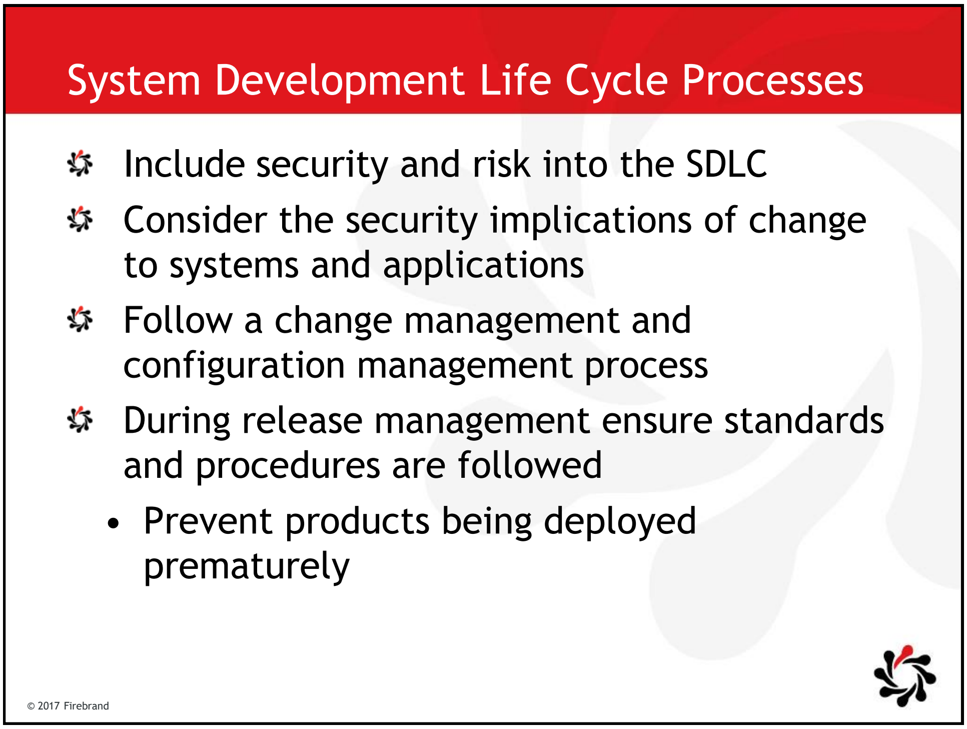
## Selecting a Cloud Service Provider

- Cost
- Data center provider
- Backbone transport
- Internet service provider (ISP)



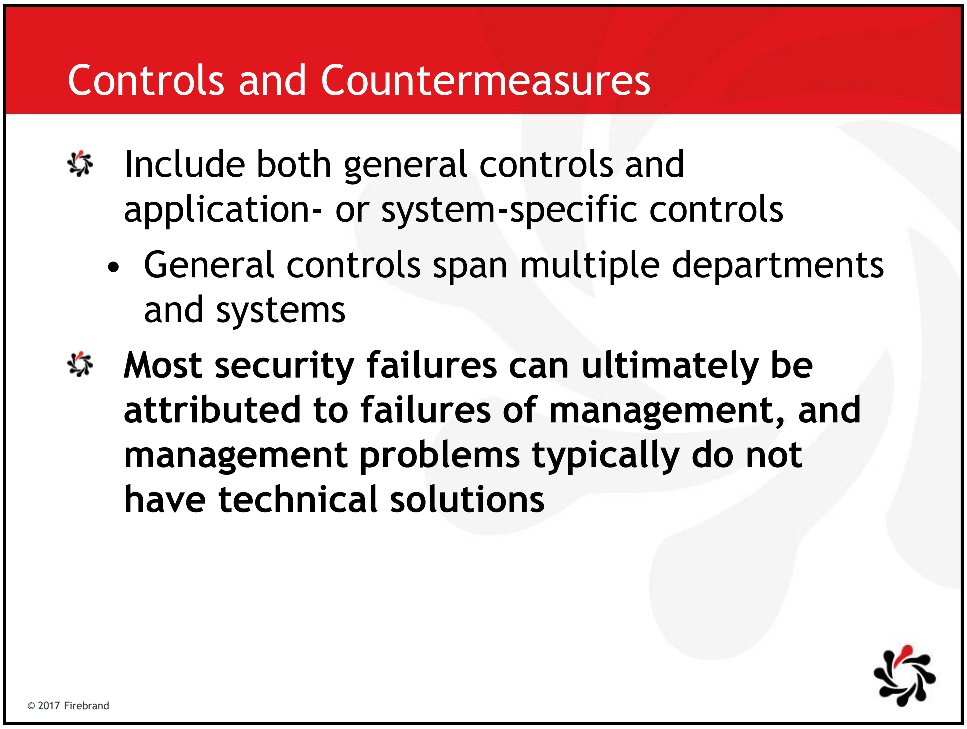
## Integration with IT Processes

- Security must integrate with other organisational processes:
  - BCP
  - Incident response
  - Risk management
- Avoid gaps and overlaps
  - Bi-directional communications



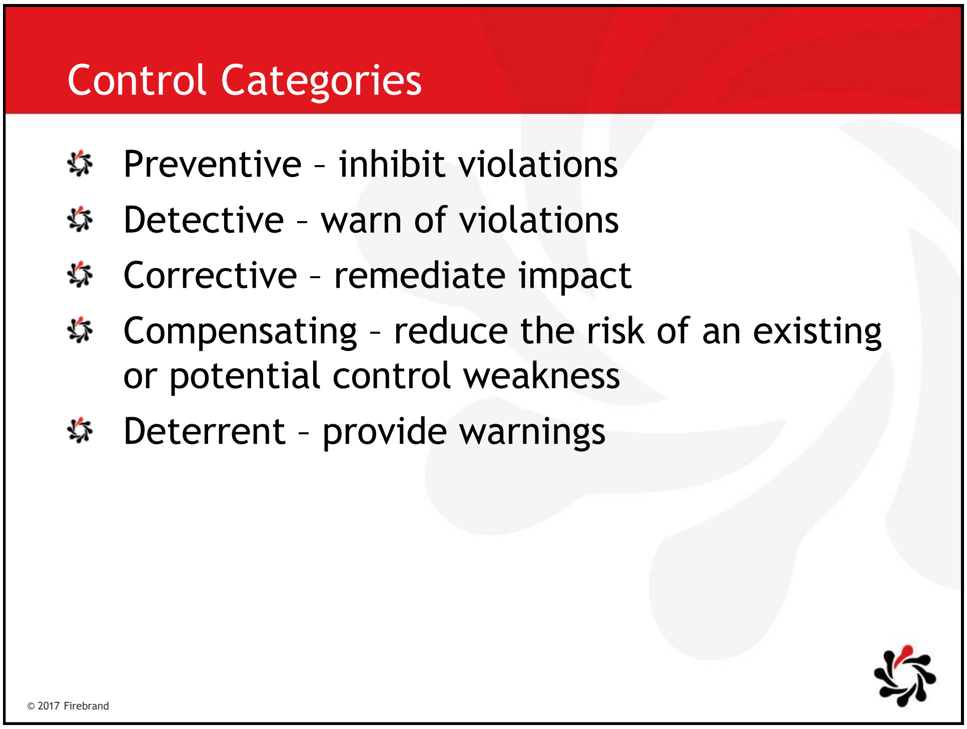
## System Development Life Cycle Processes

- Include security and risk into the SDLC
- Consider the security implications of change to systems and applications
- Follow a change management and configuration management process
- During release management ensure standards and procedures are followed
  - Prevent products being deployed prematurely



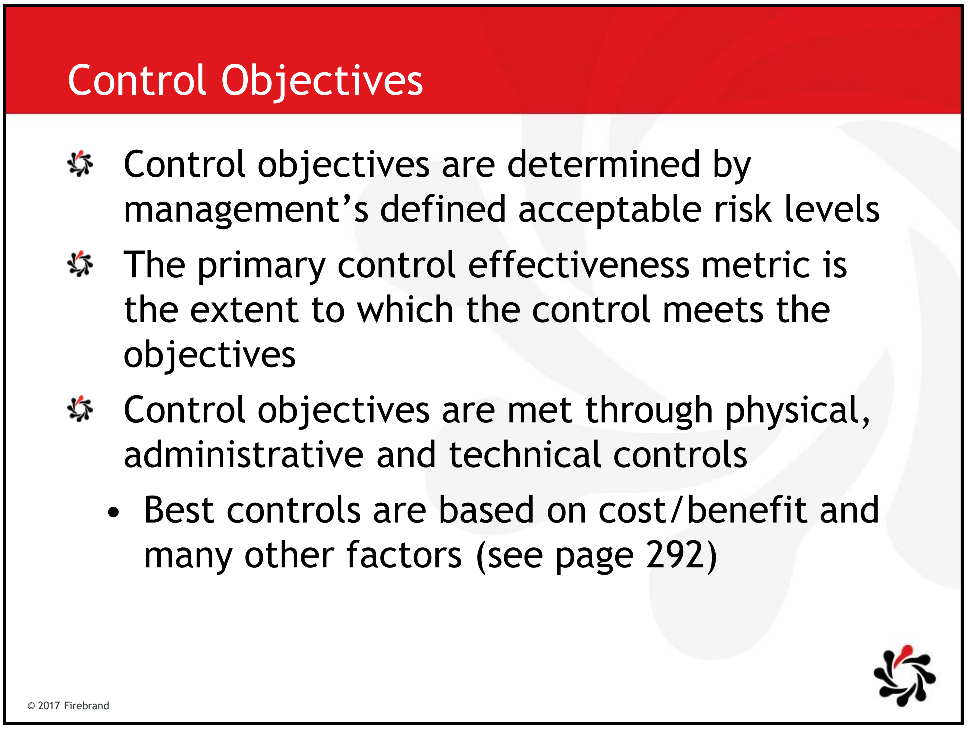
## Controls and Countermeasures

- Include both general controls and application- or system-specific controls
  - General controls span multiple departments and systems
- **Most security failures can ultimately be attributed to failures of management, and management problems typically do not have technical solutions**



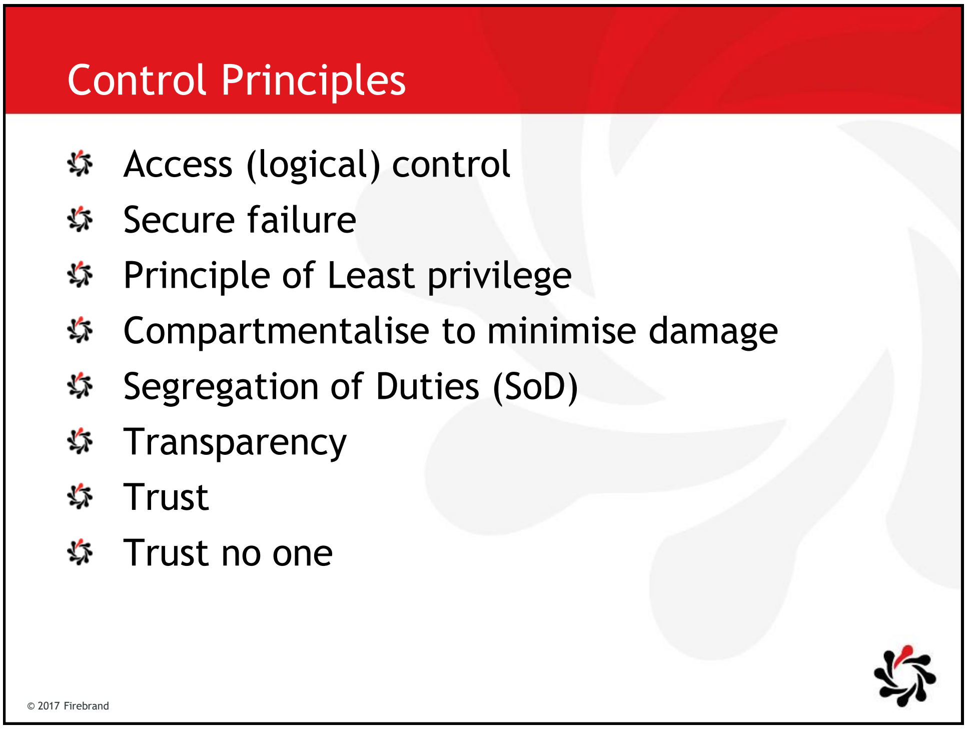
## Control Categories

- Preventive – inhibit violations
- Detective – warn of violations
- Corrective – remediate impact
- Compensating – reduce the risk of an existing or potential control weakness
- Deterrent – provide warnings



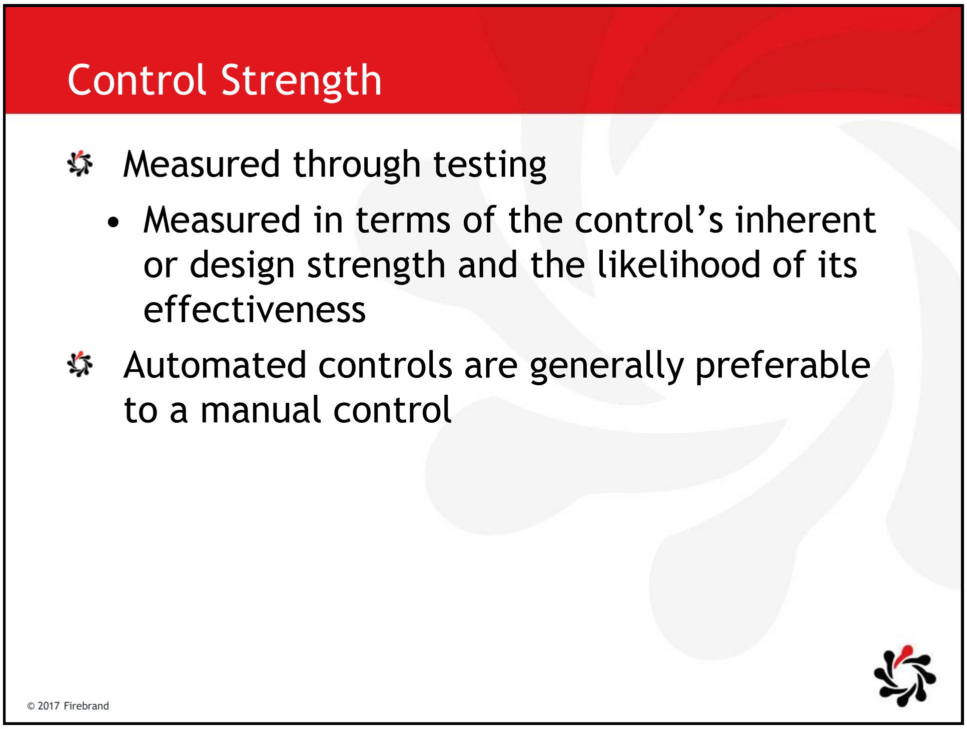
## Control Objectives

- Control objectives are determined by management’s defined acceptable risk levels
- The primary control effectiveness metric is the extent to which the control meets the objectives
- Control objectives are met through physical, administrative and technical controls
  - Best controls are based on cost/benefit and many other factors (see page 292)



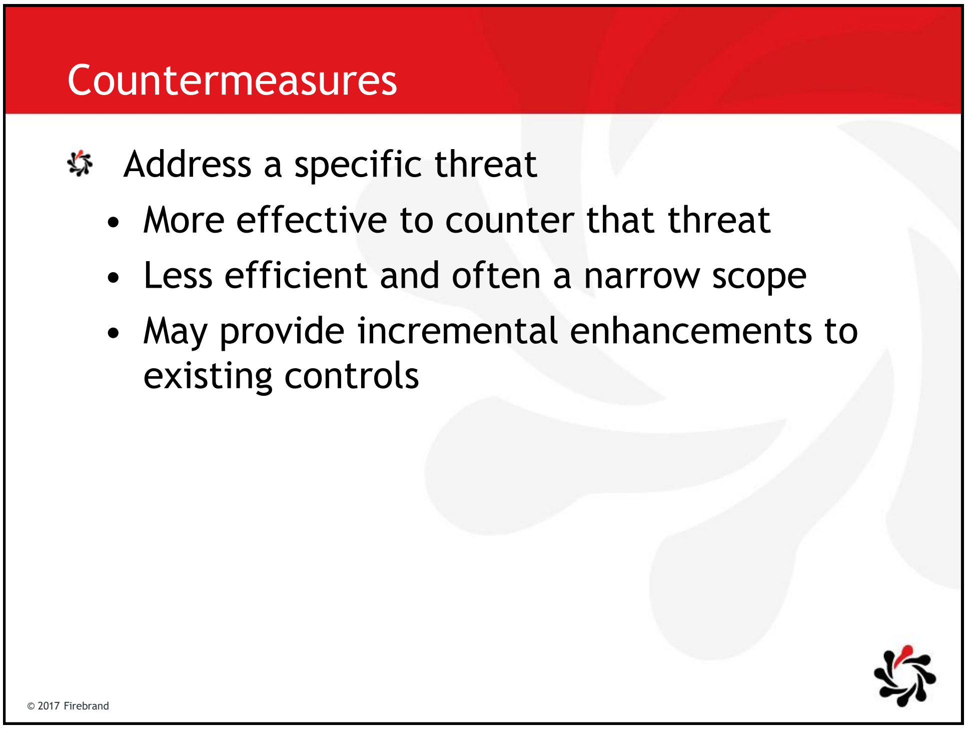
## Control Principles

- Access (logical) control
- Secure failure
- Principle of Least privilege
- Compartmentalise to minimise damage
- Segregation of Duties (SoD)
- Transparency
- Trust
- Trust no one



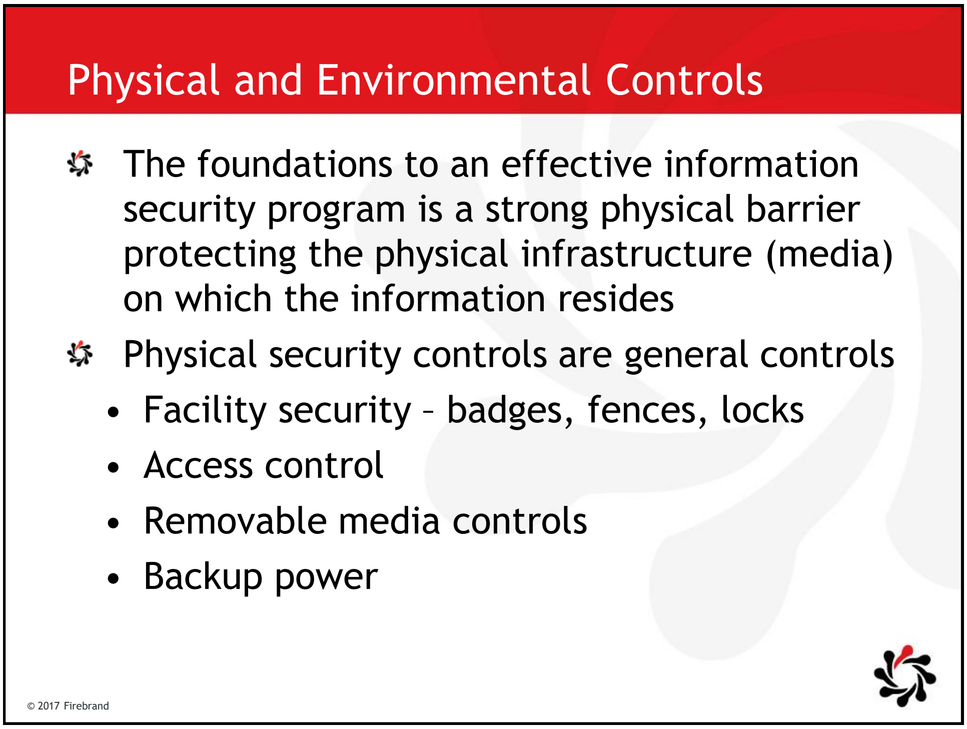
## Control Strength

- Measured through testing
  - Measured in terms of the control’s inherent or design strength and the likelihood of its effectiveness
- Automated controls are generally preferable to a manual control



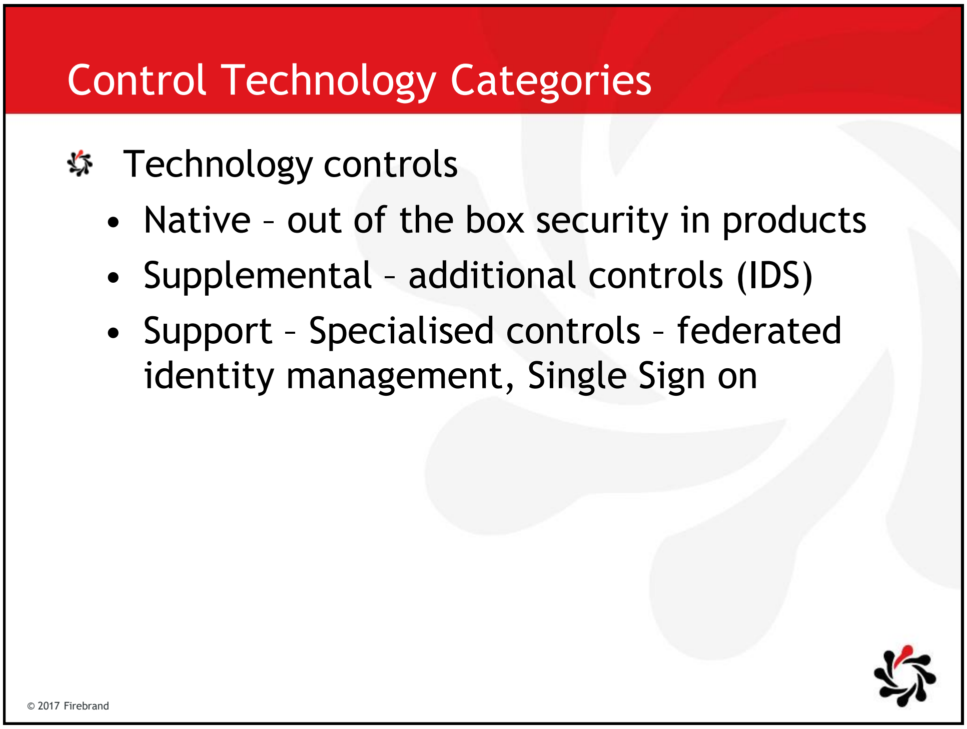
## Countermeasures

- Address a specific threat
  - More effective to counter that threat
  - Less efficient and often a narrow scope
  - May provide incremental enhancements to existing controls



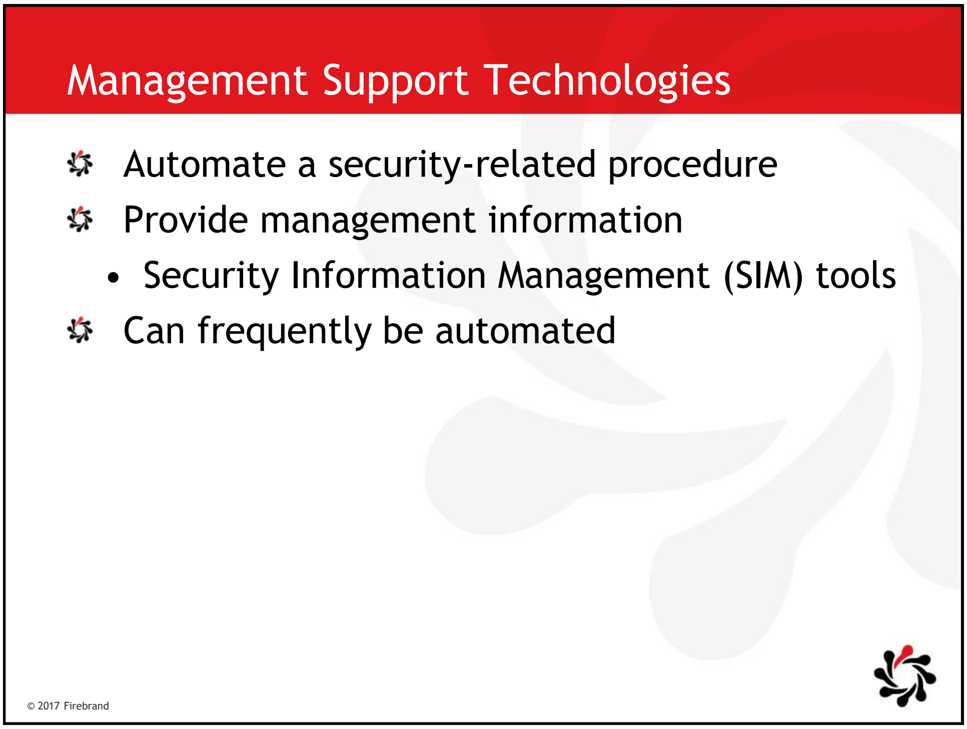
## Physical and Environmental Controls

- The foundations to an effective information security program is a strong physical barrier protecting the physical infrastructure (media) on which the information resides
- Physical security controls are general controls
  - Facility security – badges, fences, locks
  - Access control
  - Removable media controls
  - Backup power



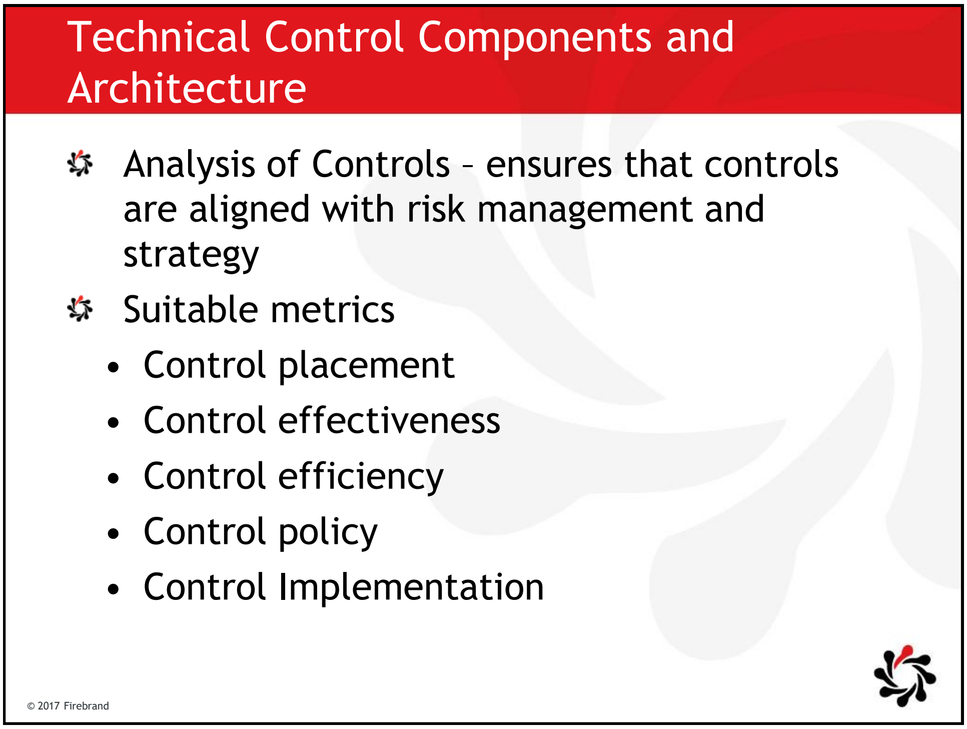
## Control Technology Categories

- Technology controls
  - Native – out of the box security in products
  - Supplemental – additional controls (IDS)
  - Support – Specialised controls – federated identity management, Single Sign on



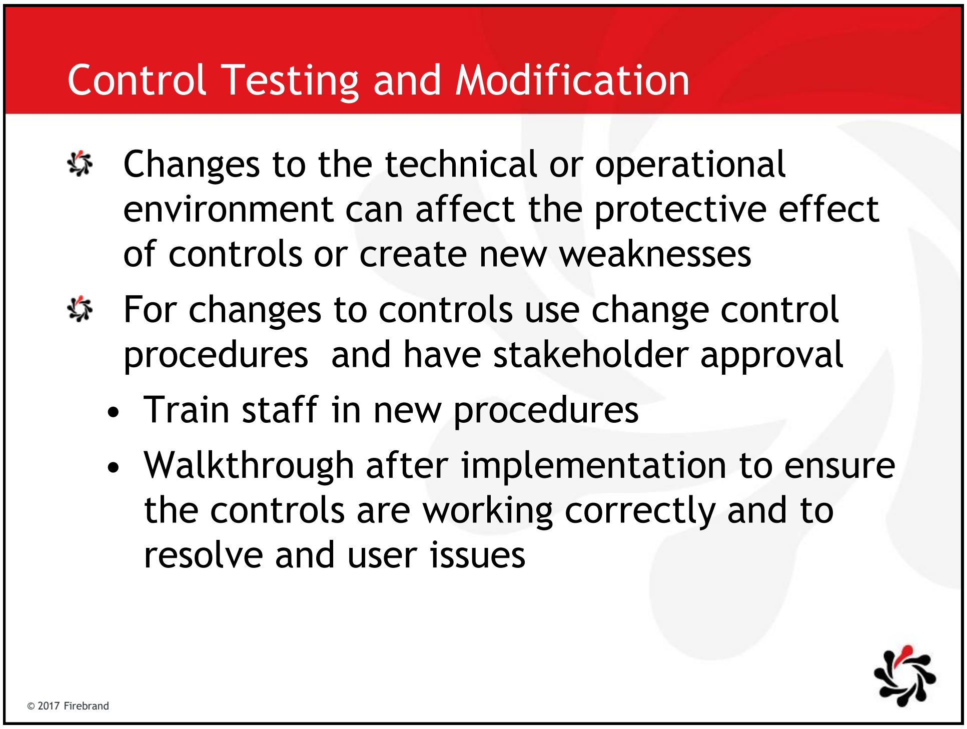
## Management Support Technologies

- Automate a security-related procedure
- Provide management information
  - Security Information Management (SIM) tools
- Can frequently be automated



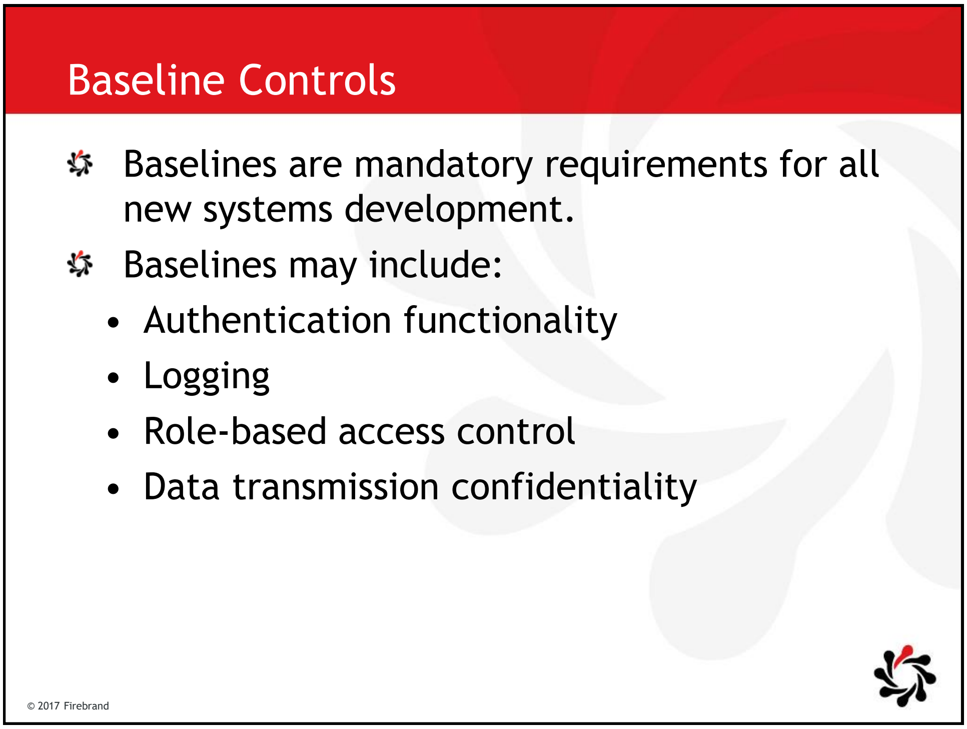
## Technical Control Components and Architecture

- Analysis of Controls – ensures that controls are aligned with risk management and strategy
- Suitable metrics
  - Control placement
  - Control effectiveness
  - Control efficiency
  - Control policy
  - Control Implementation



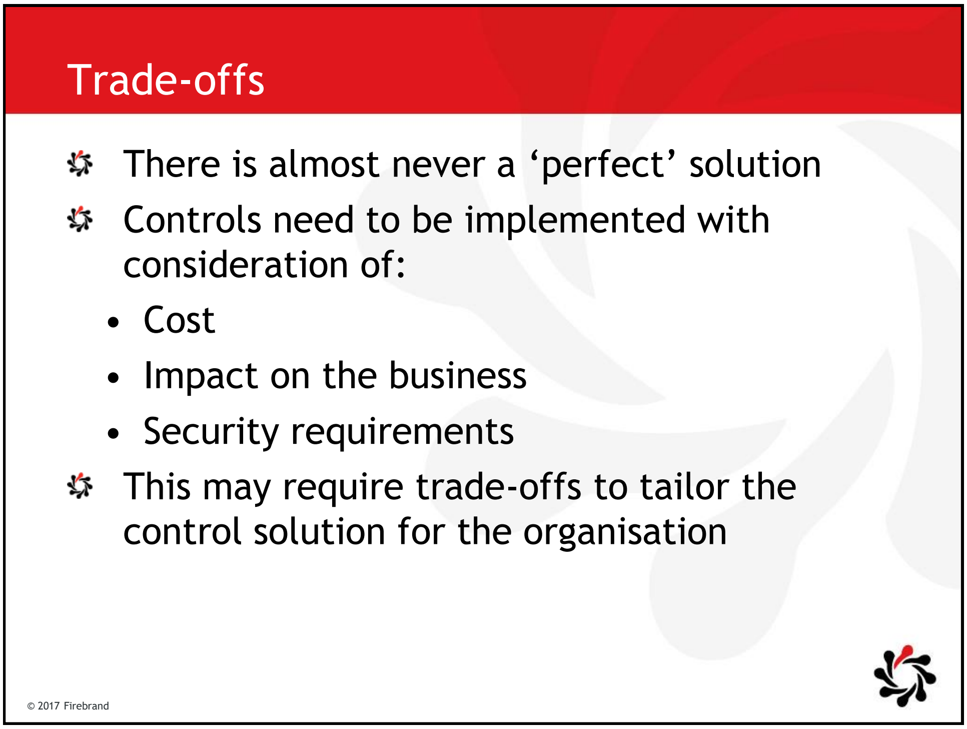
## Control Testing and Modification

- Changes to the technical or operational environment can affect the protective effect of controls or create new weaknesses
- For changes to controls use change control procedures  and have stakeholder approval
  - Train staff in new procedures
  - Walkthrough after implementation to ensure the controls are working correctly and to resolve and user issues



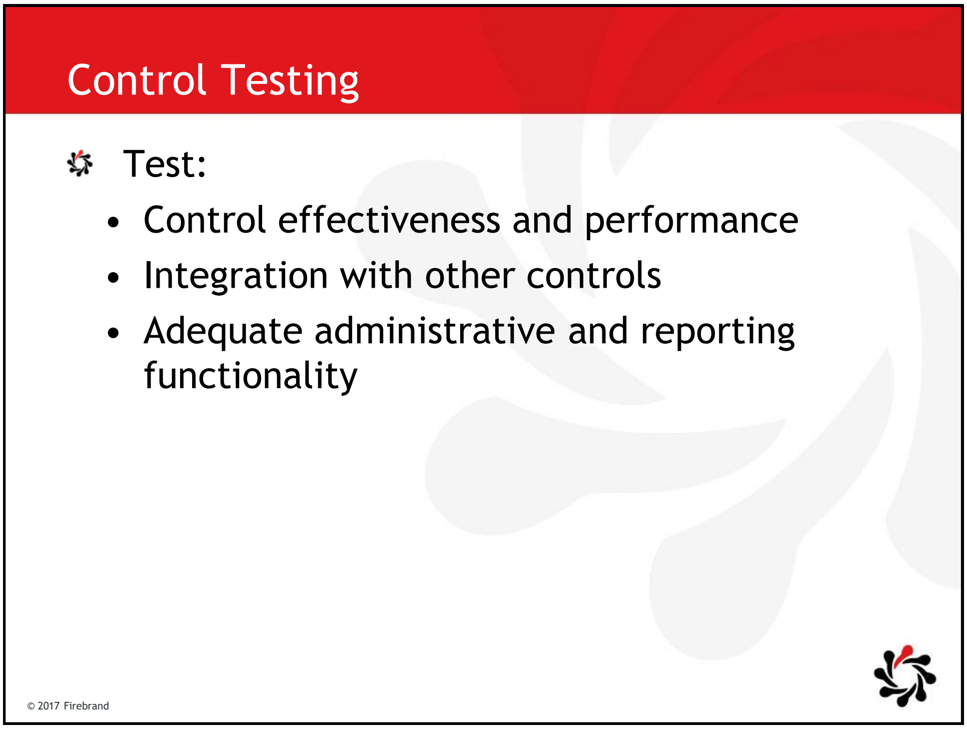
## Baseline Controls

- Baselines are mandatory requirements for all new systems development.
- Baselines may include:
  - Authentication functionality
  - Logging
  - Role-based access control
  - Data transmission confidentiality



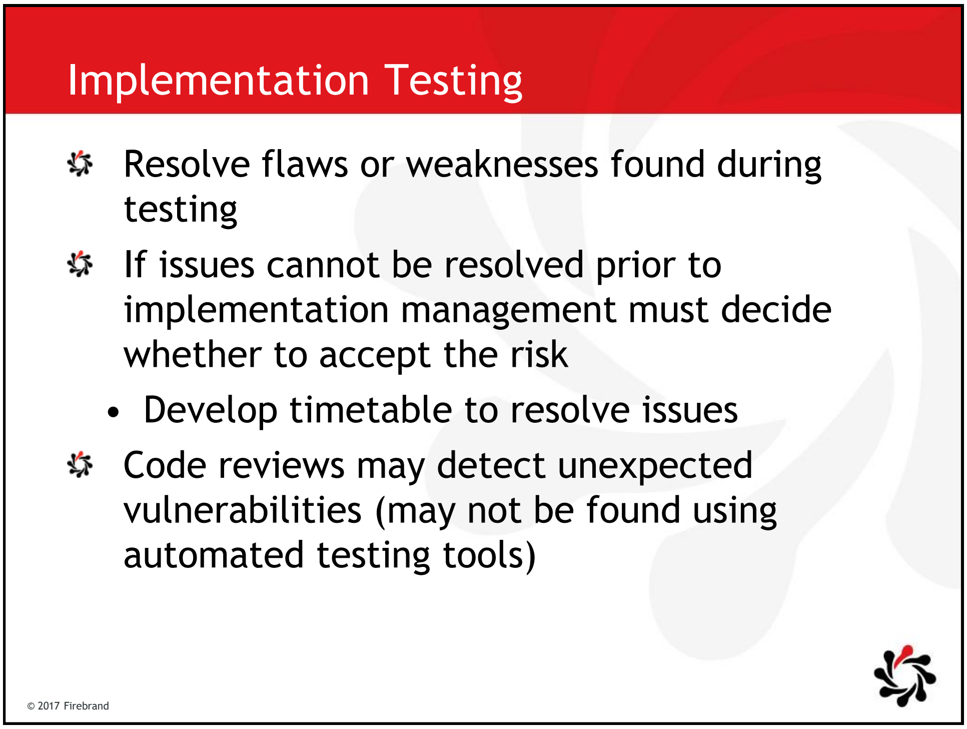
## Trade-offs

- There is almost never a ‘perfect’ solution
- Controls need to be implemented with consideration of:
  - Cost
  - Impact on the business
  - Security requirements
- This may require trade-offs to tailor the control solution for the organisation



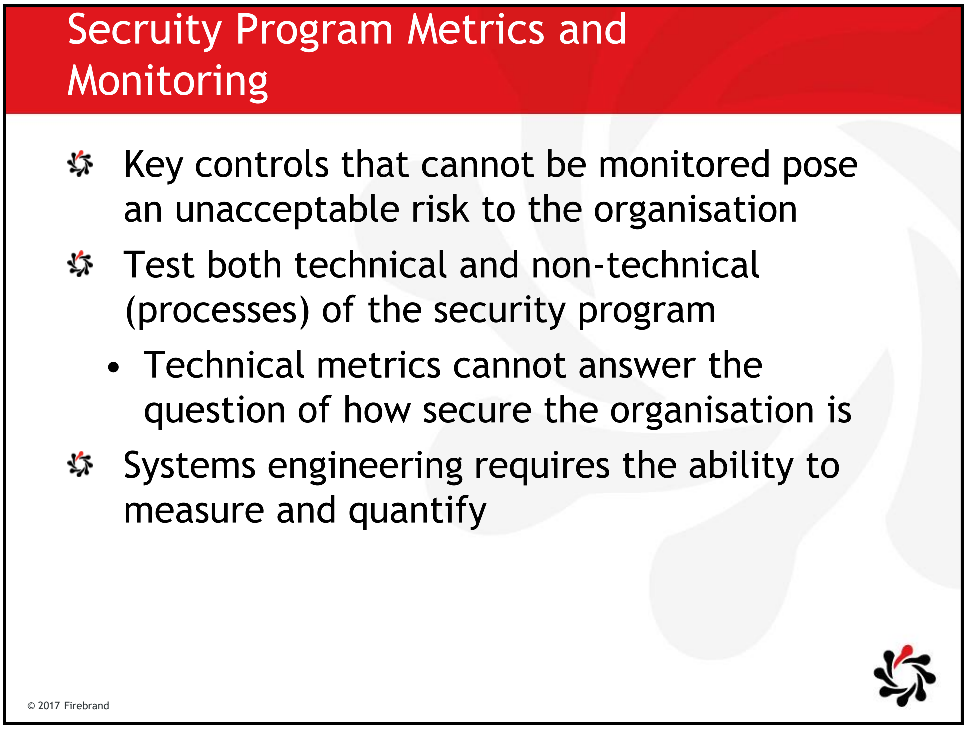
## Control Testing

- Test:
  - Control effectiveness and performance
  - Integration with other controls
  - Adequate administrative and reporting functionality



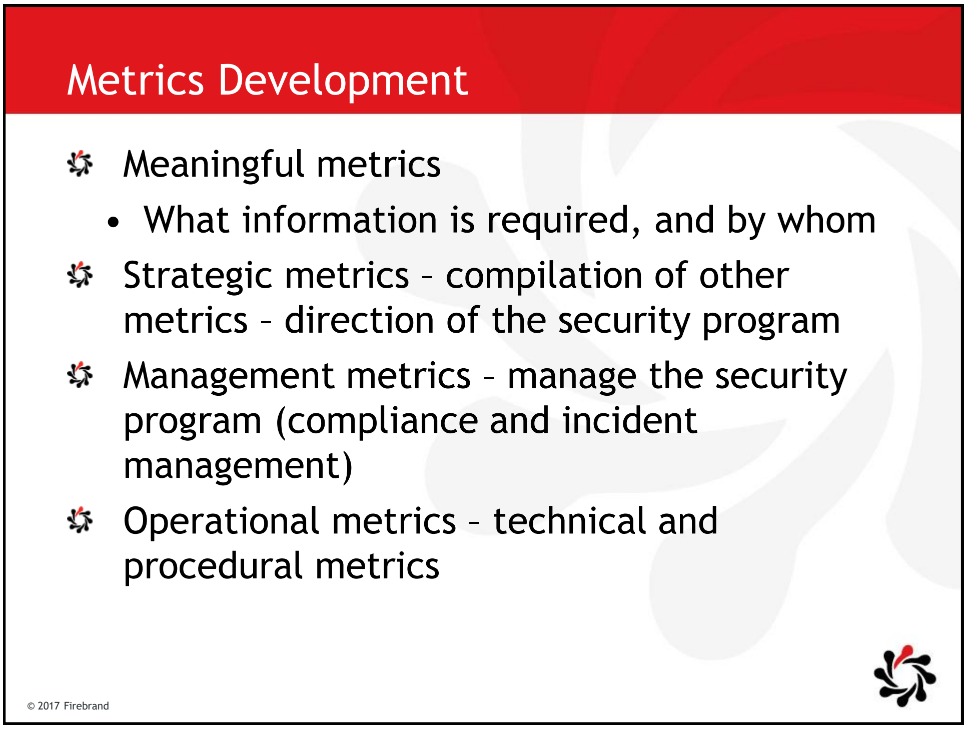
## Implementation Testing

- Resolve flaws or weaknesses found during testing
- If issues cannot be resolved prior to implementation management must decide whether to accept the risk
  - Develop timetable to resolve issues
- Code reviews may detect unexpected vulnerabilities (may not be found using automated testing tools)



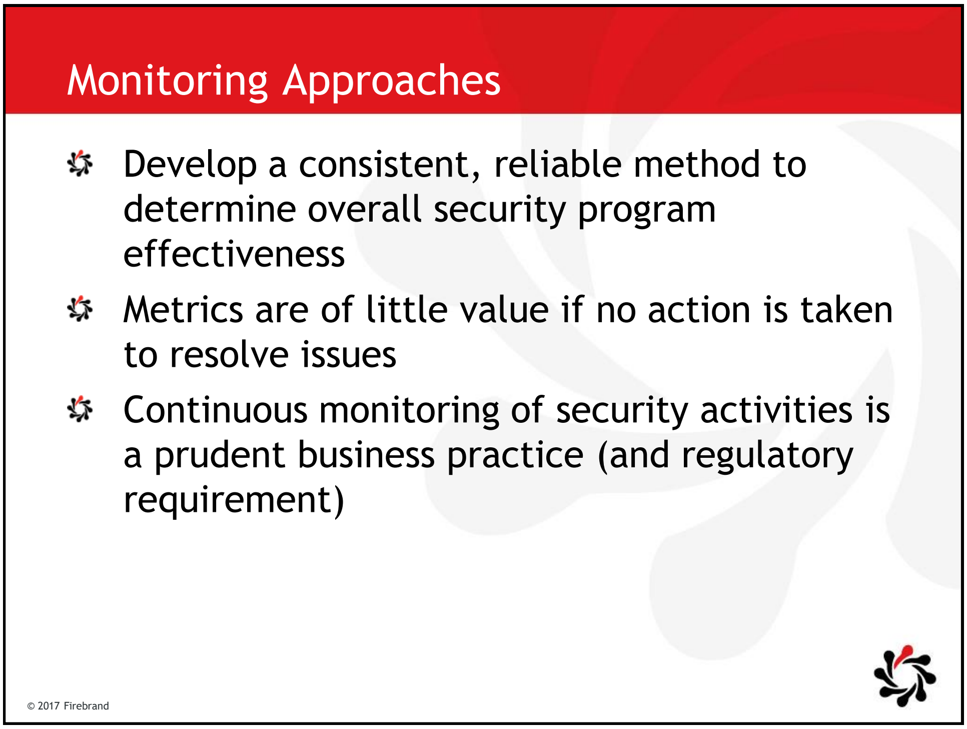
## Secruity Program Metrics and Monitoring

- Key controls that cannot be monitored pose an unacceptable risk to the organisation
- Test both technical and non-technical (processes) of the security program
  - Technical metrics cannot answer the question of how secure the organisation is
- Systems engineering requires the ability to measure and quantify



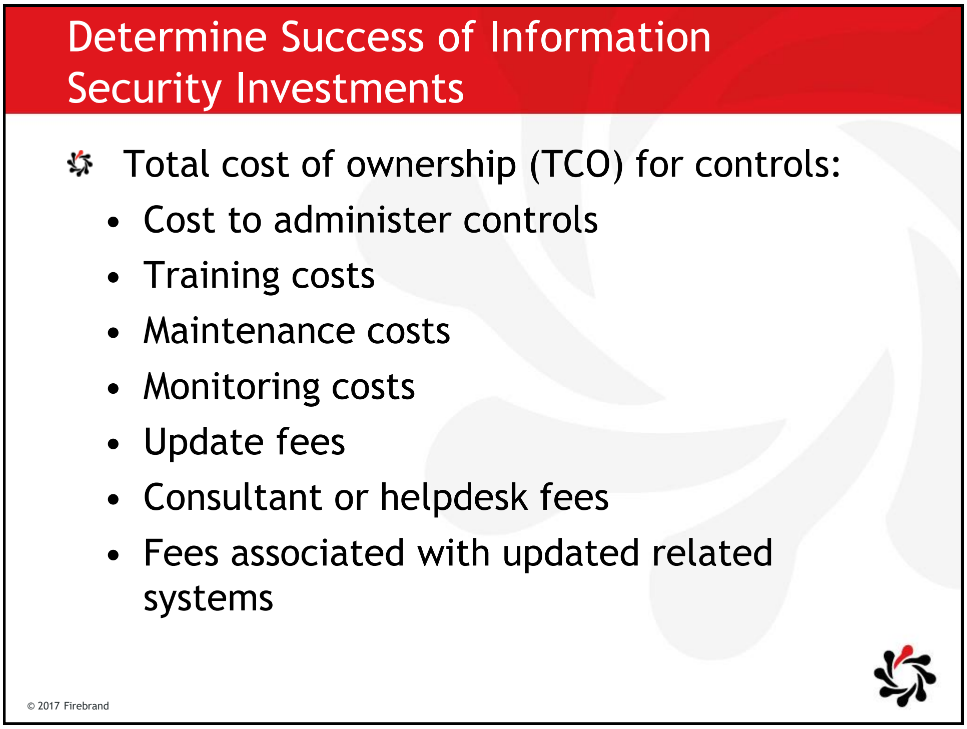
## Metrics Development

- Meaningful metrics
  - What information is required, and by whom
- Strategic metrics – compilation of other metrics – direction of the security program
- Management metrics – manage the security program (compliance and incident management)
- Operational metrics – technical and procedural metrics



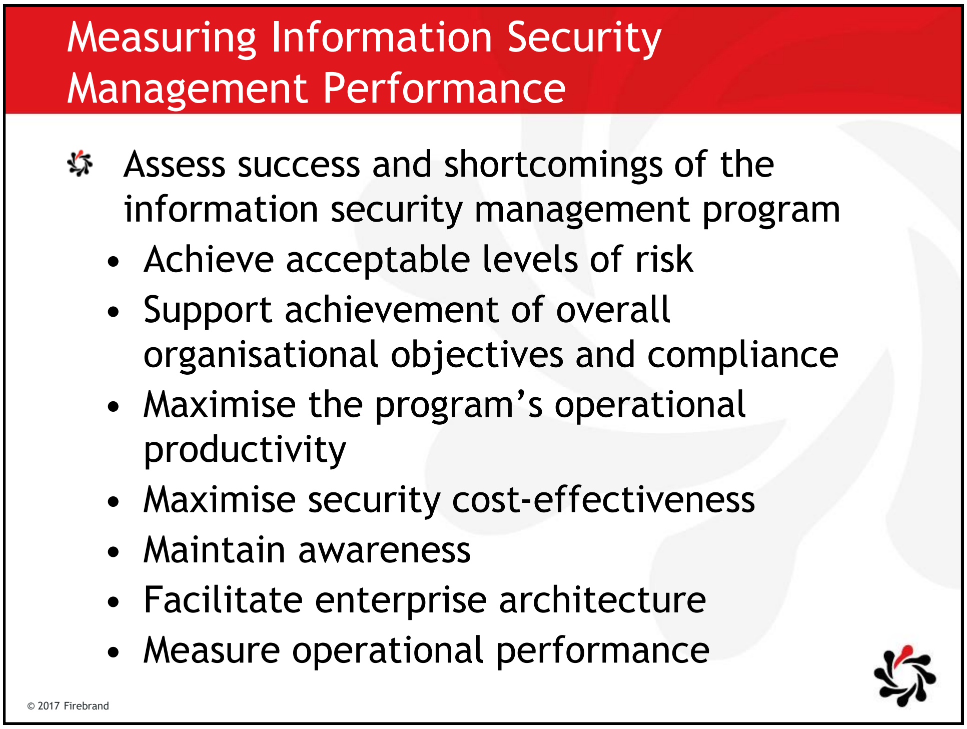
## Monitoring Approaches

- Develop a consistent, reliable method to determine overall security program effectiveness
- Metrics are of little value if no action is taken to resolve issues
- Continuous monitoring of security activities is a prudent business practice (and regulatory requirement)



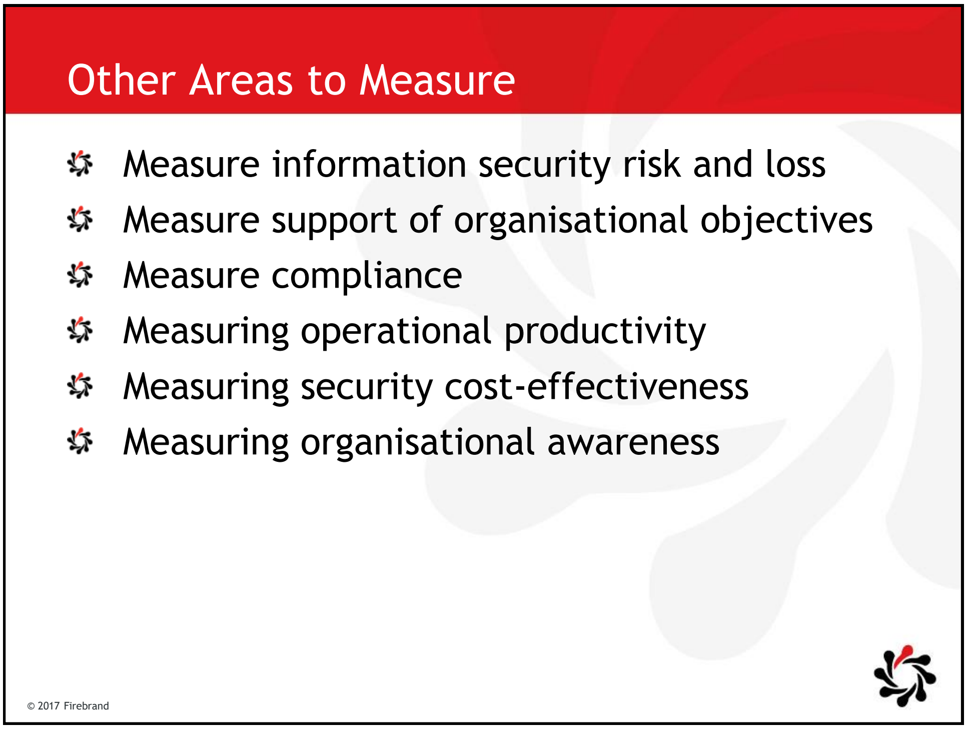
## Determine Success of Information Security Investments

- Total cost of ownership (TCO) for controls:
  - Cost to administer controls
  - Training costs
  - Maintenance costs
  - Monitoring costs
  - Update fees
  - Consultant or helpdesk fees
  - Fees associated with updated related systems



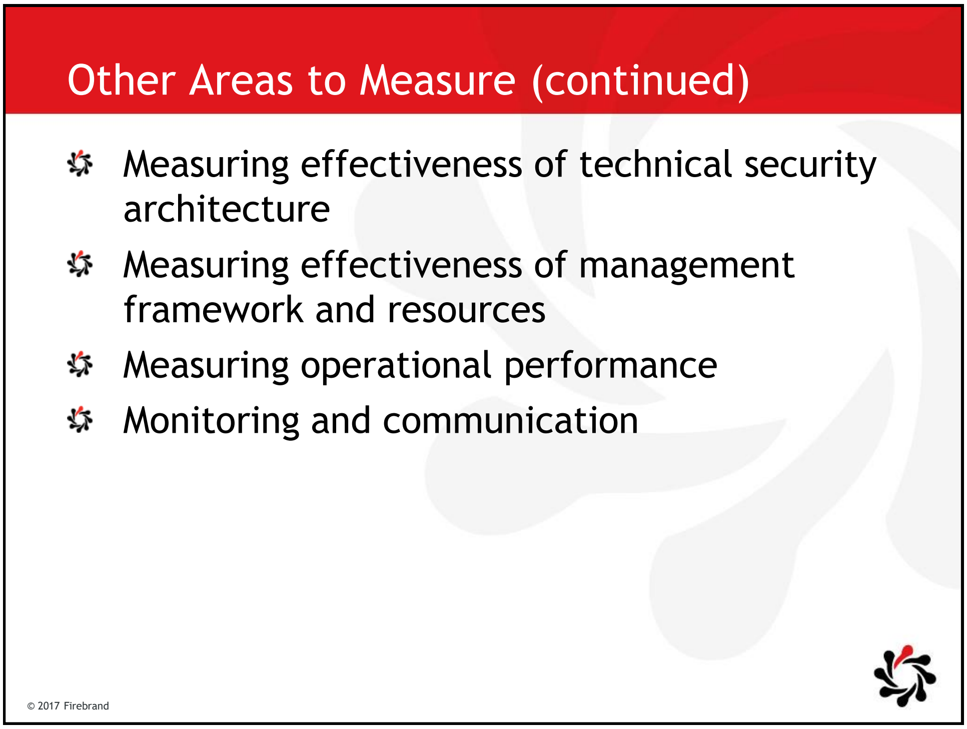
## Measuring Information Security Management Performance

- Assess success and shortcomings of the information security management program
  - Achieve acceptable levels of risk
  - Support achievement of overall organisational objectives and compliance
  - Maximise the program’s operational productivity
  - Maximise security cost-effectiveness
  - Maintain awareness
  - Facilitate enterprise architecture
  - Measure operational performance



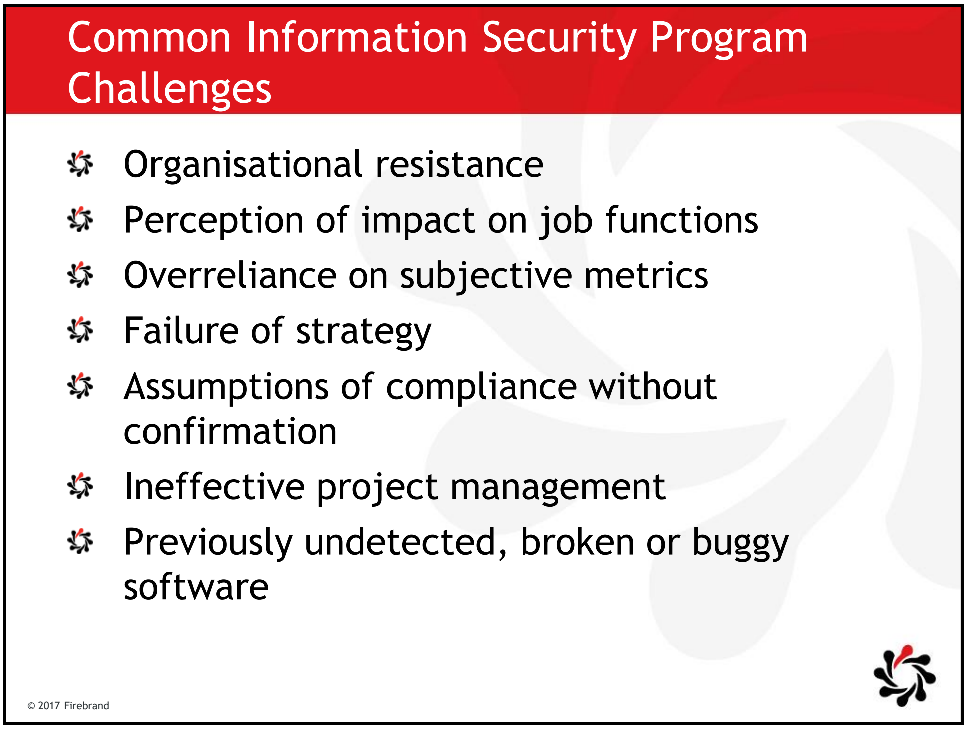
## Other Areas to Measure

- Measure information security risk and loss
- Measure support of organisational objectives
- Measure compliance
- Measuring operational productivity
- Measuring security cost-effectiveness
- Measuring organisational awareness



## Other Areas to Measure (continued)

- Measuring effectiveness of technical security architecture
- Measuring effectiveness of management framework and resources
- Measuring operational performance
- Monitoring and communication

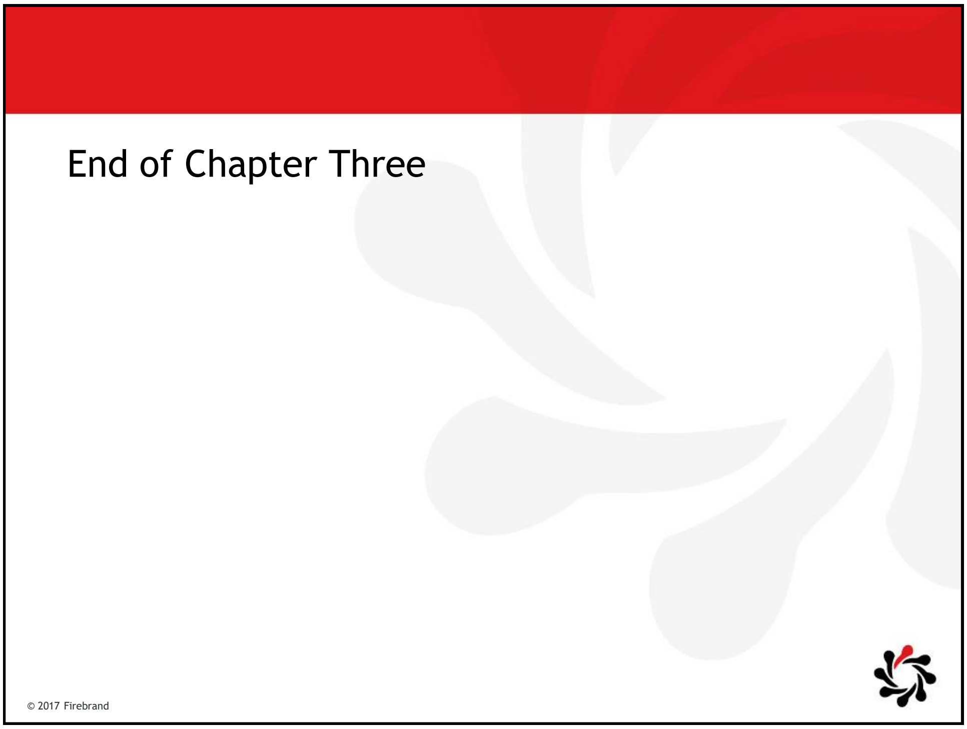


## Common Information Security Program Challenges

- Organisational resistance
- Perception of impact on job functions
- Overreliance on subjective metrics
- Failure of strategy
- Assumptions of compliance without confirmation
- Ineffective project management
- Previously undetected, broken or buggy software

## Improving Security

- Start from where the organisation is
- Educate
- Gain agreement and consensus
- Align with business objectives
- Develop meaningful metrics
- Gain management support
- Justify funding
- Develop and train staff

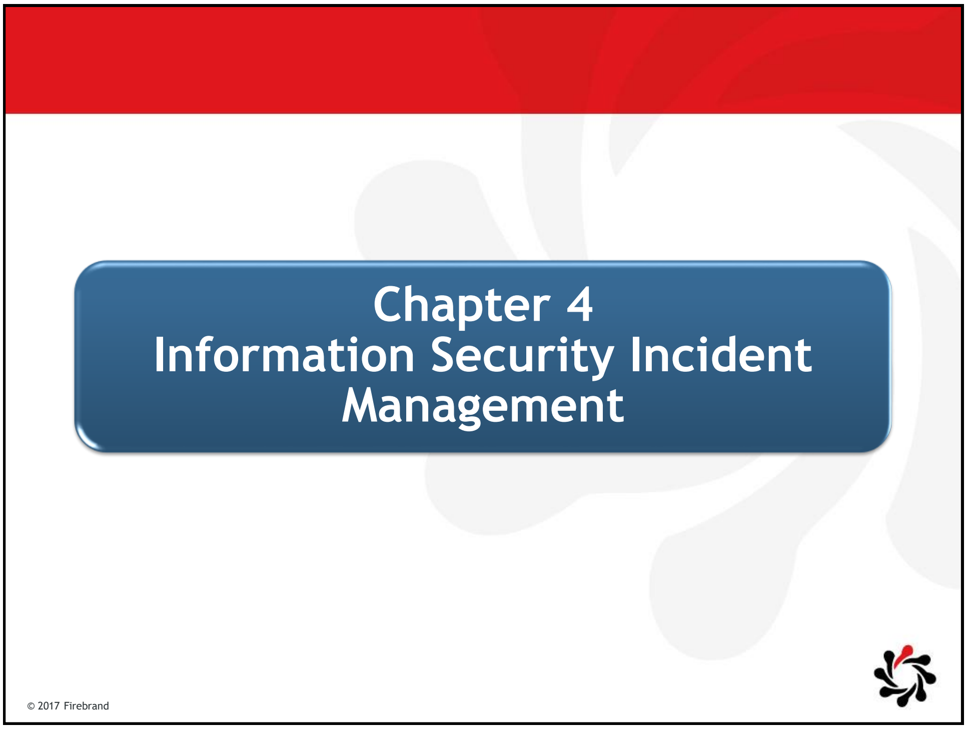


## End of Chapter Three

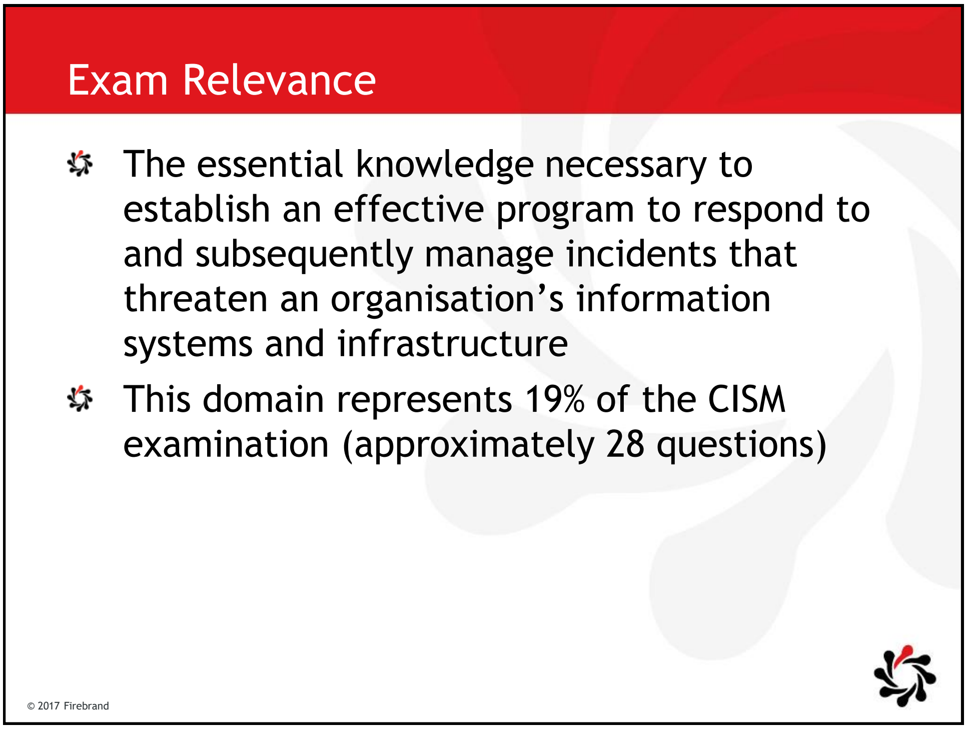
# CISM™

## Certified Information Security Manager

Firebrand Custom Designed Courseware

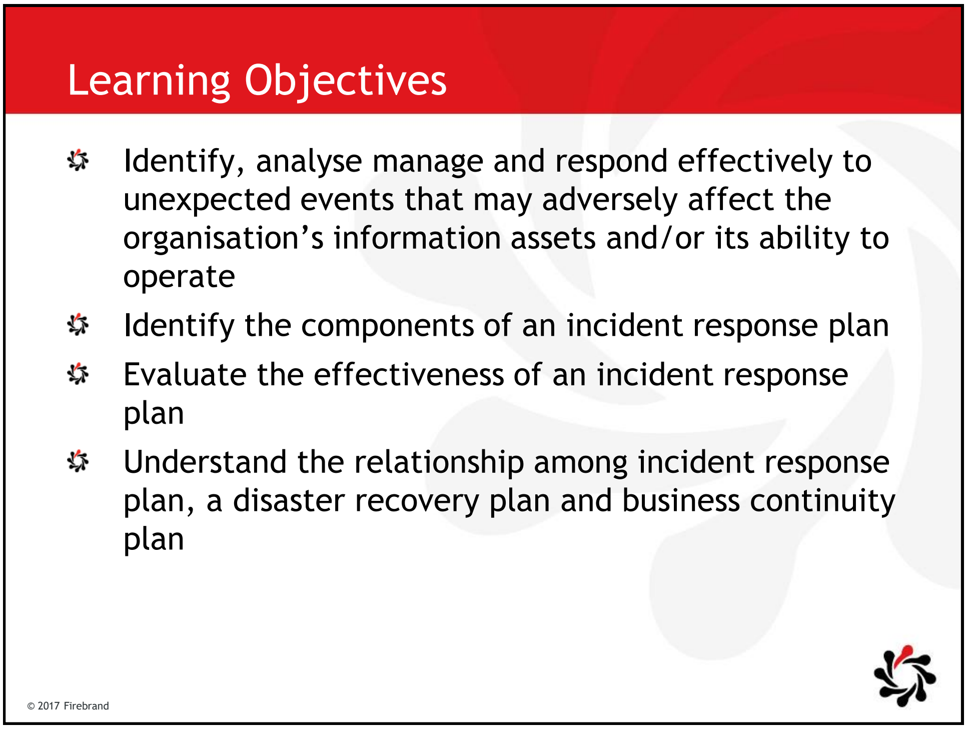


## Chapter 4 Information Security Incident Management



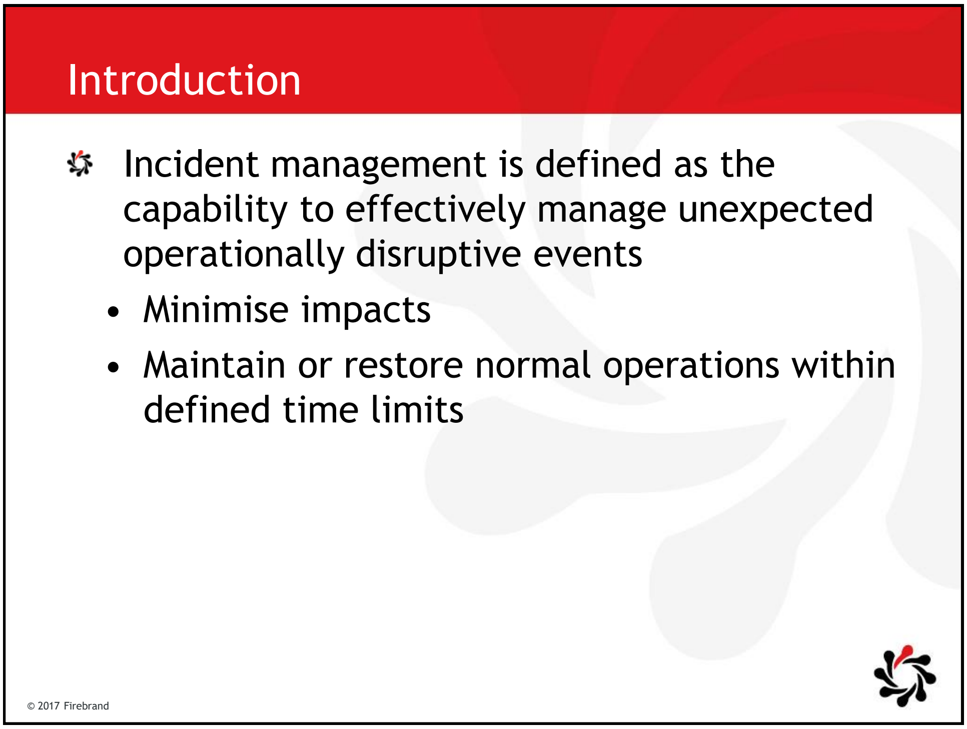
## Exam Relevance

- The essential knowledge necessary to establish an effective program to respond to and subsequently manage incidents that threaten an organisation’s information systems and infrastructure
- This domain represents 19% of the CISM examination (approximately 28 questions)



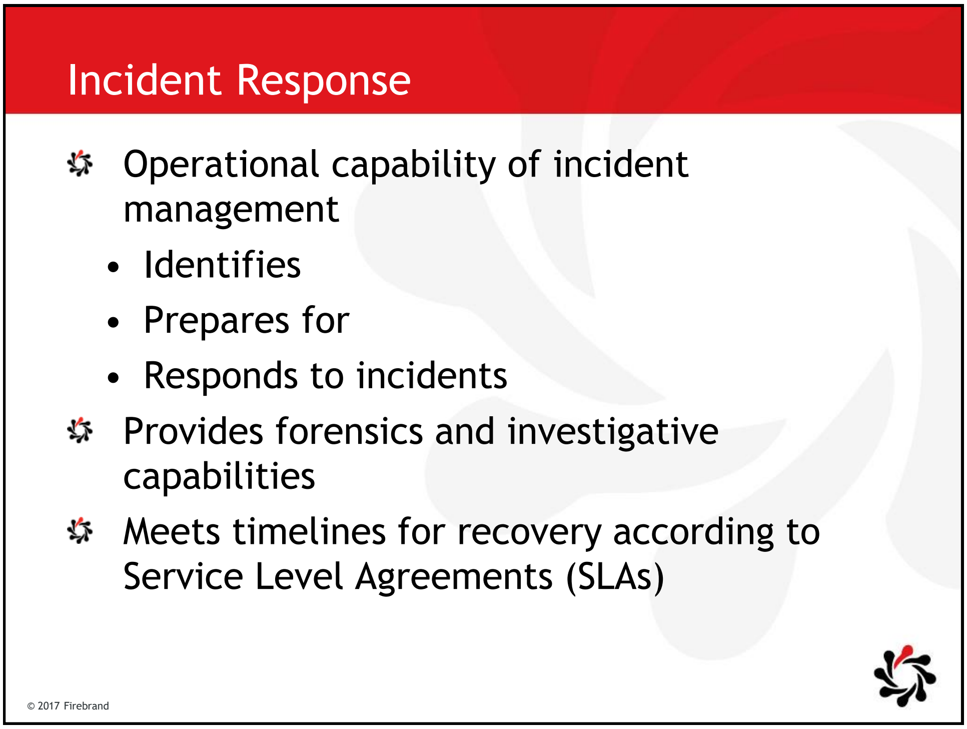
## Learning Objectives

- Identify, analyse manage and respond effectively to unexpected events that may adversely affect the organisation’s information assets and/or its ability to operate
- Identify the components of an incident response plan
- Evaluate the effectiveness of an incident response plan
- Understand the relationship among incident response plan, a disaster recovery plan and business continuity plan



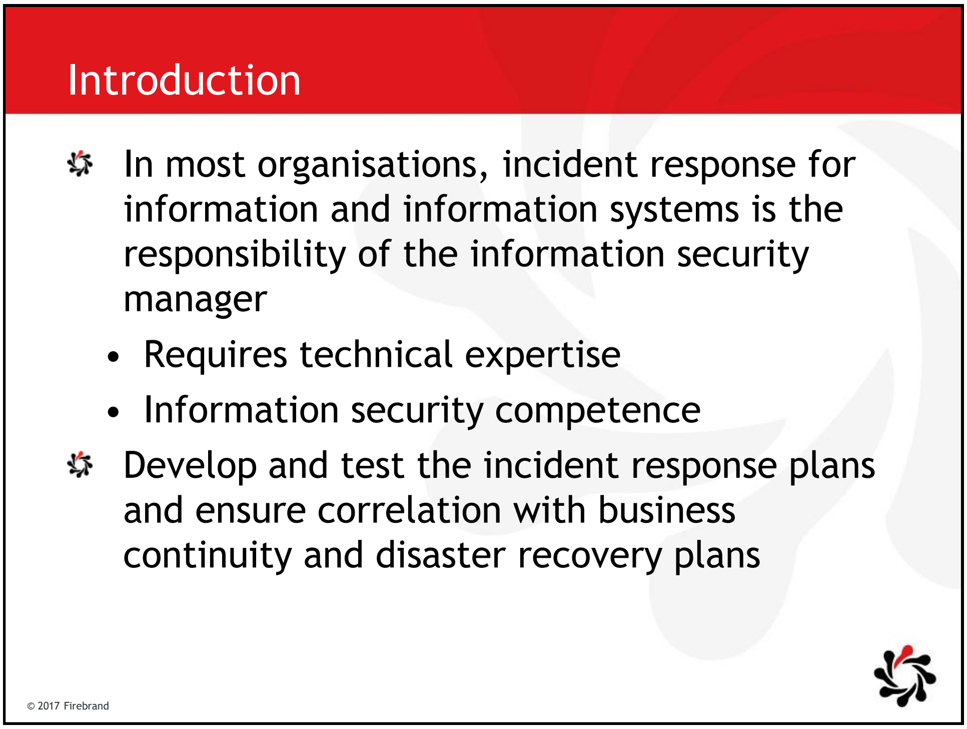
## Introduction

- Incident management is defined as the capability to effectively manage unexpected operationally disruptive events
  - Minimise impacts
  - Maintain or restore normal operations within defined time limits



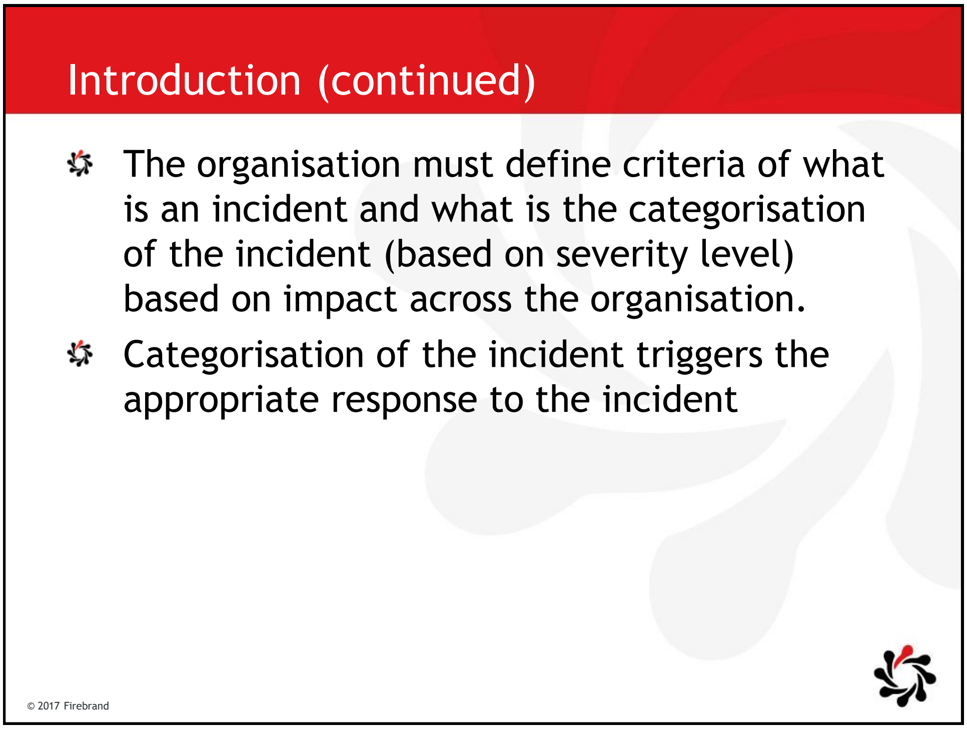
## Incident Response

- Operational capability of incident management
  - Identifies
  - Prepares for
  - Responds to incidents
- Provides forensics and investigative capabilities
- Meets timelines for recovery according to Service Level Agreements (SLAs)



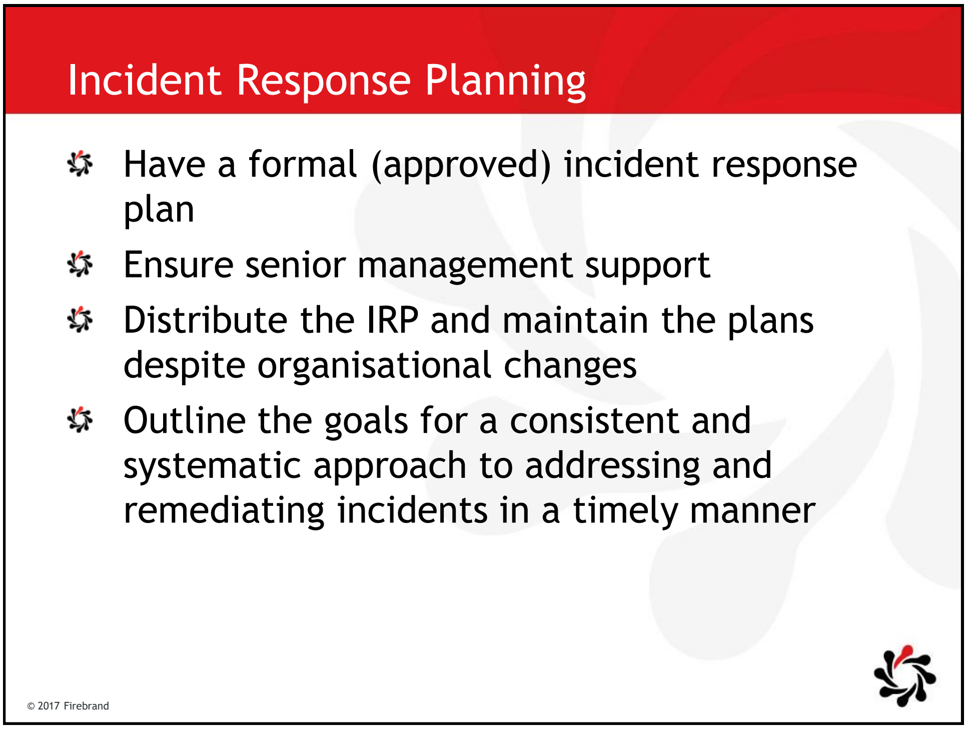
## Introduction

- In most organisations, incident response for information and information systems is the responsibility of the information security manager
  - Requires technical expertise
  - Information security competence
- Develop and test the incident response plans and ensure correlation with business continuity and disaster recovery plans



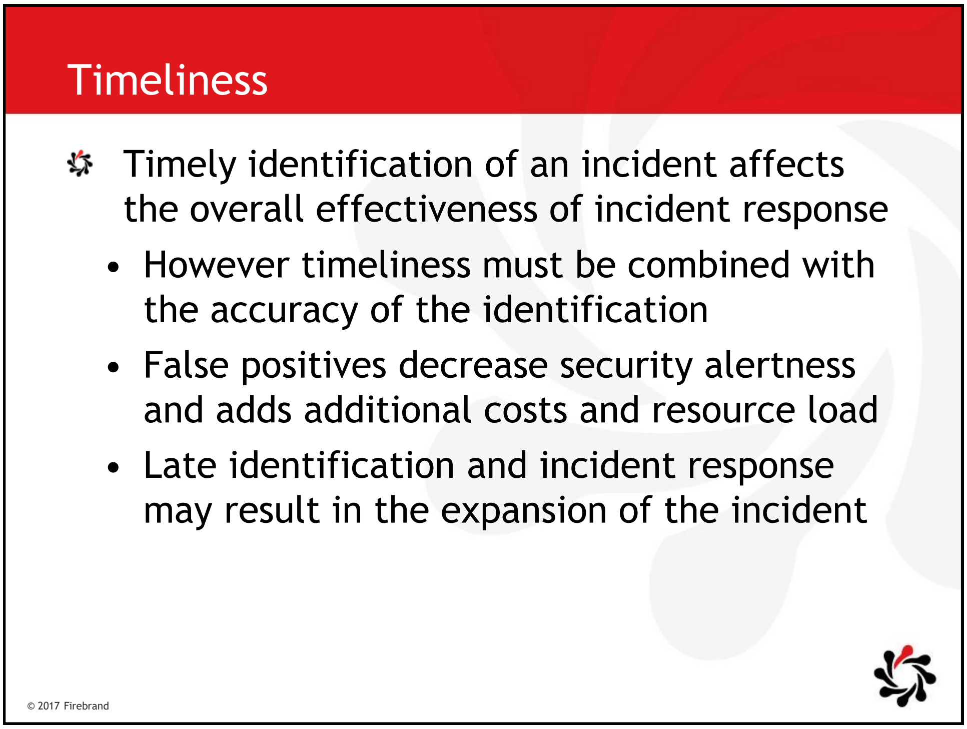
## Introduction (continued)

- The organisation must define criteria of what is an incident and what is the categorisation of the incident (based on severity level) based on impact across the organisation.
- Categorisation of the incident triggers the appropriate response to the incident



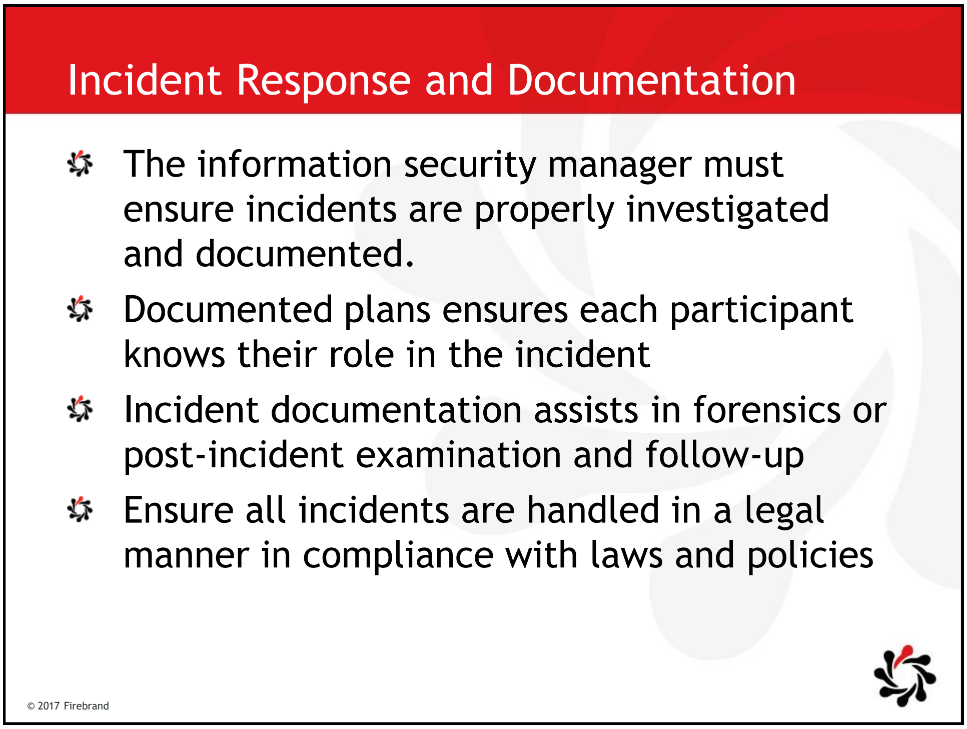
## Incident Response Planning

- Have a formal (approved) incident response plan
- Ensure senior management support
- Distribute the IRP and maintain the plans despite organisational changes
- Outline the goals for a consistent and systematic approach to addressing and remediating incidents in a timely manner



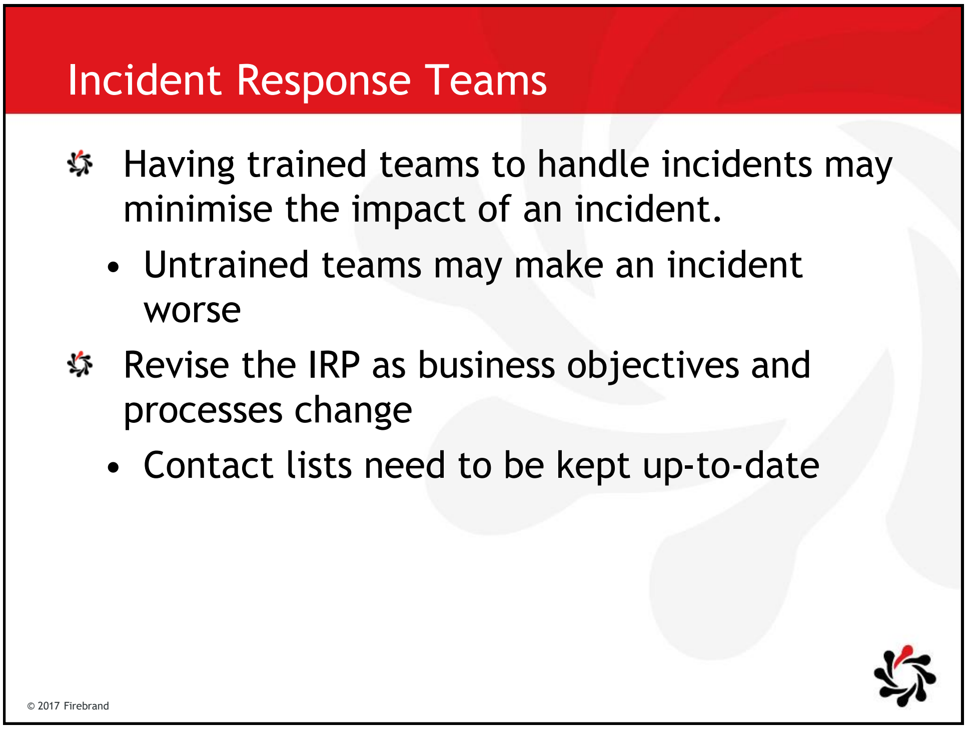
## Timeliness

- Timely identification of an incident affects the overall effectiveness of incident response
  - However timeliness must be combined with the accuracy of the identification
  - False positives decrease security alertness and adds additional costs and resource load
  - Late identification and incident response may result in the expansion of the incident



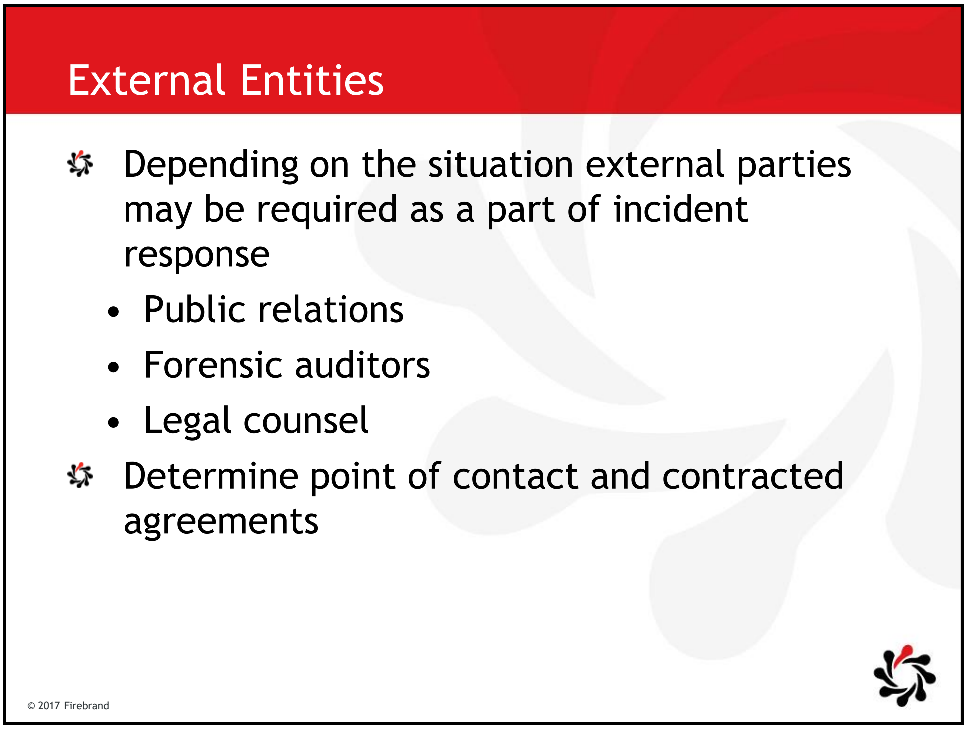
## Incident Response and Documentation

- The information security manager must ensure incidents are properly investigated and documented.
- Documented plans ensures each participant knows their role in the incident
- Incident documentation assists in forensics or post-incident examination and follow-up
- Ensure all incidents are handled in a legal manner in compliance with laws and policies



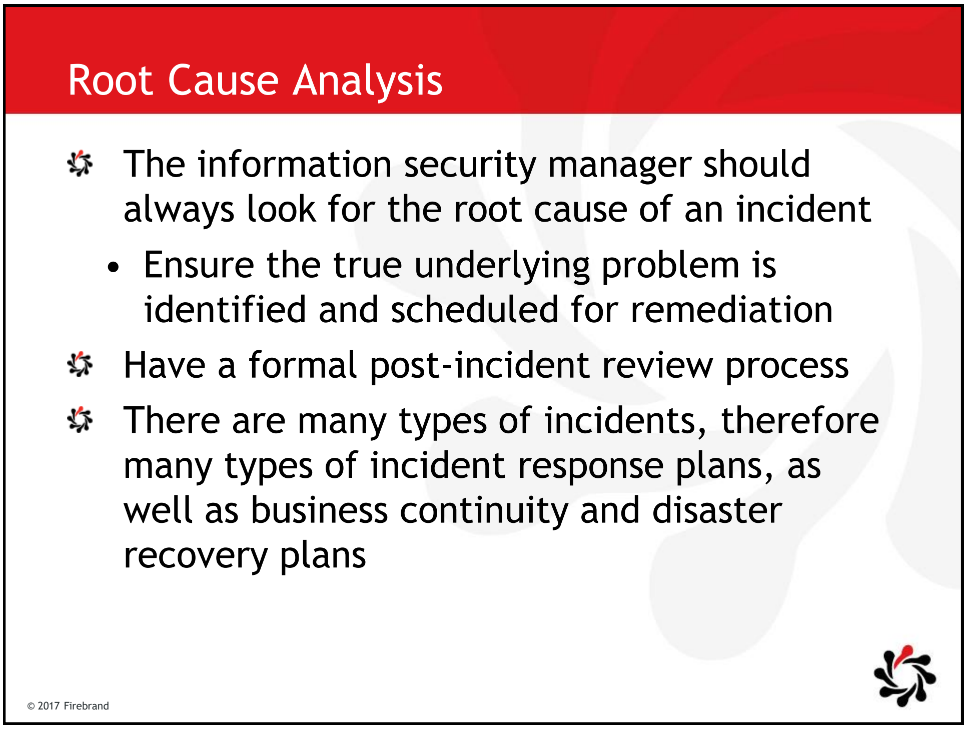
## Incident Response Teams

- Having trained teams to handle incidents may minimise the impact of an incident.
  - Untrained teams may make an incident worse
- Revise the IRP as business objectives and processes change
  - Contact lists need to be kept up-to-date



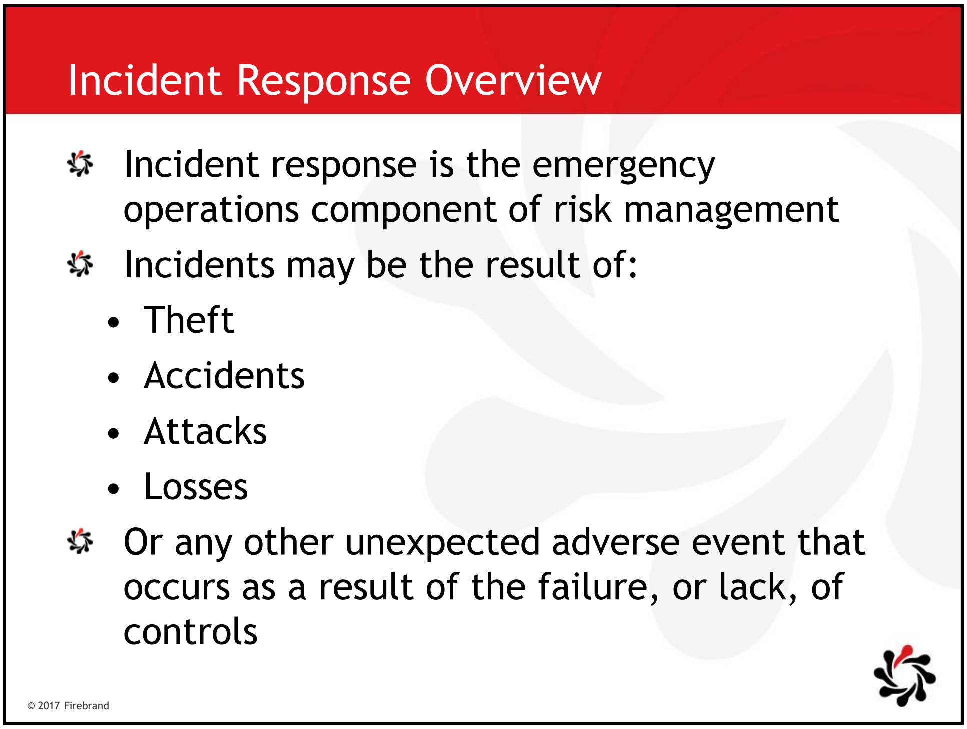
## External Entities

- Depending on the situation external parties may be required as a part of incident response
  - Public relations
  - Forensic auditors
  - Legal counsel
- Determine point of contact and contracted agreements



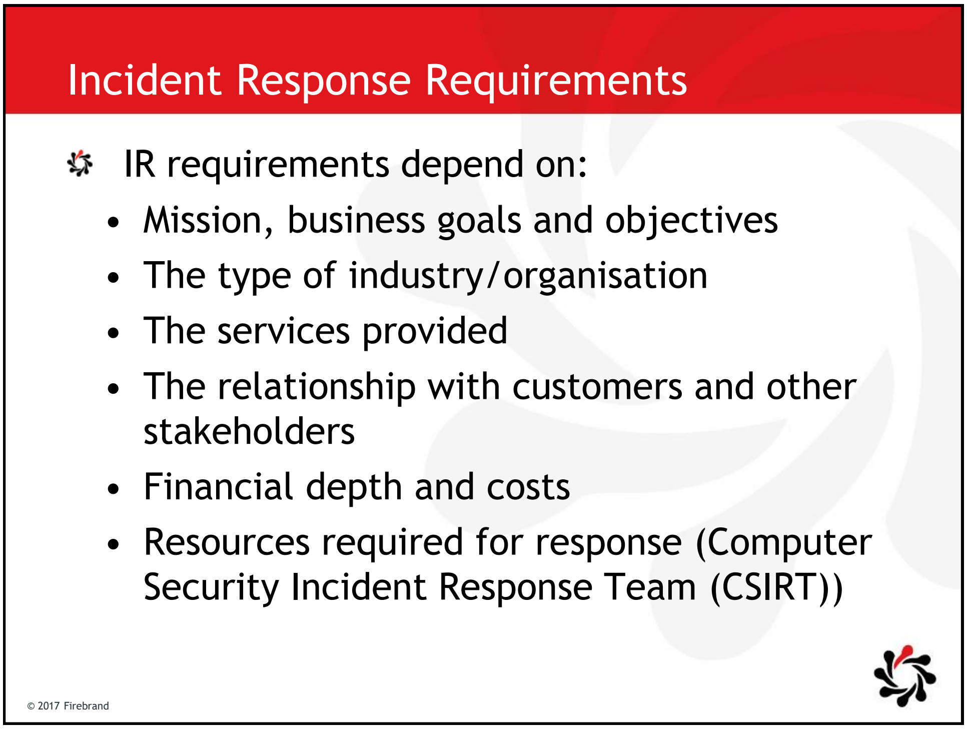
## Root Cause Analysis

- The information security manager should always look for the root cause of an incident
  - Ensure the true underlying problem is identified and scheduled for remediation
- Have a formal post-incident review process
- There are many types of incidents, therefore many types of incident response plans, as well as business continuity and disaster recovery plans



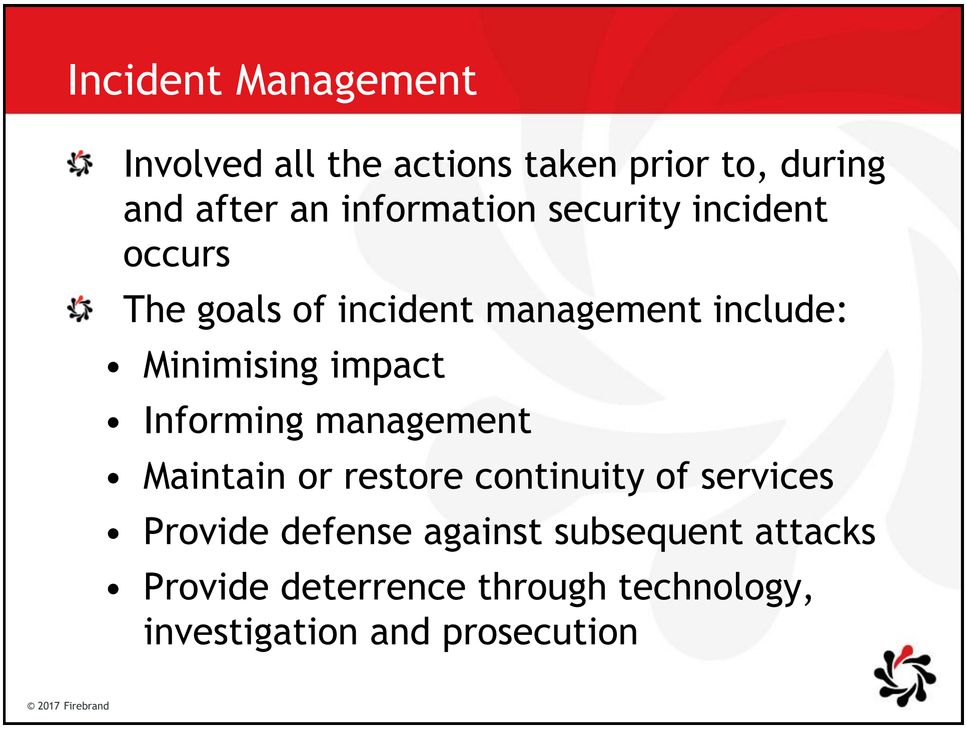
## Incident Response Overview

- Incident response is the emergency operations component of risk management
- Incidents may be the result of:
  - Theft
  - Accidents
  - Attacks
  - Losses
- Or any other unexpected adverse event that occurs as a result of the failure, or lack, of controls



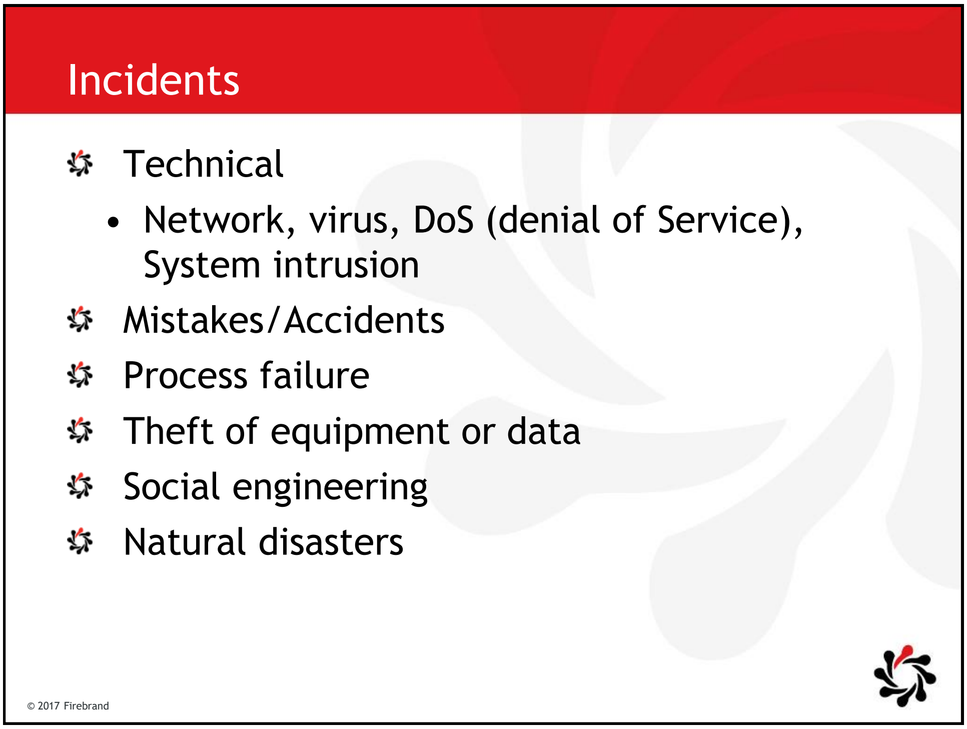
## Incident Response Requirements

- IR requirements depend on:
  - Mission, business goals and objectives
  - The type of industry/organisation
  - The services provided
  - The relationship with customers and other stakeholders
  - Financial depth and costs
  - Resources required for response (Computer Security Incident Response Team (CSIRT))



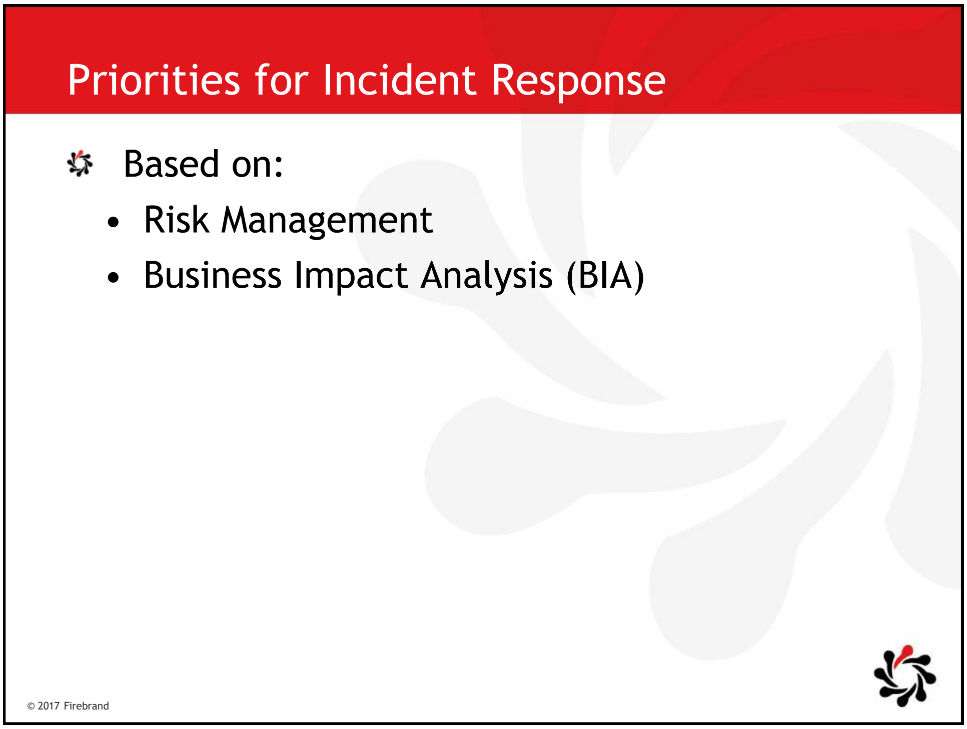
## Incident Management

- Involved all the actions taken prior to, during and after an information security incident occurs
- The goals of incident management include:
  - Minimising impact
  - Informing management
  - Maintain or restore continuity of services
  - Provide defense against subsequent attacks
  - Provide deterrence through technology, investigation and prosecution



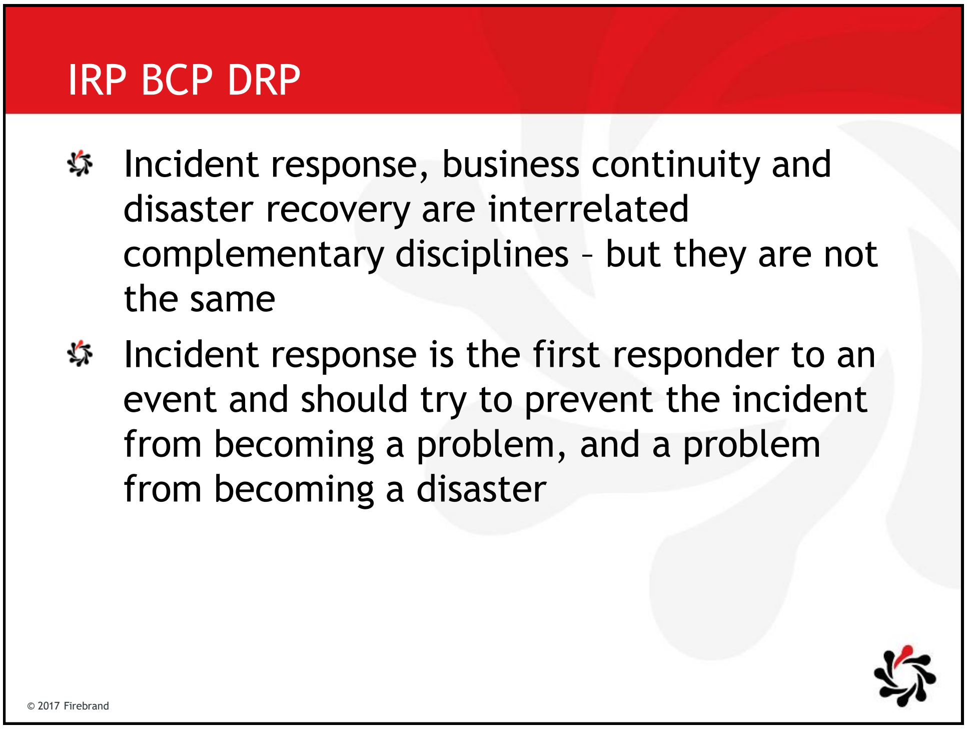
## Incidents

- Technical
  - Network, virus, DoS (denial of Service), System intrusion
- Mistakes/Accidents
- Process failure
- Theft of equipment or data
- Social engineering
- Natural disasters



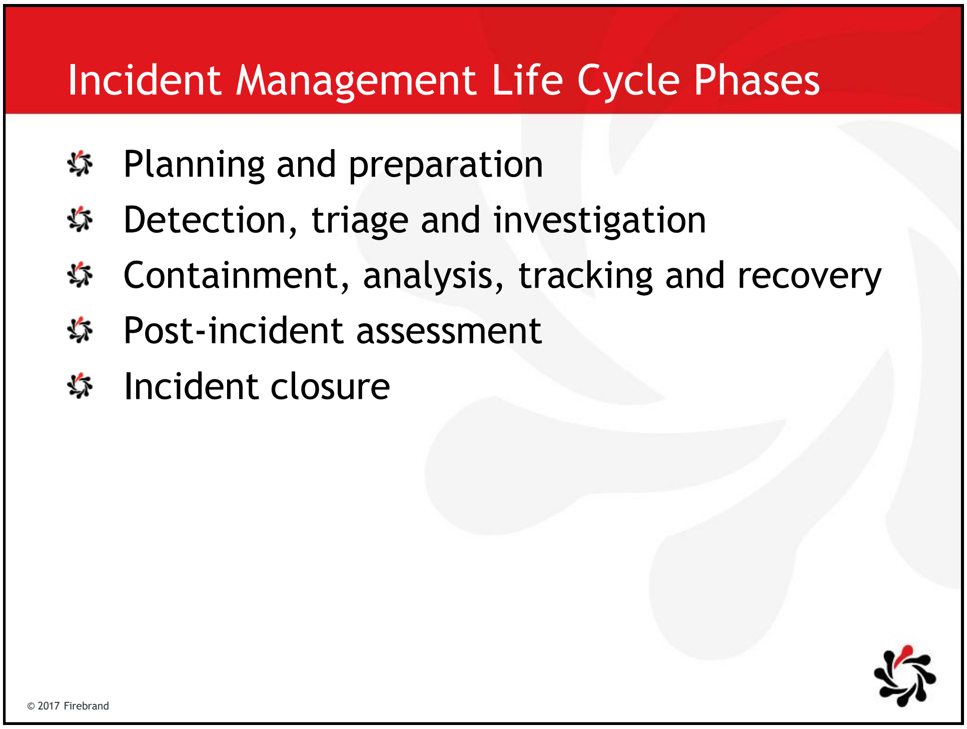
## Priorities for Incident Response

- Based on:
  - Risk Management
  - Business Impact Analysis (BIA)



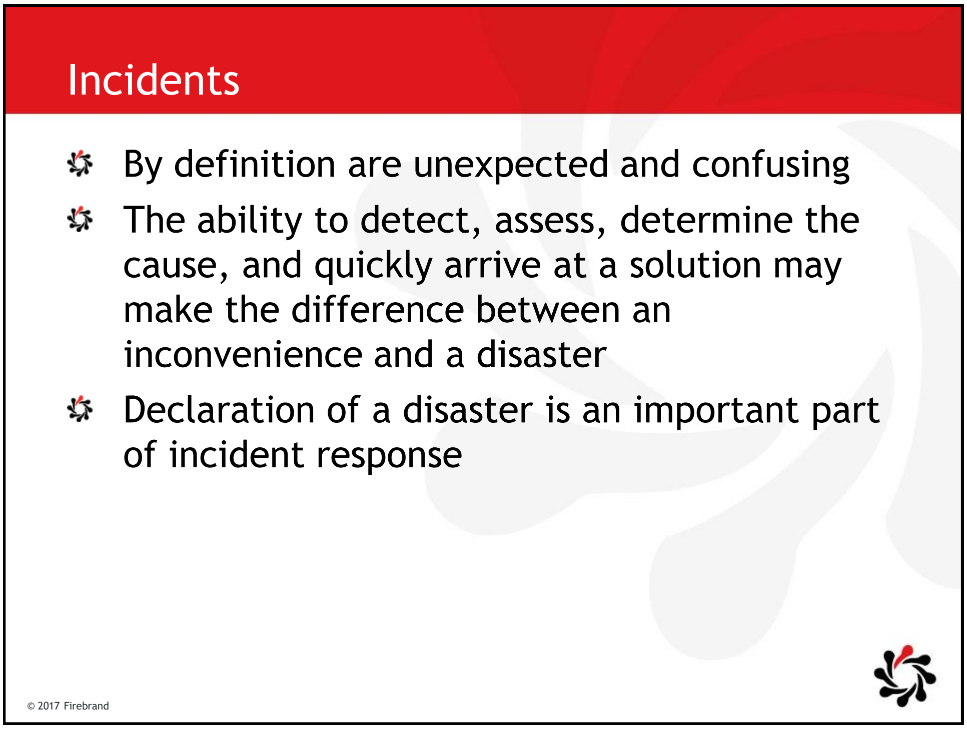
## IRP BCP DRP

- Incident response, business continuity and disaster recovery are interrelated complementary disciplines – but they are not the same
- Incident response is the first responder to an event and should try to prevent the incident from becoming a problem, and a problem from becoming a disaster



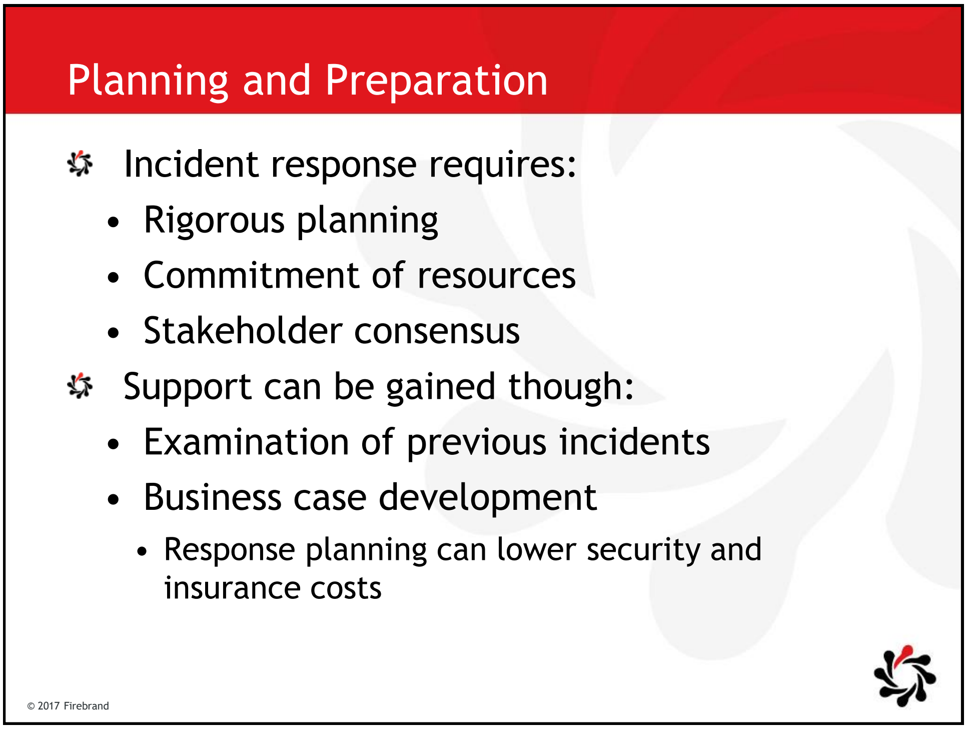
## Incident Management Life Cycle Phases

- Planning and preparation
- Detection, triage and investigation
- Containment, analysis, tracking and recovery
- Post-incident assessment
- Incident closure



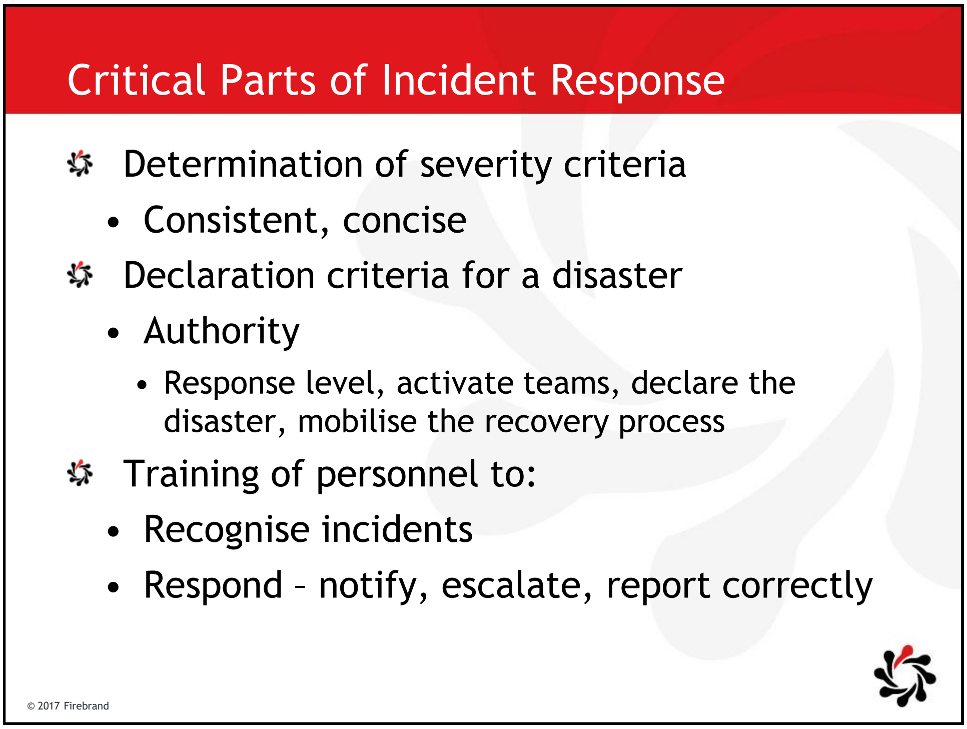
## Incidents

- By definition are unexpected and confusing
- The ability to detect, assess, determine the cause, and quickly arrive at a solution may make the difference between an inconvenience and a disaster
- Declaration of a disaster is an important part of incident response



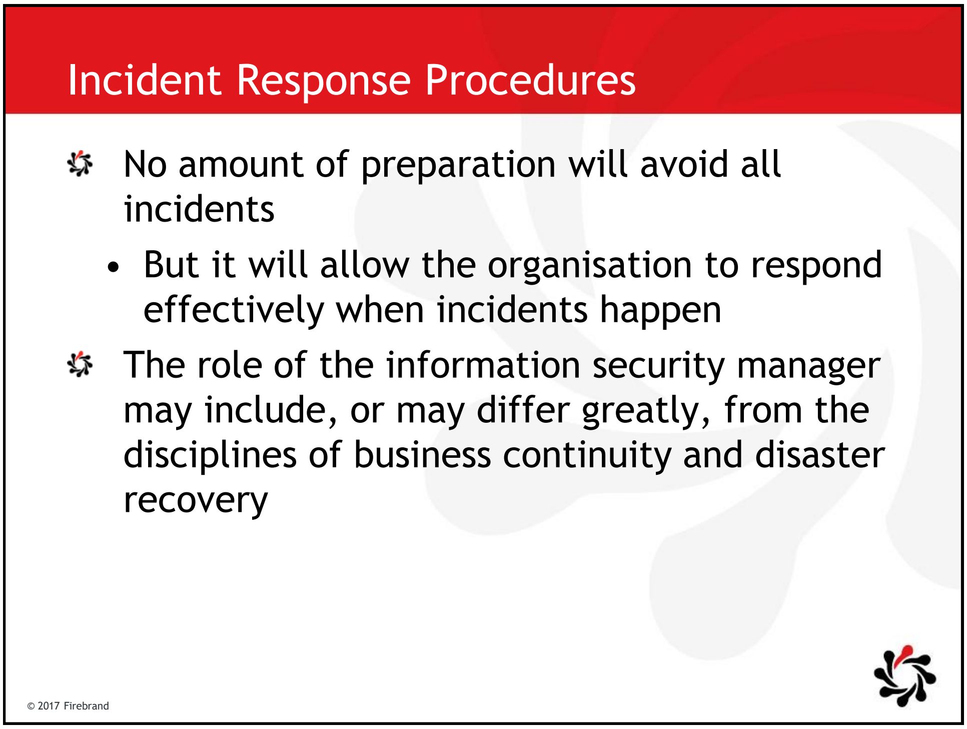
## Planning and Preparation

- Incident response requires:
  - Rigorous planning
  - Commitment of resources
  - Stakeholder consensus
- Support can be gained though:
  - Examination of previous incidents
  - Business case development
    - Response planning can lower security and insurance costs



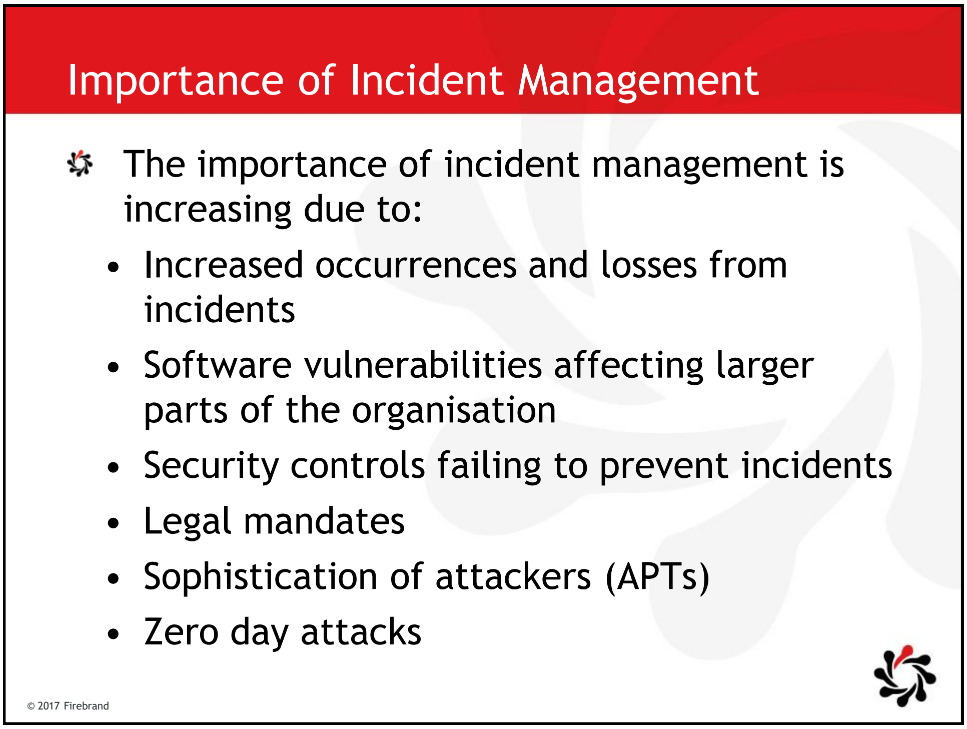
## Critical Parts of Incident Response

- Determination of severity criteria
  - Consistent, concise
- Declaration criteria for a disaster
  - Authority
    - Response level, activate teams, declare the disaster, mobilise the recovery process
- Training of personnel to:
  - Recognise incidents
  - Respond – notify, escalate, report correctly



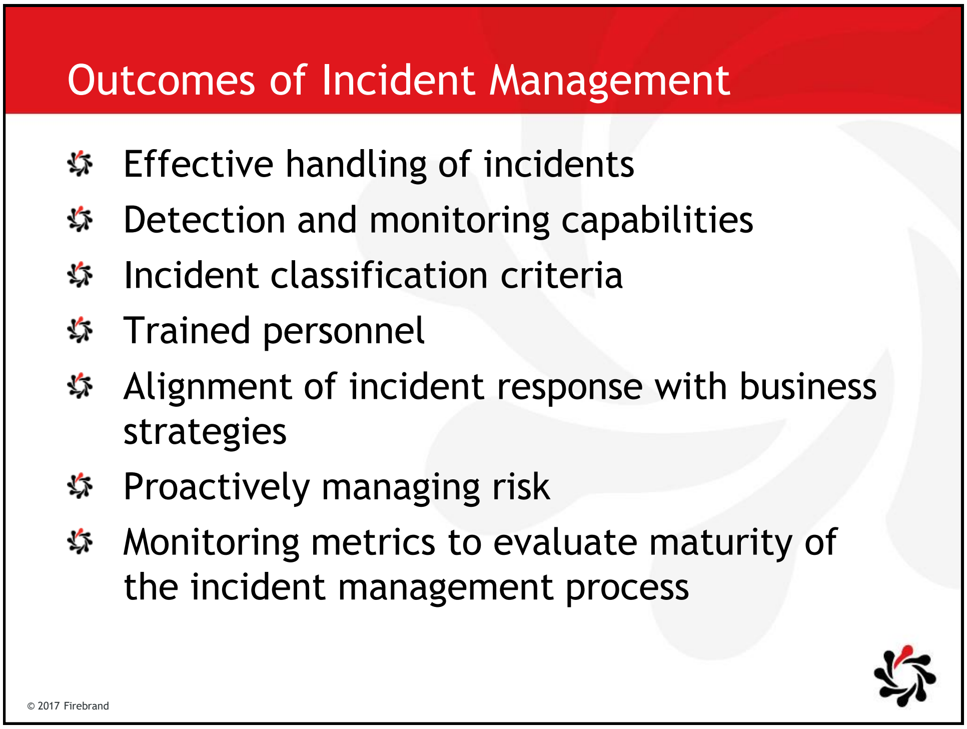
## Incident Response Procedures

- No amount of preparation will avoid all incidents
  - But it will allow the organisation to respond effectively when incidents happen
- The role of the information security manager may include, or may differ greatly, from the disciplines of business continuity and disaster recovery



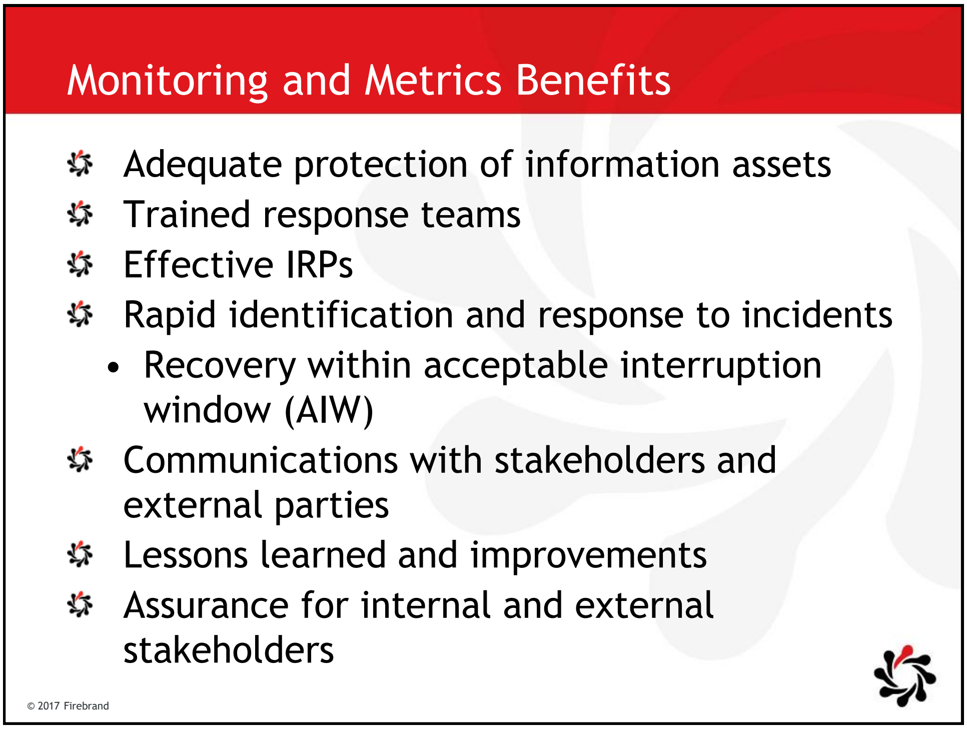
## Importance of Incident Management

- The importance of incident management is increasing due to:
  - Increased occurrences and losses from incidents
  - Software vulnerabilities affecting larger parts of the organisation
  - Security controls failing to prevent incidents
  - Legal mandates
  - Sophistication of attackers (APTs)
  - Zero day attacks



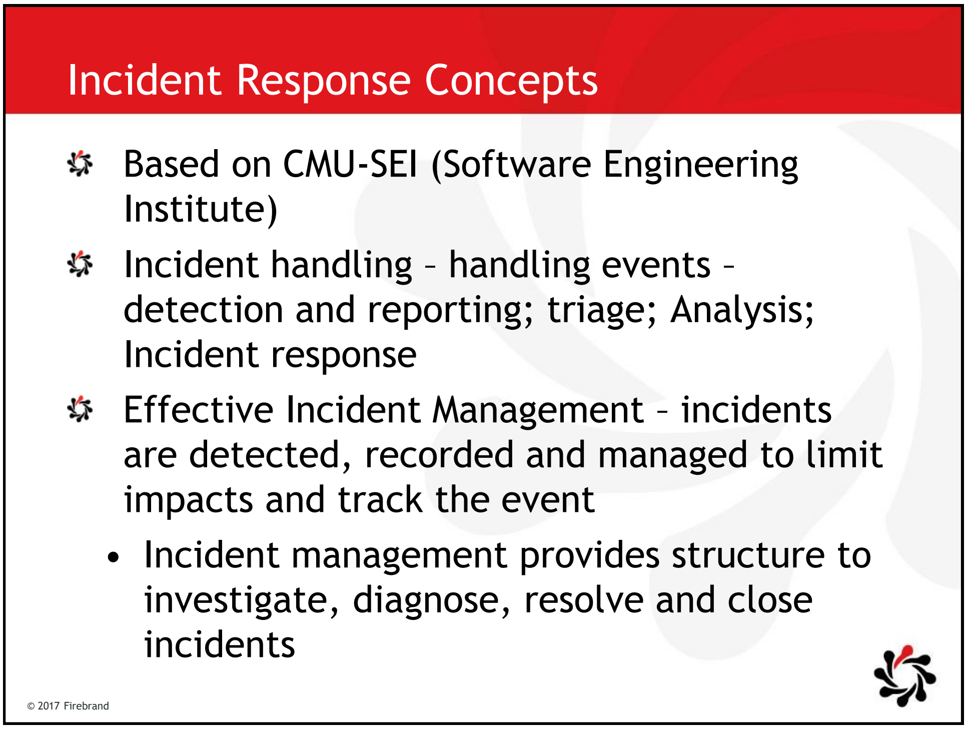
## Outcomes of Incident Management

- Effective handling of incidents
- Detection and monitoring capabilities
- Incident classification criteria
- Trained personnel
- Alignment of incident response with business strategies
- Proactively managing risk
- Monitoring metrics to evaluate maturity of the incident management process



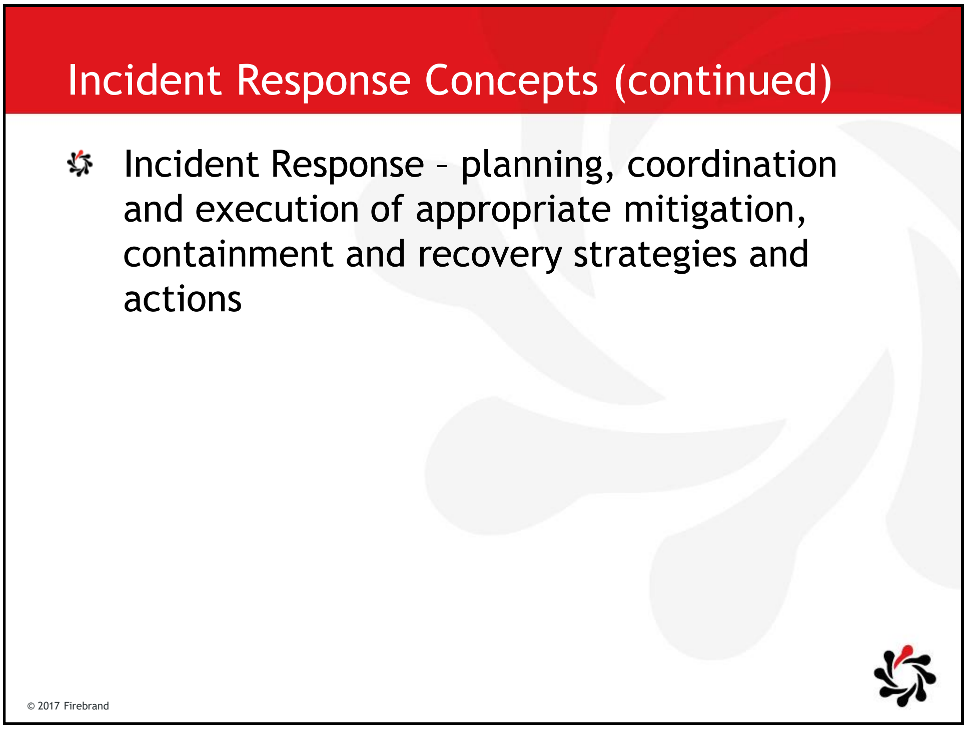
## Monitoring and Metrics Benefits

- Adequate protection of information assets
- Trained response teams
- Effective IRPs
- Rapid identification and response to incidents
  - Recovery within acceptable interruption window (AIW)
- Communications with stakeholders and external parties
- Lessons learned and improvements
- Assurance for internal and external stakeholders



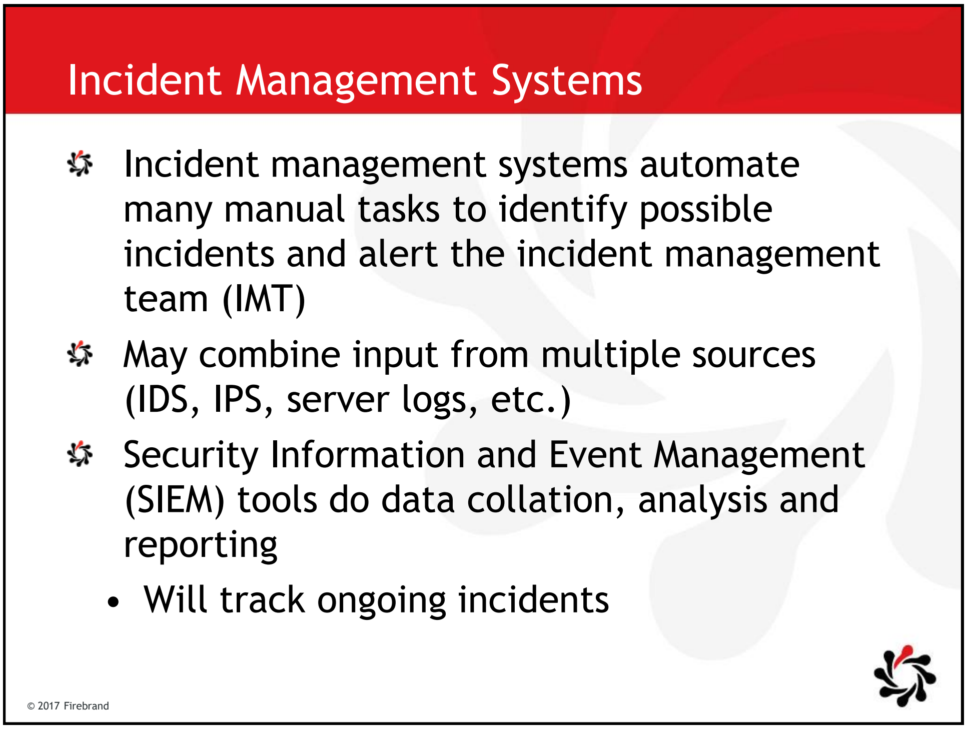
## Incident Response Concepts

- Based on CMU-SEI (Software Engineering Institute)
- Incident handling – handling events – detection and reporting; triage; Analysis; Incident response
- Effective Incident Management – incidents are detected, recorded and managed to limit impacts and track the event
  - Incident management provides structure to investigate, diagnose, resolve and close incidents



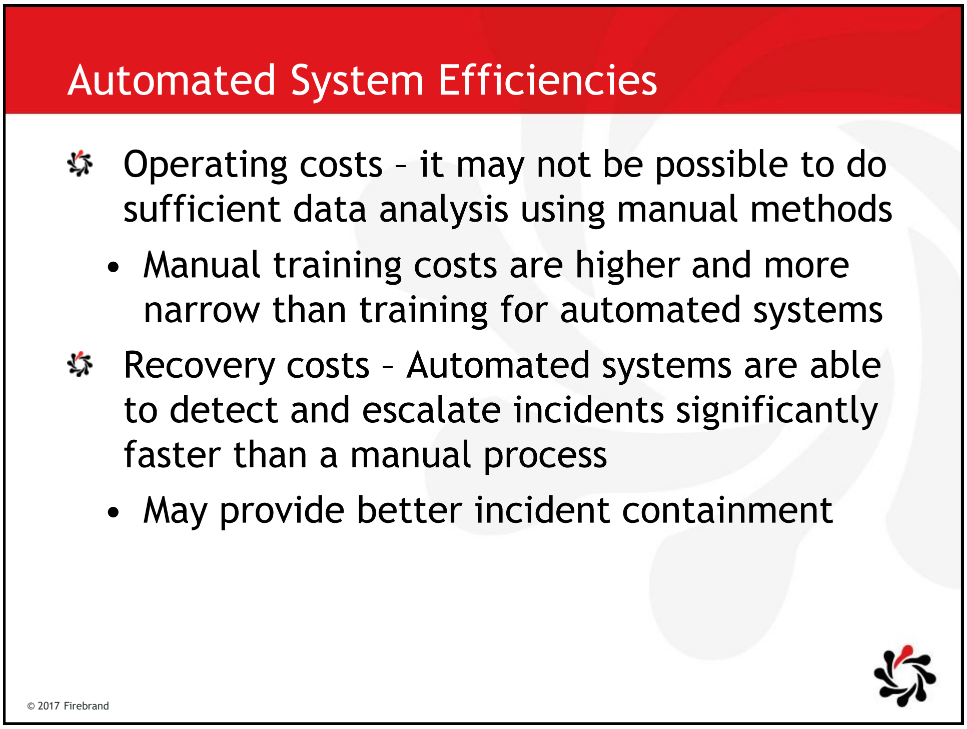
## Incident Response Concepts (continued)

- Incident Response – planning, coordination and execution of appropriate mitigation, containment and recovery strategies and actions



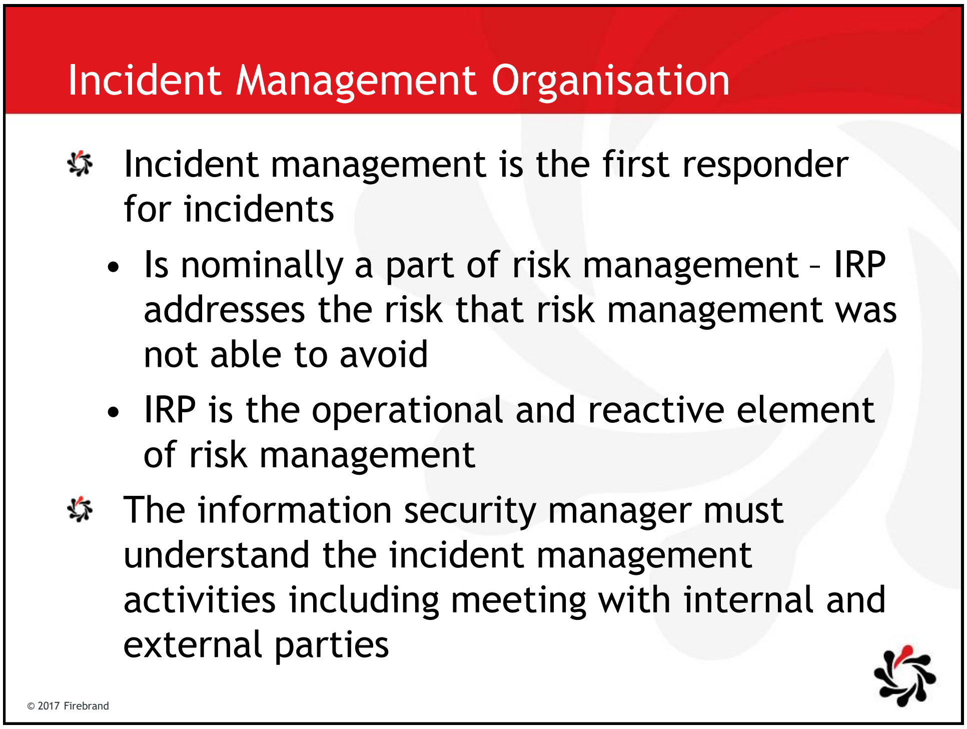
## Incident Management Systems

- Incident management systems automate many manual tasks to identify possible incidents and alert the incident management team (IMT)
- May combine input from multiple sources (IDS, IPS, server logs, etc.)
- Security Information and Event Management (SIEM) tools do data collation, analysis and reporting
  - Will track ongoing incidents



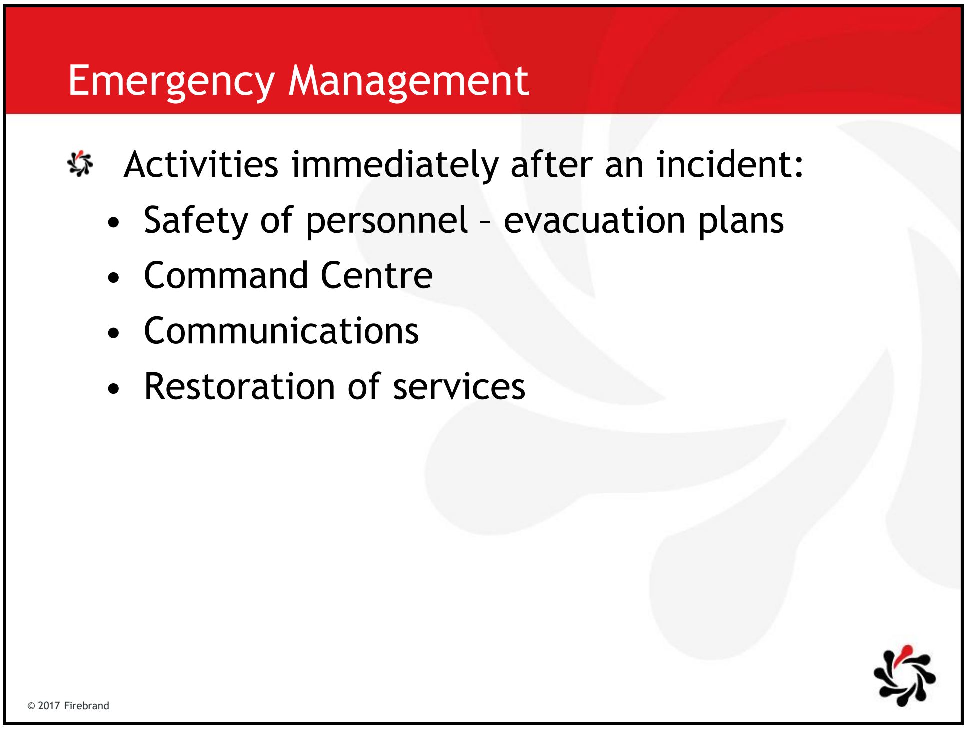
## Automated System Efficiencies

- Operating costs – it may not be possible to do sufficient data analysis using manual methods
  - Manual training costs are higher and more narrow than training for automated systems
- Recovery costs – Automated systems are able to detect and escalate incidents significantly faster than a manual process
  - May provide better incident containment



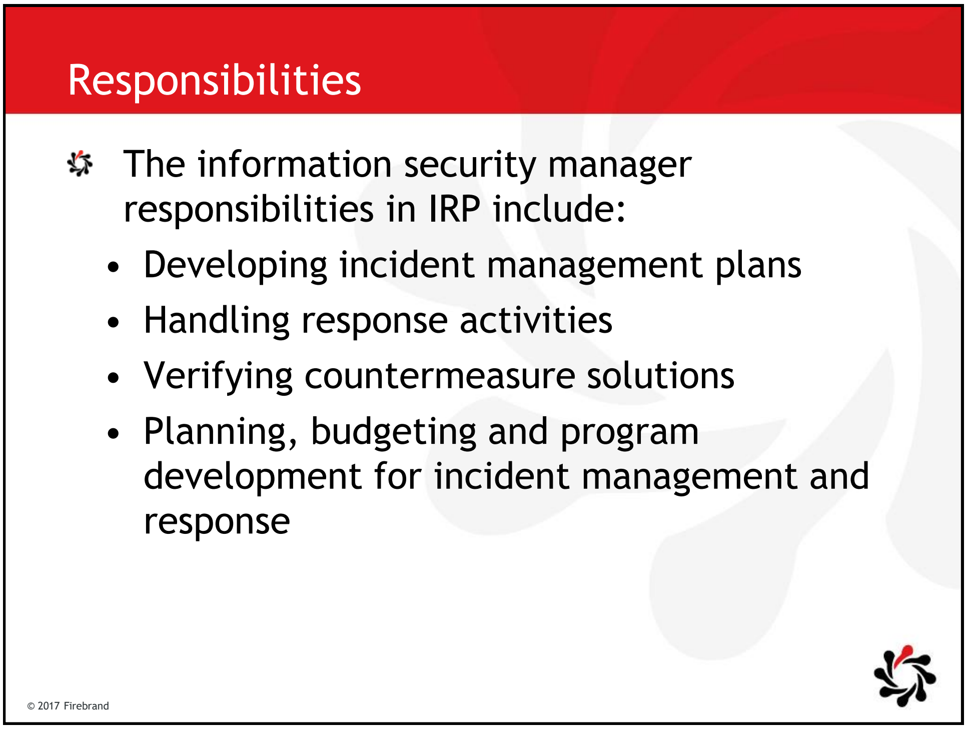
## Incident Management Organisation

- Incident management is the first responder for incidents
  - Is nominally a part of risk management – IRP addresses the risk that risk management was not able to avoid
  - IRP is the operational and reactive element of risk management
- The information security manager must understand the incident management activities including meeting with internal and external parties



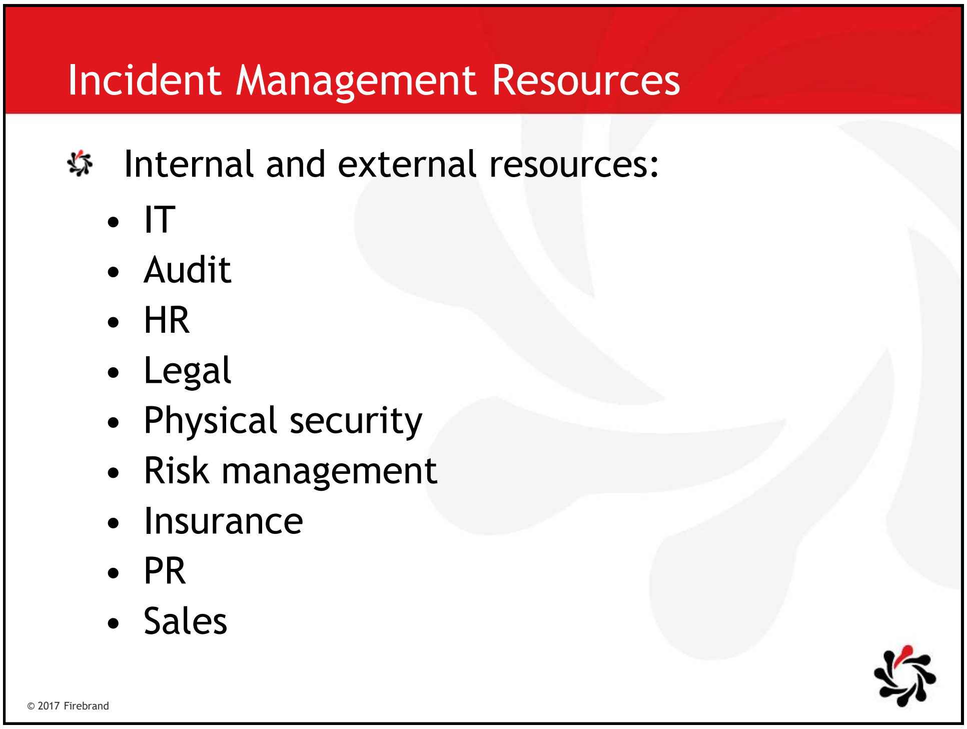
## Emergency Management

- Activities immediately after an incident:
  - Safety of personnel – evacuation plans
  - Command Centre
  - Communications
  - Restoration of services



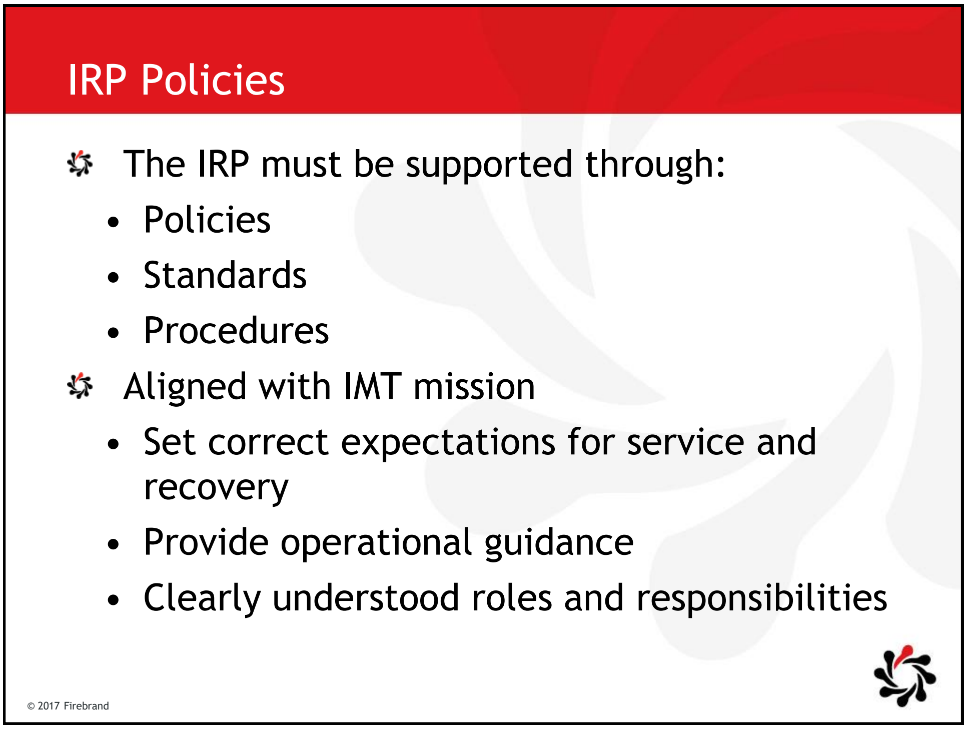
## Responsibilities

- The information security manager responsibilities in IRP include:
  - Developing incident management plans
  - Handling response activities
  - Verifying countermeasure solutions
  - Planning, budgeting and program development for incident management and response



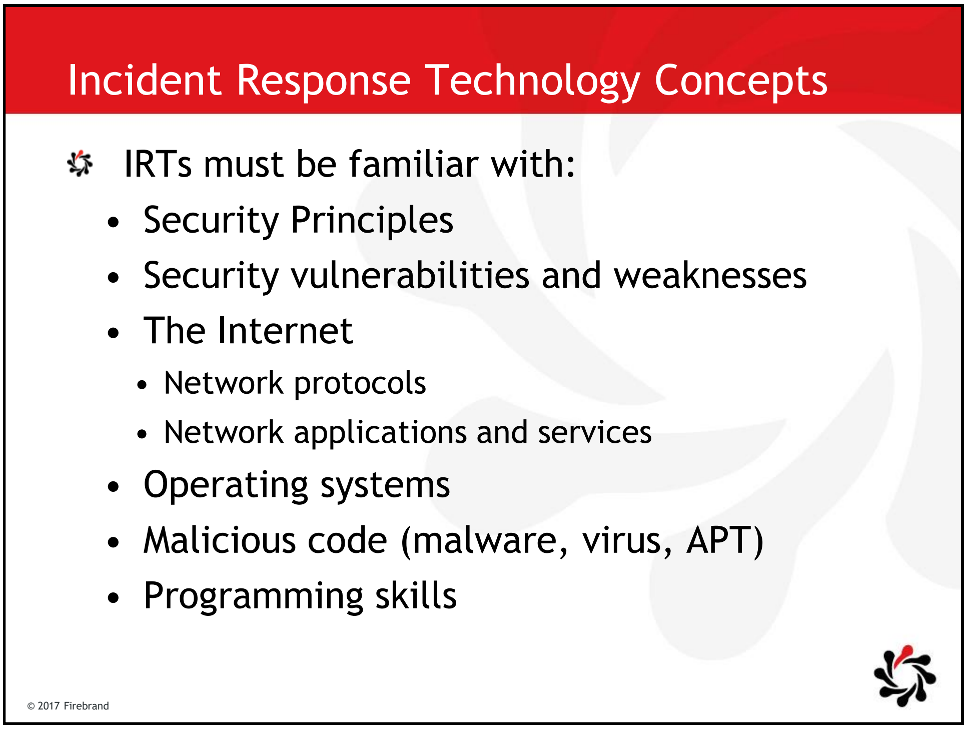
## Incident Management Resources

- Internal and external resources:
  - IT
  - Audit
  - HR
  - Legal
  - Physical security
  - Risk management
  - Insurance
  - PR
  - Sales



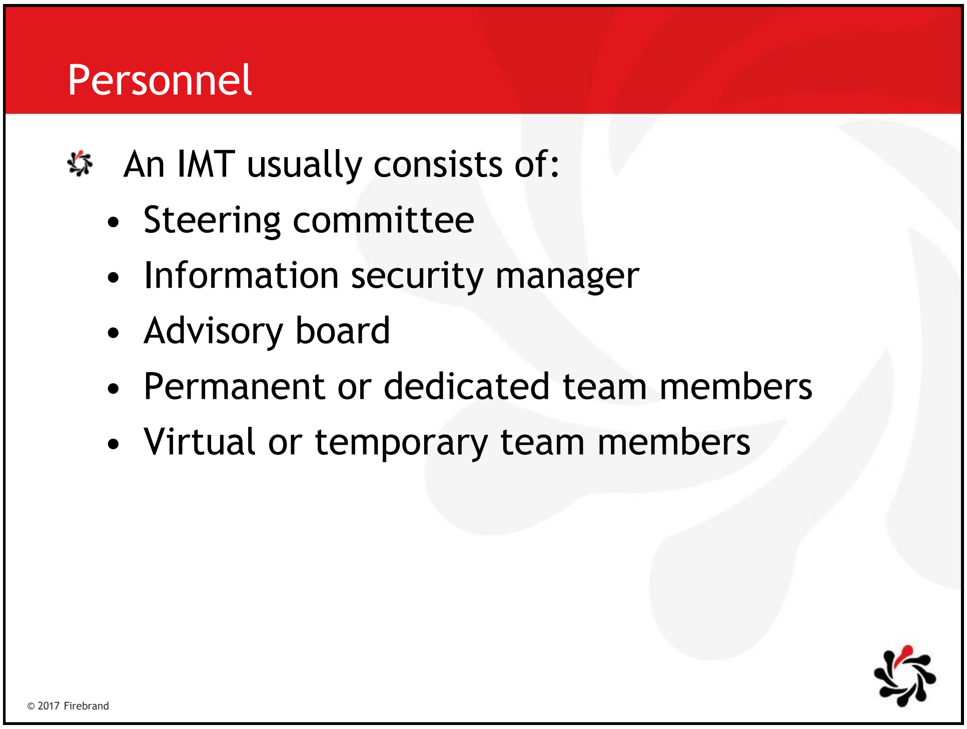
## IRP Policies

- The IRP must be supported through:
  - Policies
  - Standards
  - Procedures
- Aligned with IMT mission
  - Set correct expectations for service and recovery
  - Provide operational guidance
  - Clearly understood roles and responsibilities



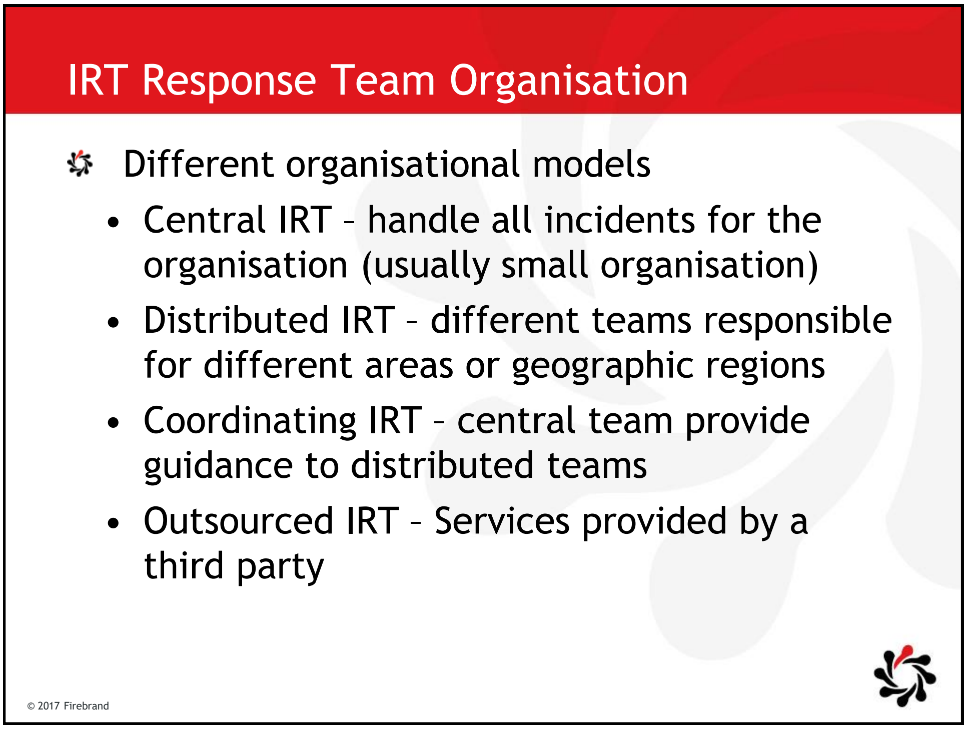
## Incident Response Technology Concepts

- IRTs must be familiar with:
  - Security Principles
  - Security vulnerabilities and weaknesses
  - The Internet
    - Network protocols
    - Network applications and services
  - Operating systems
  - Malicious code (malware, virus, APT)
  - Programming skills



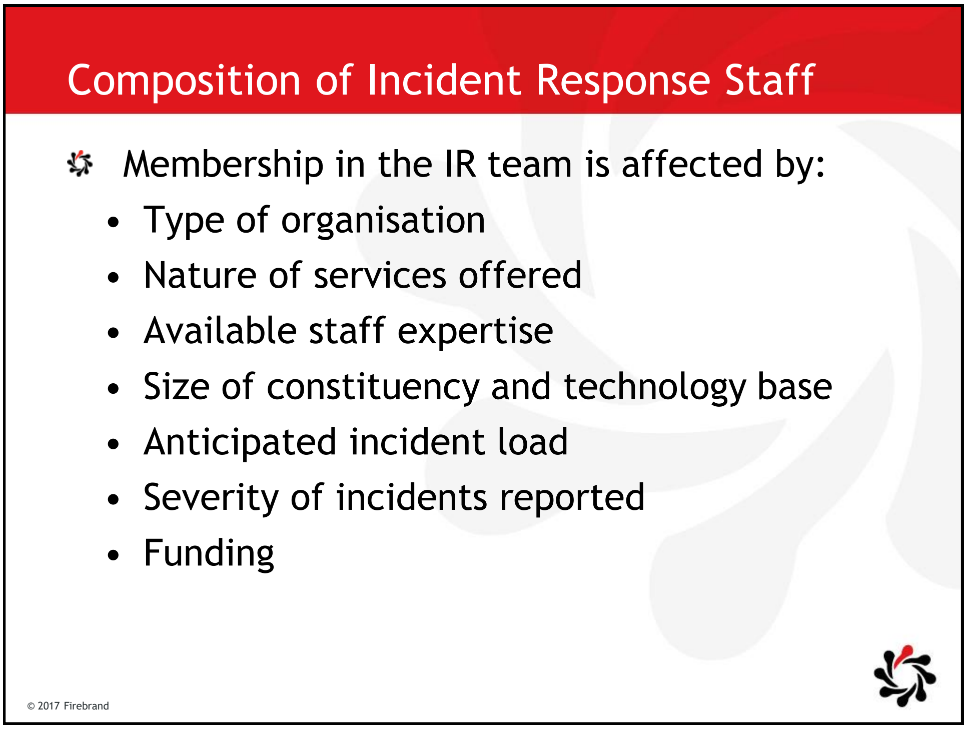
## Personnel

- An IMT usually consists of:
  - Steering committee
  - Information security manager
  - Advisory board
  - Permanent or dedicated team members
  - Virtual or temporary team members



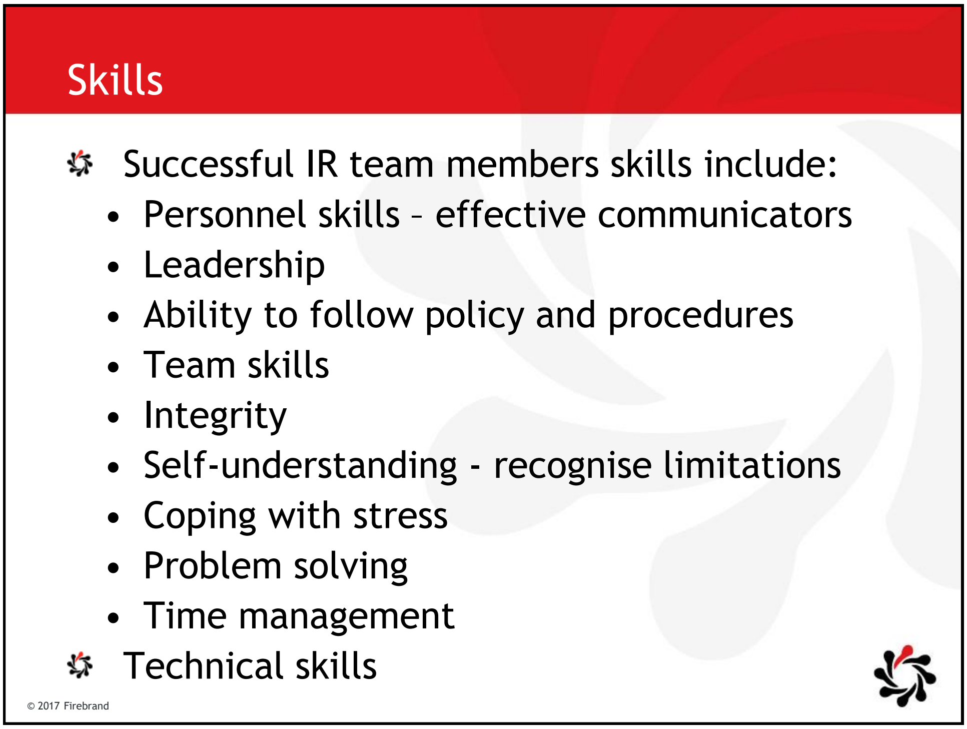
## IRT Response Team Organisation

- Different organisational models
  - Central IRT – handle all incidents for the organisation (usually small organisation)
  - Distributed IRT – different teams responsible for different areas or geographic regions
  - Coordinating IRT – central team provide guidance to distributed teams
  - Outsourced IRT – Services provided by a third party



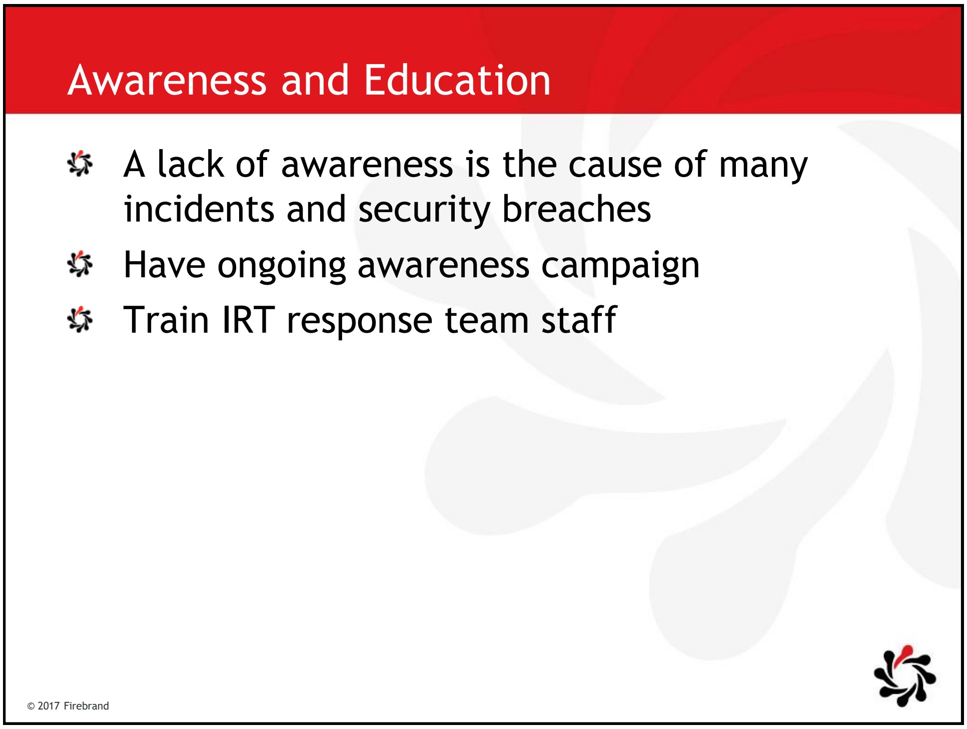
## Composition of Incident Response Staff

- Membership in the IR team is affected by:
  - Type of organisation
  - Nature of services offered
  - Available staff expertise
  - Size of constituency and technology base
  - Anticipated incident load
  - Severity of incidents reported
  - Funding



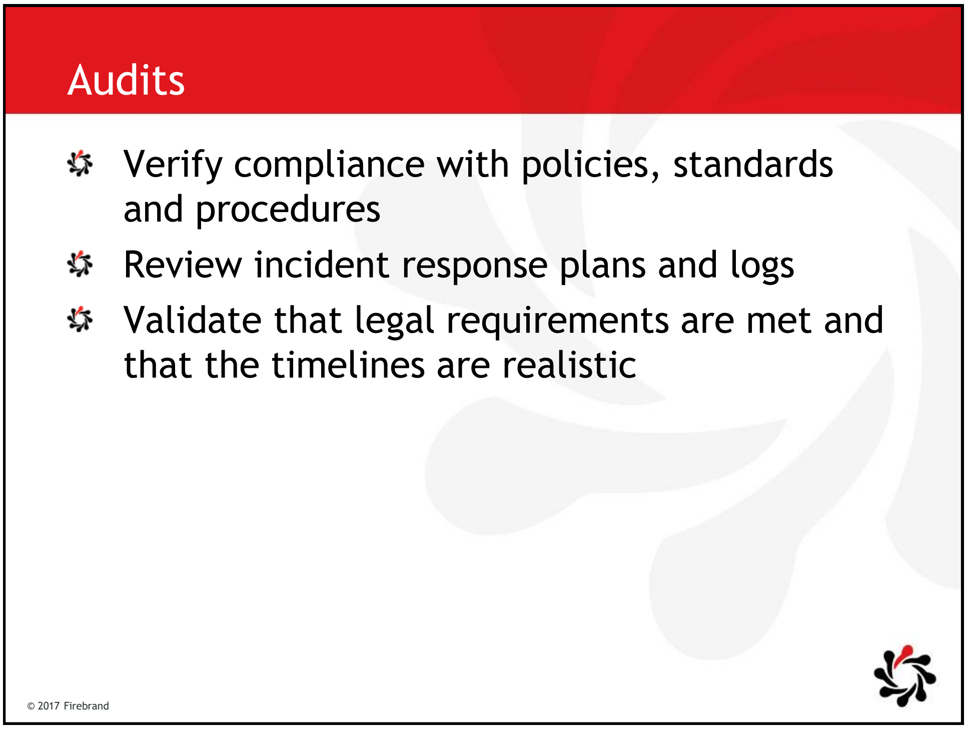
## Skills

- Successful IR team members skills include:
  - Personnel skills – effective communicators
  - Leadership
  - Ability to follow policy and procedures
  - Team skills
  - Integrity
  - Self-understanding - recognise limitations
  - Coping with stress
  - Problem solving
  - Time management
- Technical skills



## Awareness and Education

- A lack of awareness is the cause of many incidents and security breaches
- Have ongoing awareness campaign
- Train IRT response team staff

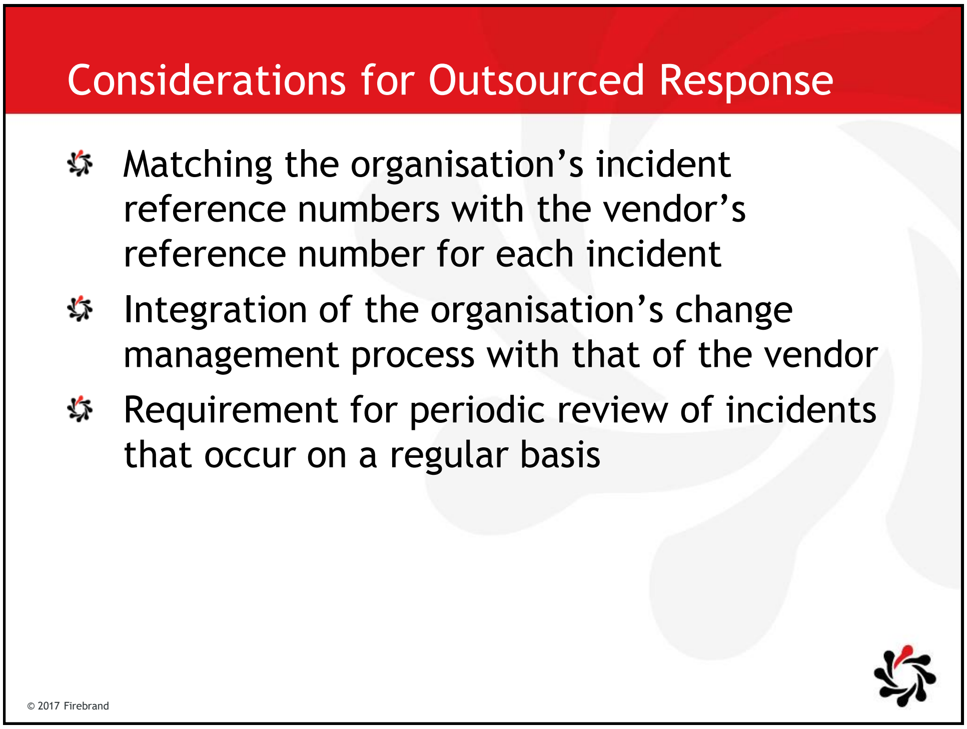


## Audits

- Verify compliance with policies, standards and procedures
- Review incident response plans and logs
- Validate that legal requirements are met and that the timelines are realistic

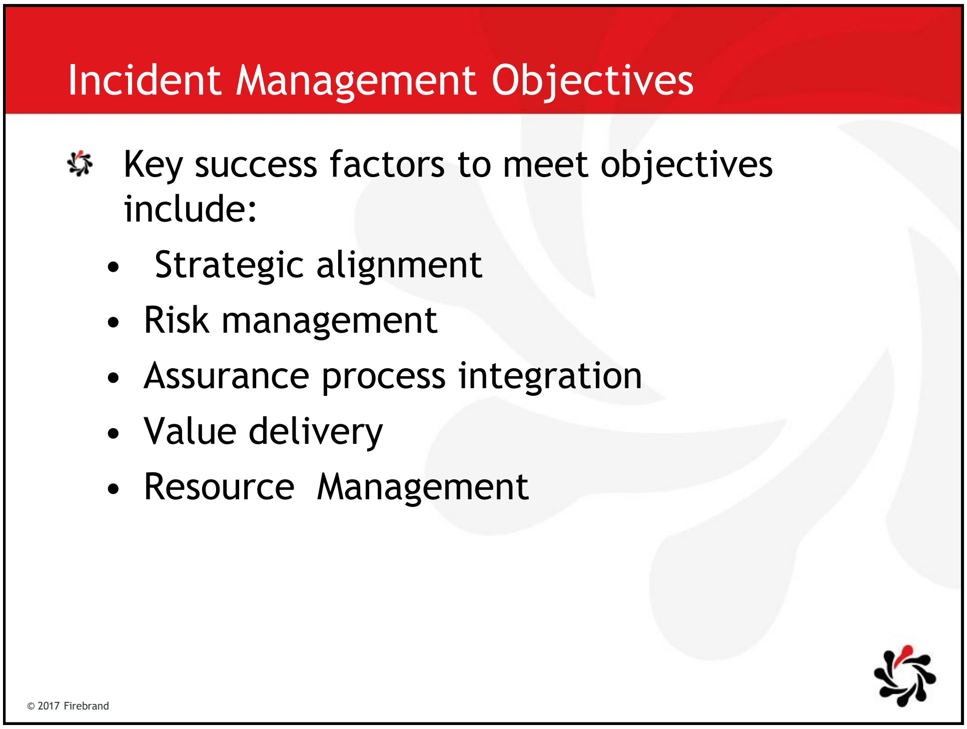
## Outsourced Security Providers

- Outsourcing incident management may be a cost-effective solution for smaller organisations
- Could use the same provider as outsourced IT operations or security operations



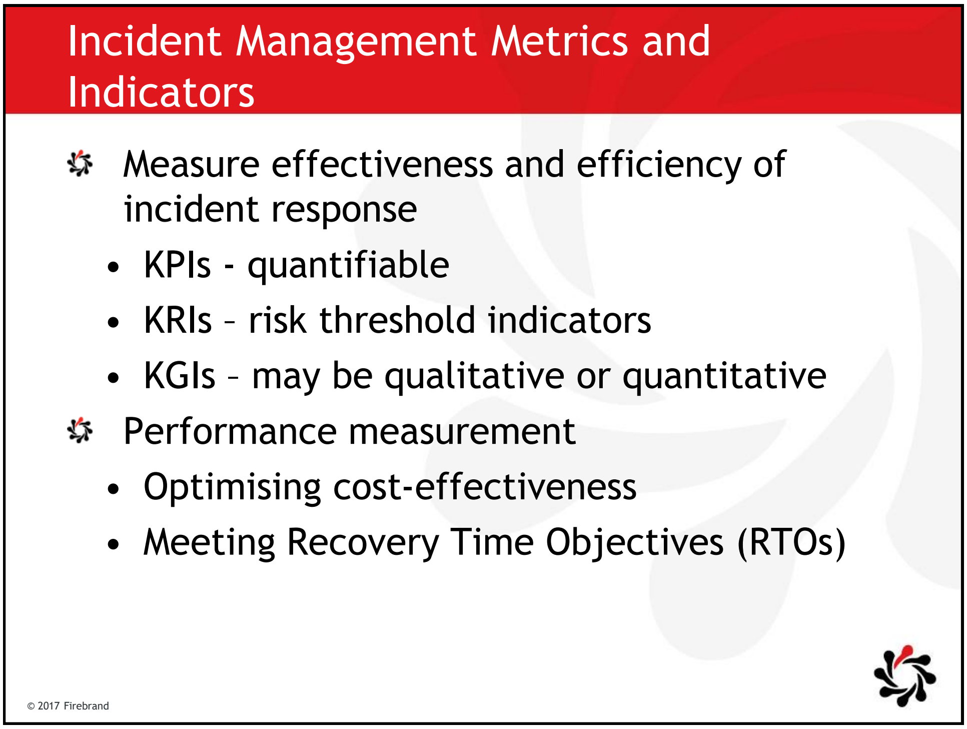
## Considerations for Outsourced Response

- Matching the organisation’s incident reference numbers with the vendor’s reference number for each incident
- Integration of the organisation’s change management process with that of the vendor
- Requirement for periodic review of incidents that occur on a regular basis



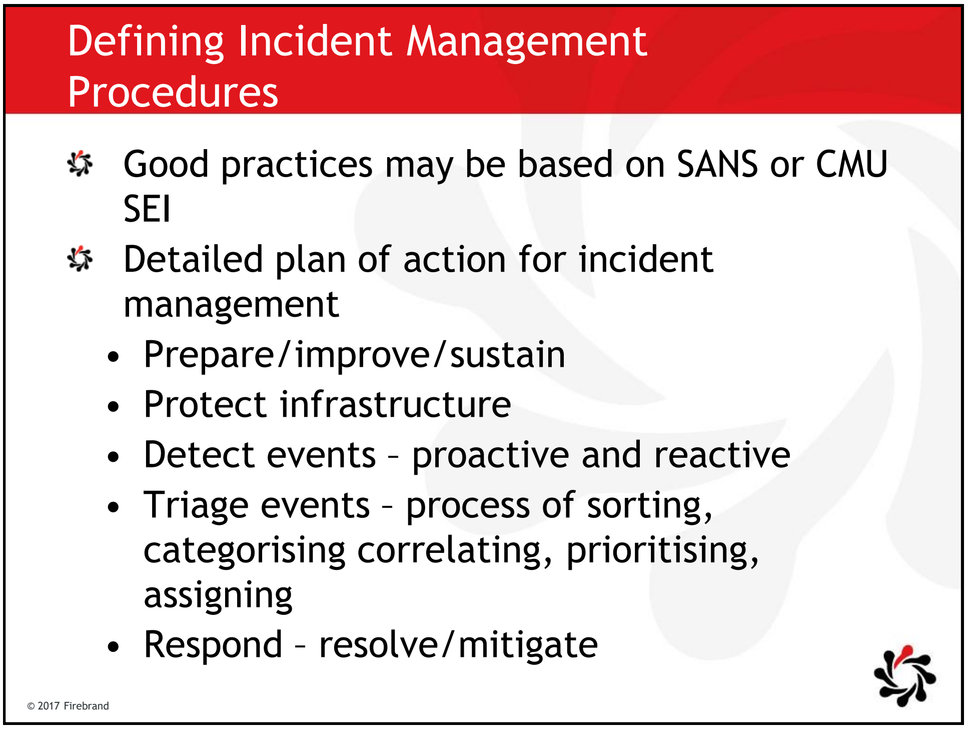
## Incident Management Objectives

- Key success factors to meet objectives include:
  - Strategic alignment
  - Risk management
  - Assurance process integration
  - Value delivery
  - Resource Management



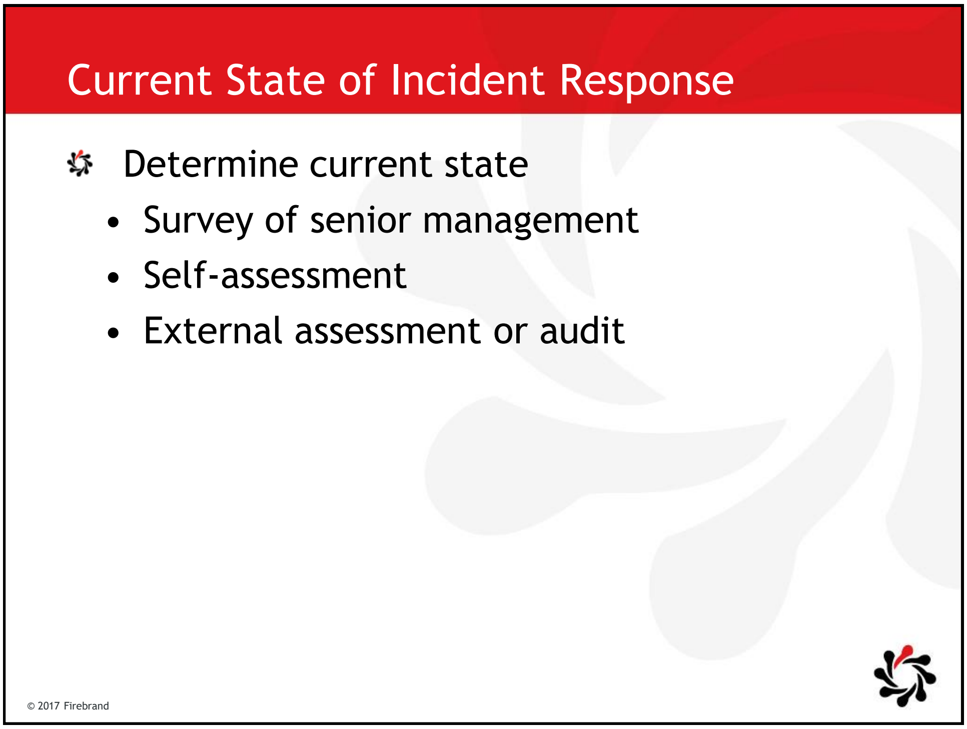
## Incident Management Metrics and Indicators

- Measure effectiveness and efficiency of incident response
  - KPIs - quantifiable
  - KRIs – risk threshold indicators
  - KGIs – may be qualitative or quantitative
- Performance measurement
  - Optimising cost-effectiveness
  - Meeting Recovery Time Objectives (RTOs)



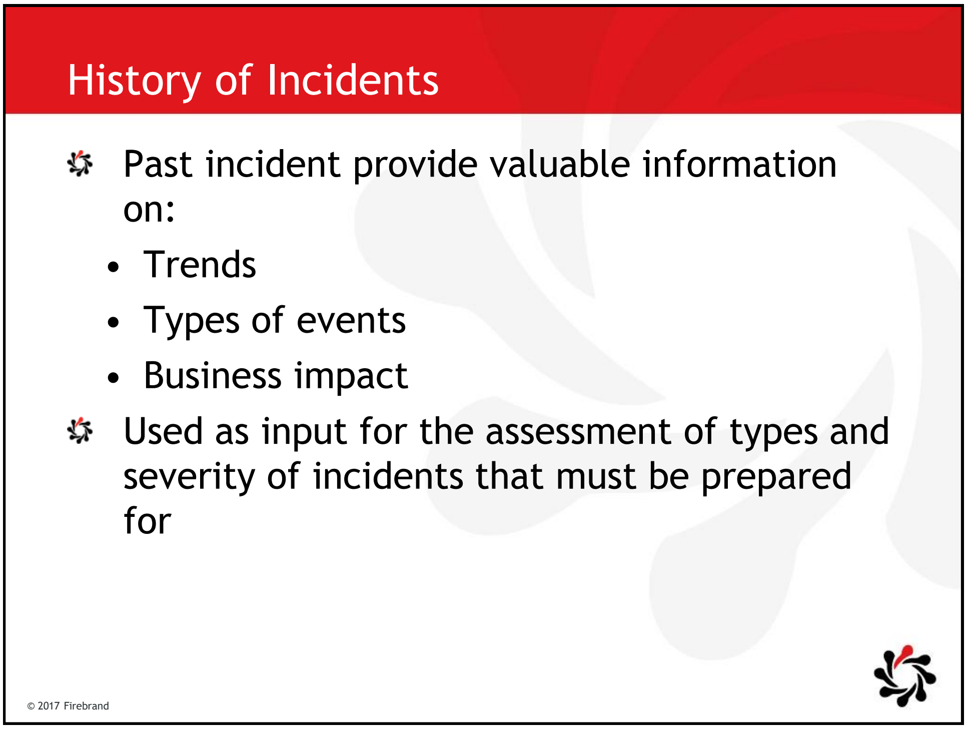
## Defining Incident Management Procedures

- Good practices may be based on SANS or CMU SEI
- Detailed plan of action for incident management
  - Prepare/improve/sustain
  - Protect infrastructure
  - Detect events – proactive and reactive
  - Triage events – process of sorting, categorising correlating, prioritising, assigning
  - Respond – resolve/mitigate



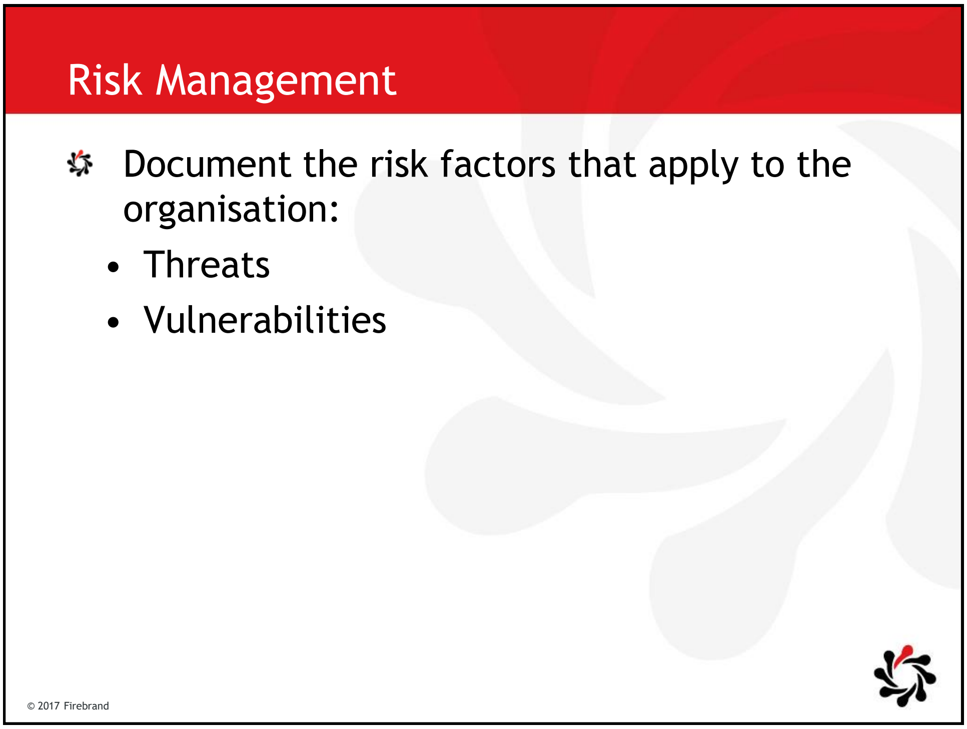
## Current State of Incident Response

- Determine current state
  - Survey of senior management
  - Self-assessment
  - External assessment or audit



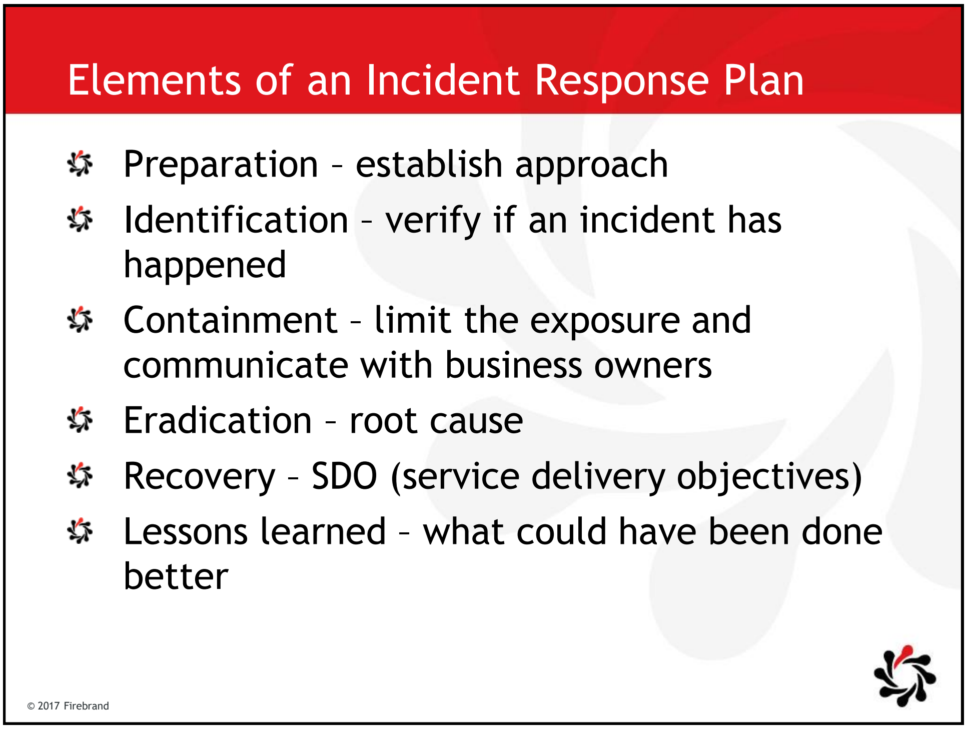
## History of Incidents

- Past incident provide valuable information on:
  - Trends
  - Types of events
  - Business impact
- Used as input for the assessment of types and severity of incidents that must be prepared for



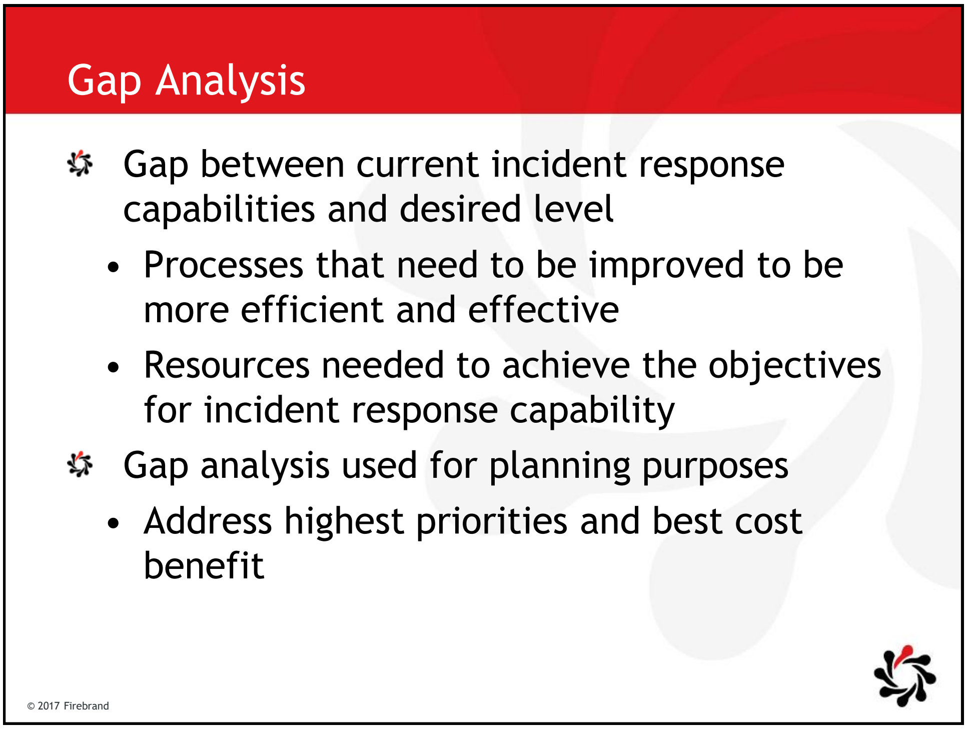
## Risk Management

- Document the risk factors that apply to the organisation:
  - Threats
  - Vulnerabilities



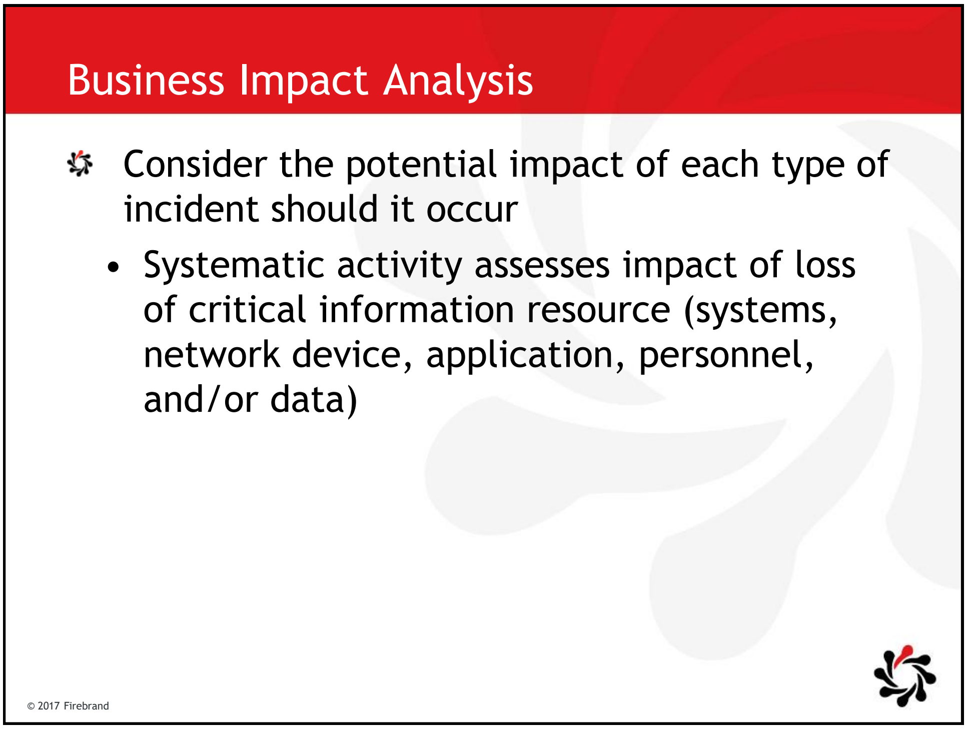
## Elements of an Incident Response Plan

- Preparation – establish approach
- Identification – verify if an incident has happened
- Containment – limit the exposure and communicate with business owners
- Eradication – root cause
- Recovery – SDO (service delivery objectives)
- Lessons learned – what could have been done better



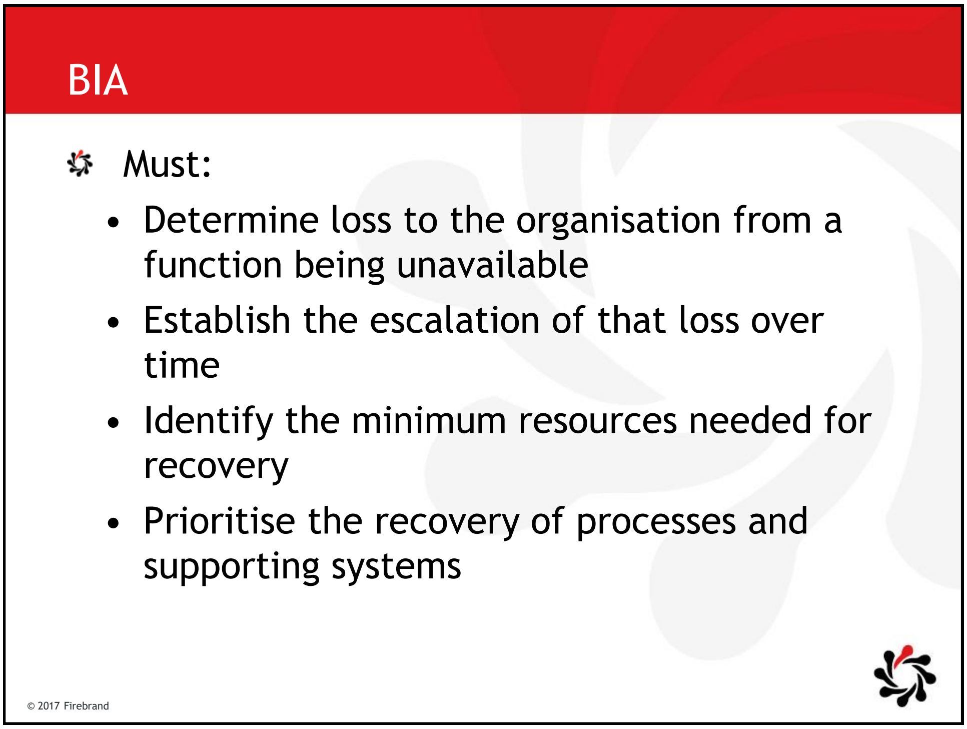
## Gap Analysis

- Gap between current incident response capabilities and desired level
  - Processes that need to be improved to be more efficient and effective
  - Resources needed to achieve the objectives for incident response capability
- Gap analysis used for planning purposes
  - Address highest priorities and best cost benefit



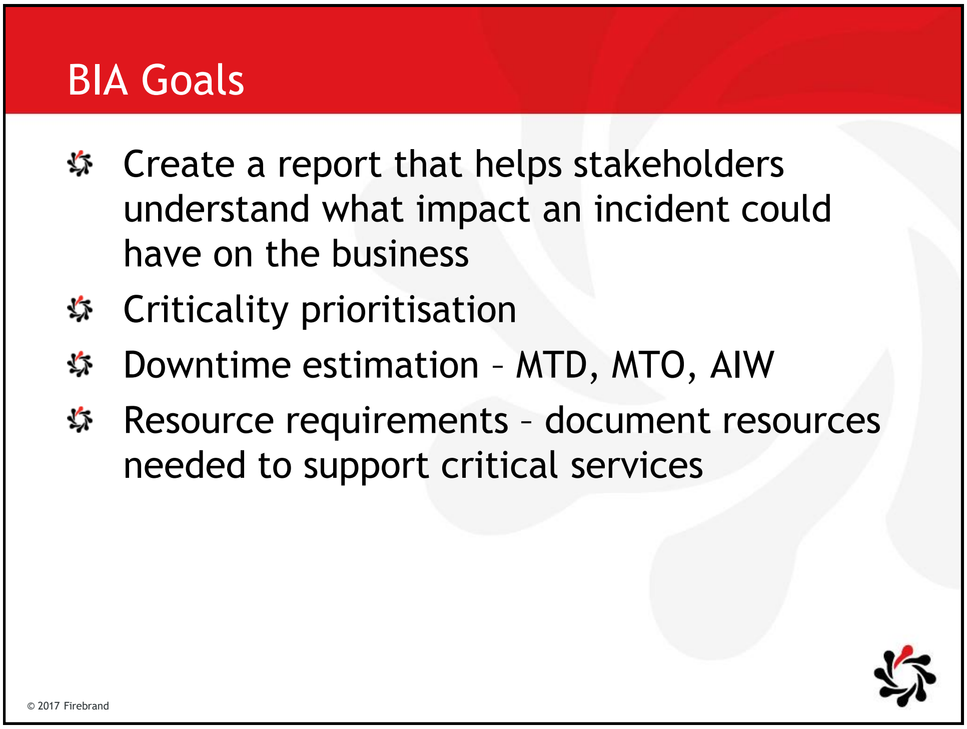
## Business Impact Analysis

- Consider the potential impact of each type of incident should it occur
  - Systematic activity assesses impact of loss of critical information resource (systems, network device, application, personnel, and/or data)



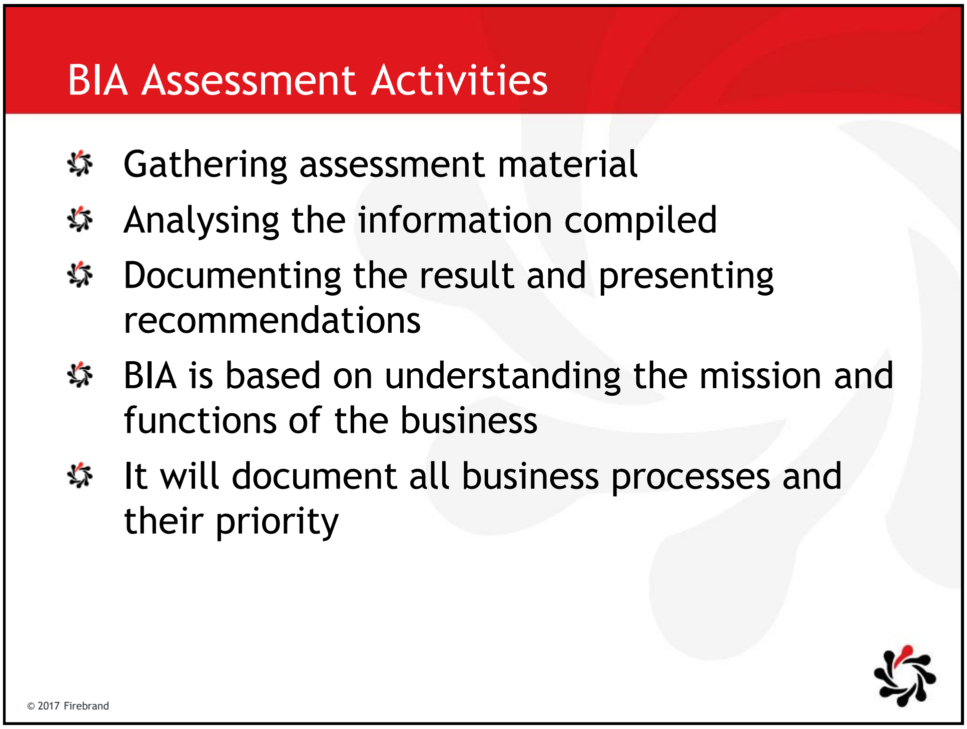
## BIA

- Must:
  - Determine loss to the organisation from a function being unavailable
  - Establish the escalation of that loss over time
  - Identify the minimum resources needed for recovery
  - Prioritise the recovery of processes and supporting systems



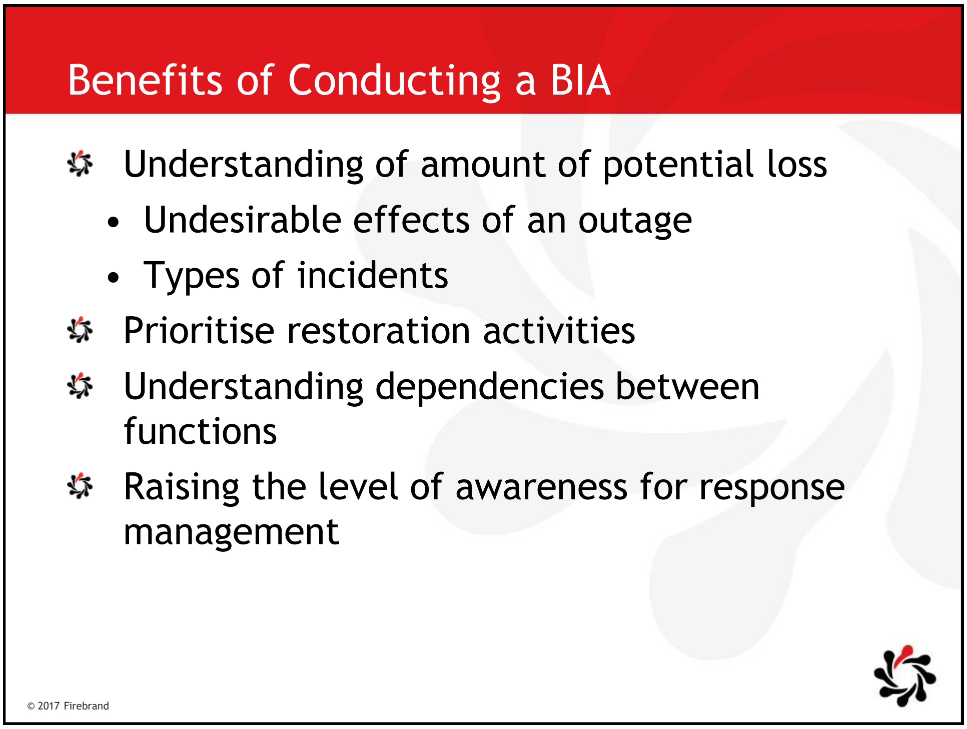
## BIA Goals

- Create a report that helps stakeholders understand what impact an incident could have on the business
- Criticality prioritisation
- Downtime estimation – MTD, MTO, AIW
- Resource requirements – document resources needed to support critical services



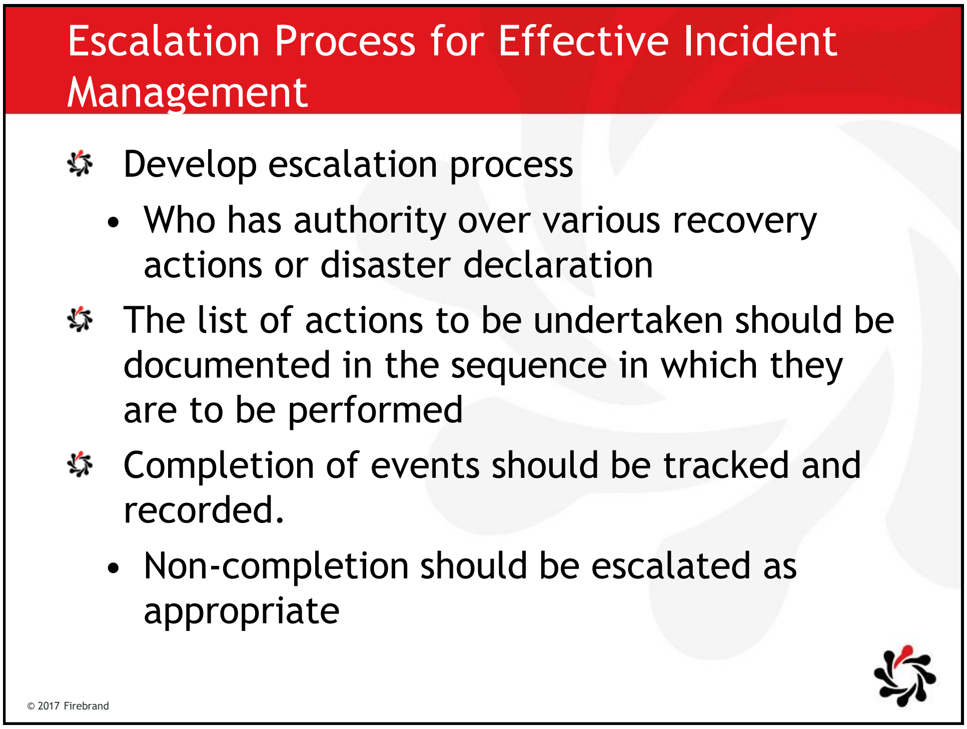
## BIA Assessment Activities

- Gathering assessment material
- Analysing the information compiled
- Documenting the result and presenting recommendations
- BIA is based on understanding the mission and functions of the business
- It will document all business processes and their priority



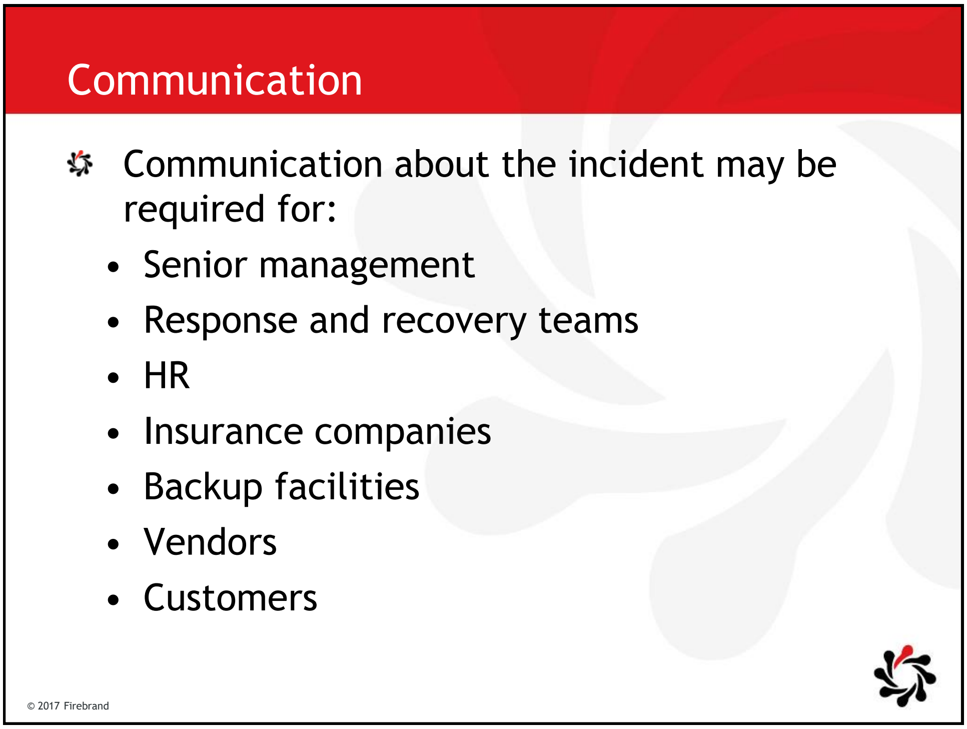
## Benefits of Conducting a BIA

- Understanding of amount of potential loss
  - Undesirable effects of an outage
  - Types of incidents
- Prioritise restoration activities
- Understanding dependencies between functions
- Raising the level of awareness for response management



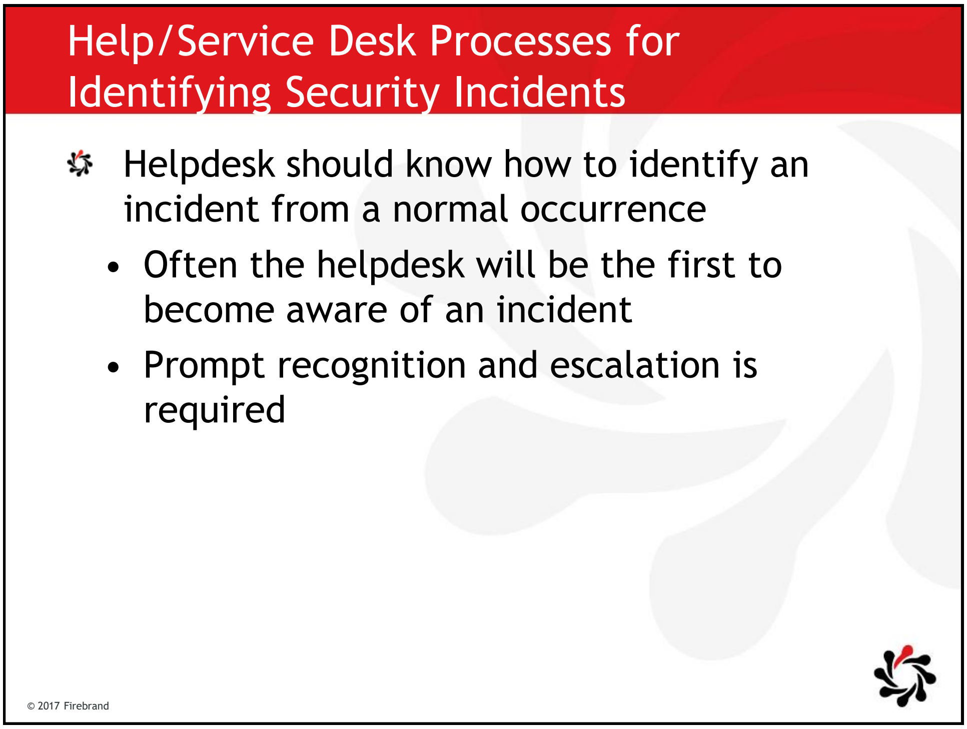
## Escalation Process for Effective Incident Management

- Develop escalation process
  - Who has authority over various recovery actions or disaster declaration
- The list of actions to be undertaken should be documented in the sequence in which they are to be performed
- Completion of events should be tracked and recorded.
  - Non-completion should be escalated as appropriate



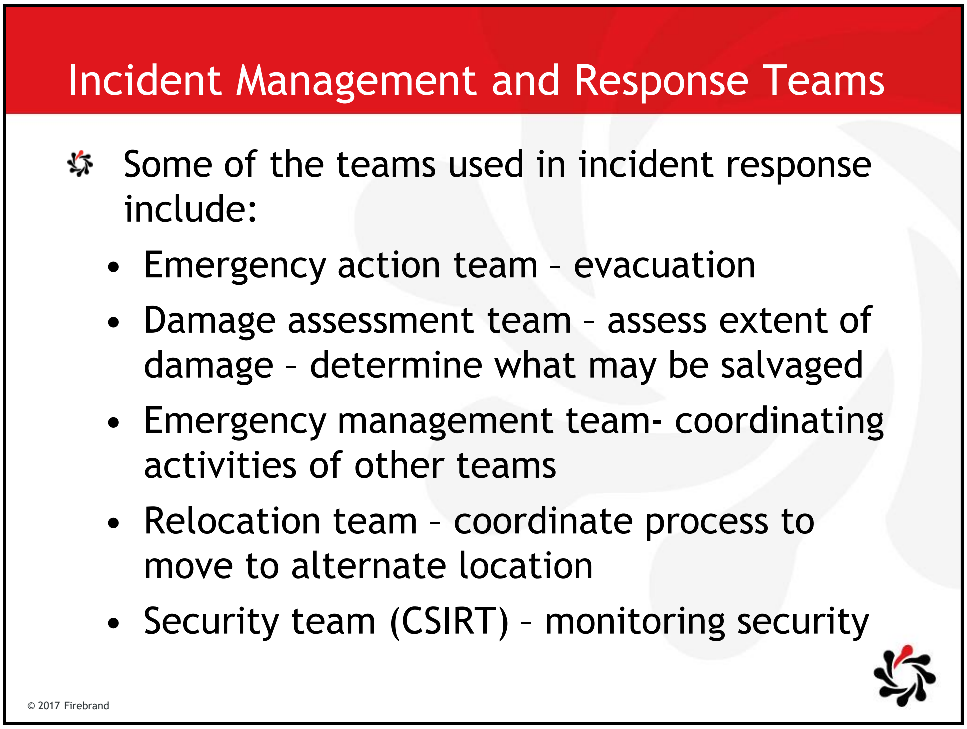
## Communication

- Communication about the incident may be required for:
  - Senior management
  - Response and recovery teams
  - HR
  - Insurance companies
  - Backup facilities
  - Vendors
  - Customers



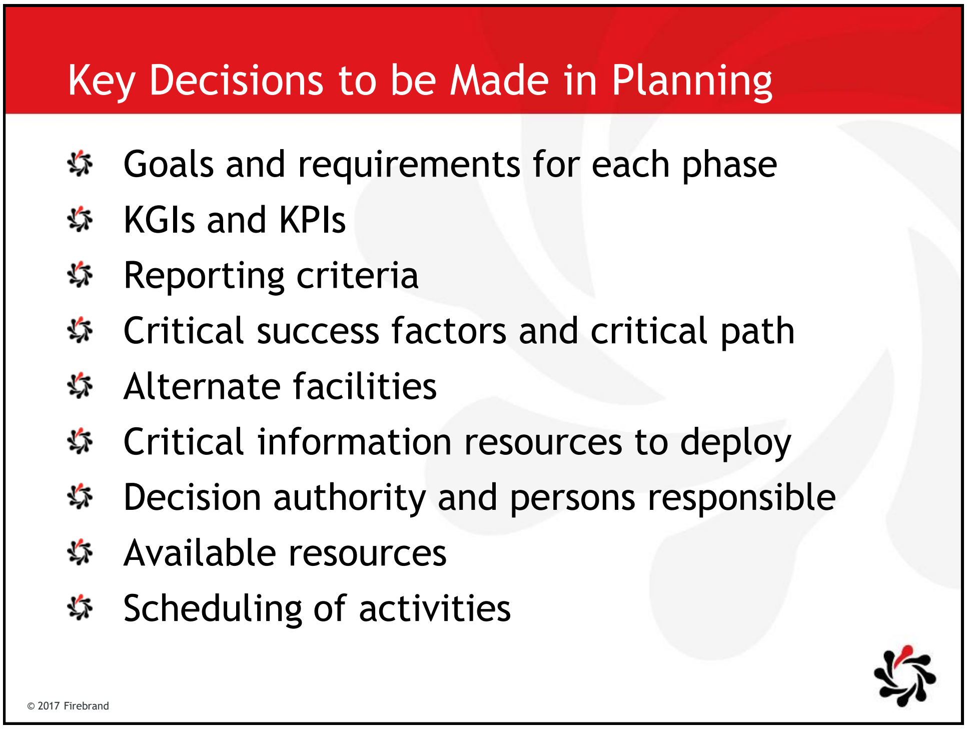
## Help/Service Desk Processes for Identifying Security Incidents

- Helpdesk should know how to identify an incident from a normal occurrence
  - Often the helpdesk will be the first to become aware of an incident
  - Prompt recognition and escalation is required



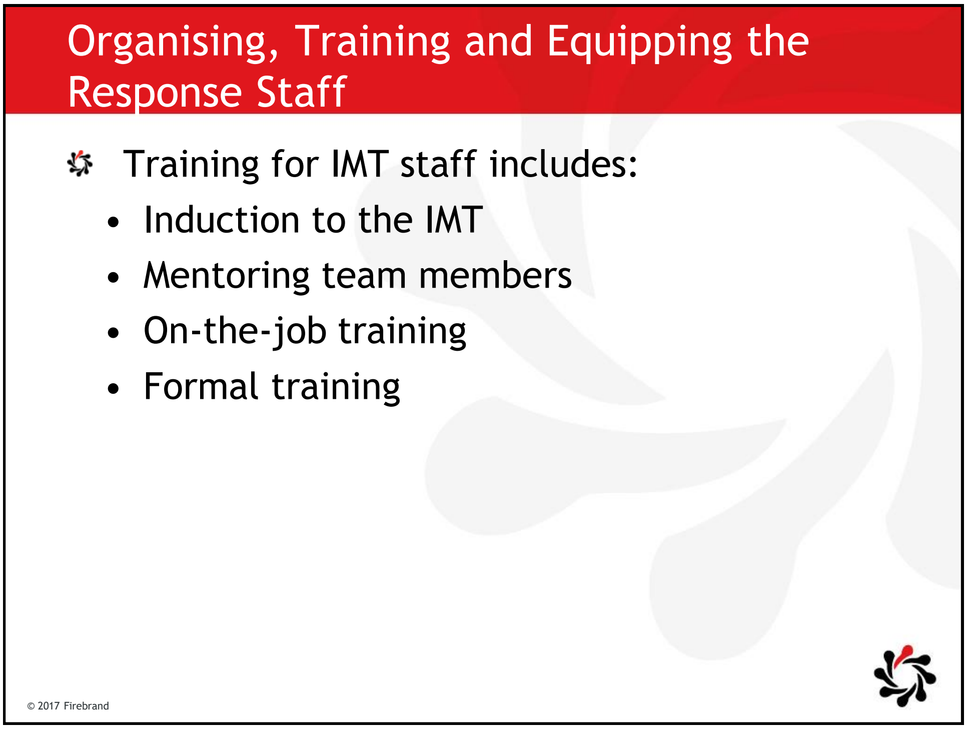
## Incident Management and Response Teams

- Some of the teams used in incident response include:
  - Emergency action team – evacuation
  - Damage assessment team – assess extent of damage – determine what may be salvaged
  - Emergency management team- coordinating activities of other teams
  - Relocation team – coordinate process to move to alternate location
  - Security team (CSIRT) – monitoring security



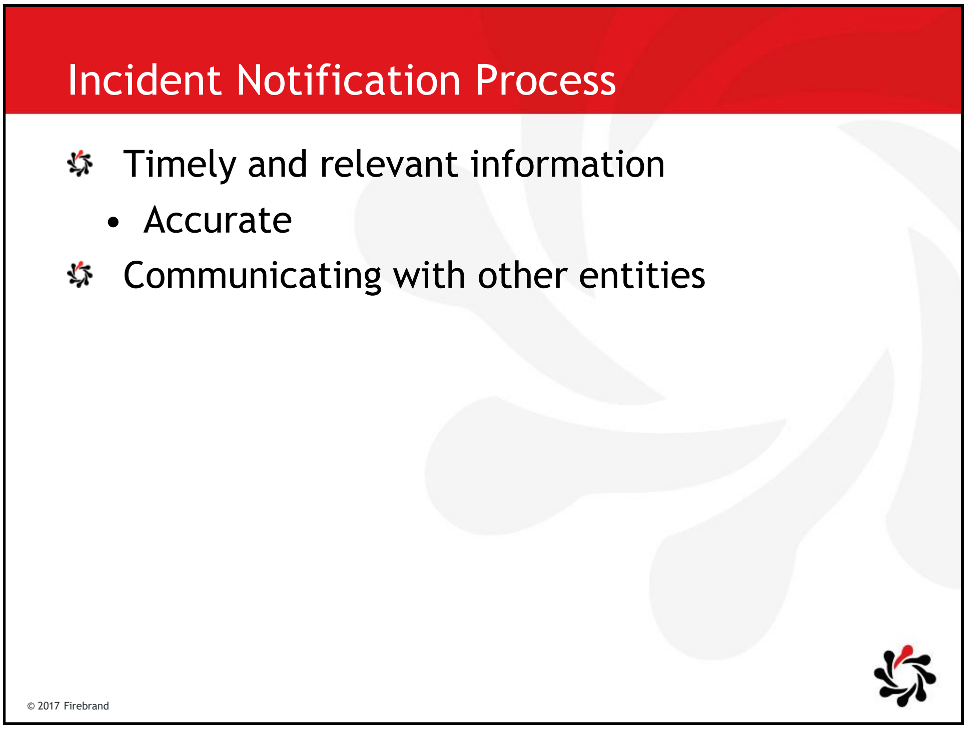
## Key Decisions to be Made in Planning

- Goals and requirements for each phase
- KGIs and KPIs
- Reporting criteria
- Critical success factors and critical path
- Alternate facilities
- Critical information resources to deploy
- Decision authority and persons responsible
- Available resources
- Scheduling of activities



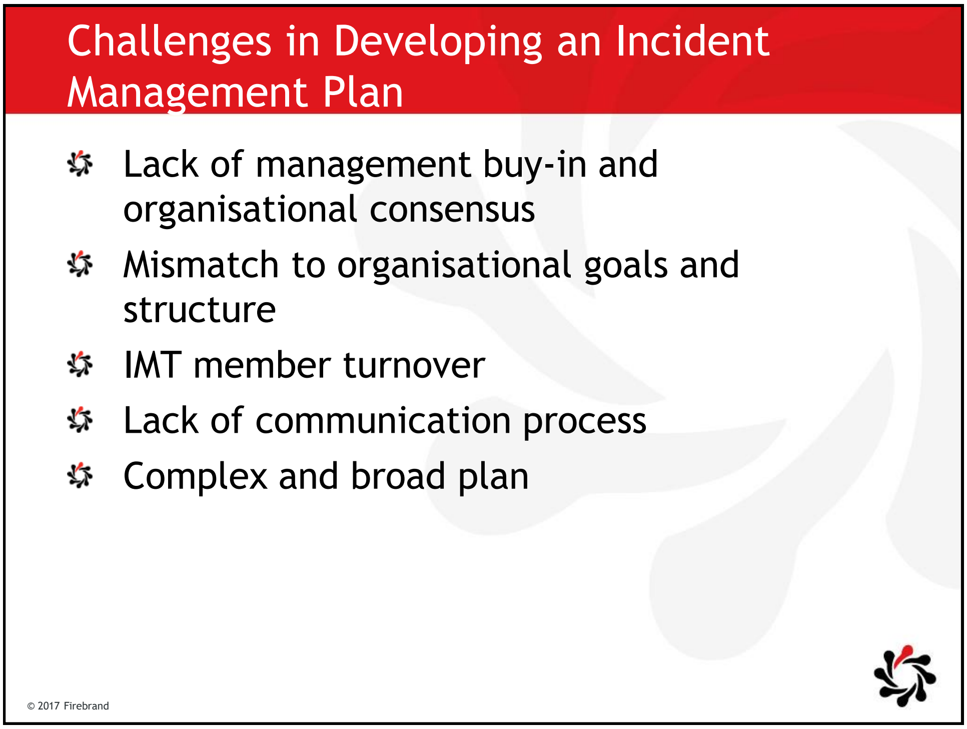
## Organising, Training and Equipping the Response Staff

- Training for IMT staff includes:
  - Induction to the IMT
  - Mentoring team members
  - On-the-job training
  - Formal training



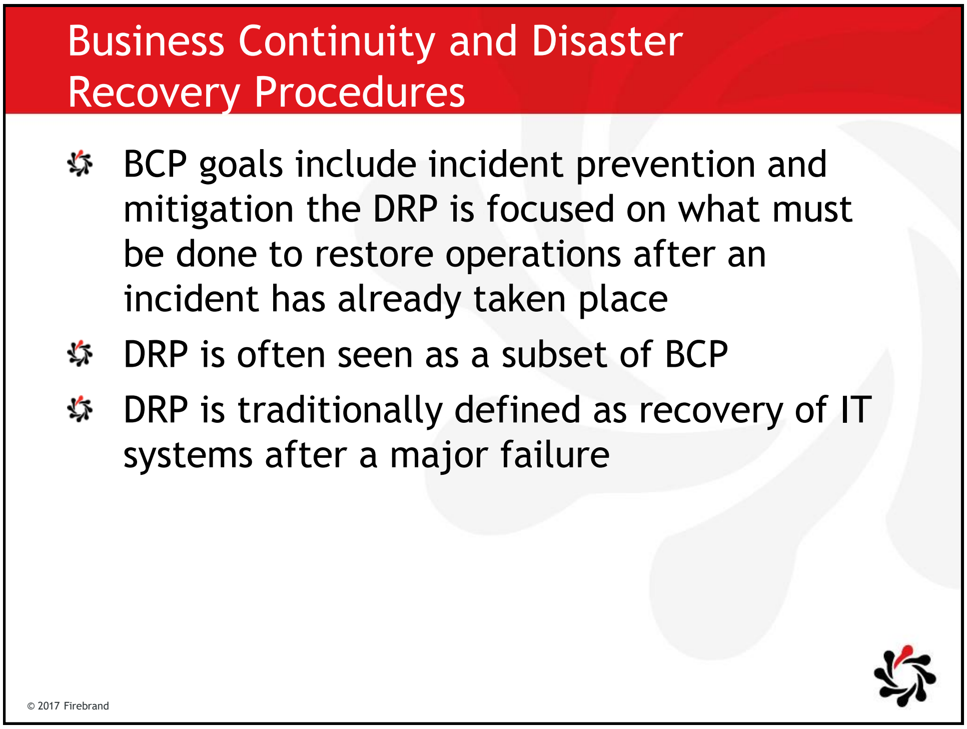
## Incident Notification Process

- Timely and relevant information
  - Accurate
- Communicating with other entities



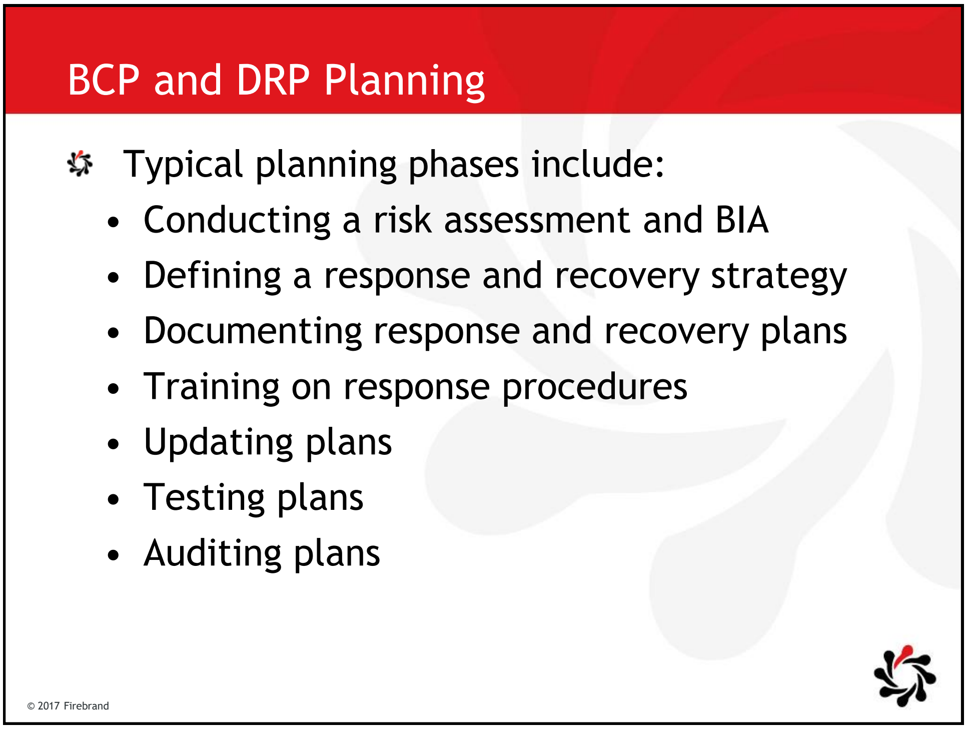
## Challenges in Developing an Incident Management Plan

- Lack of management buy-in and organisational consensus
- Mismatch to organisational goals and structure
- IMT member turnover
- Lack of communication process
- Complex and broad plan



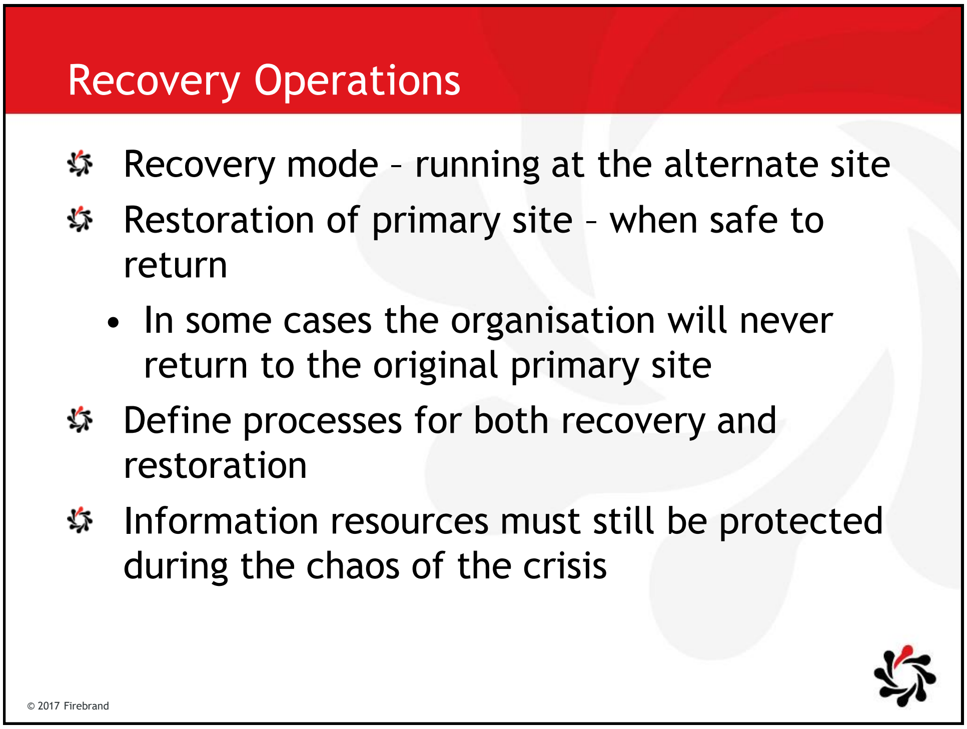
## Business Continuity and Disaster Recovery Procedures

- BCP goals include incident prevention and mitigation the DRP is focused on what must be done to restore operations after an incident has already taken place
- DRP is often seen as a subset of BCP
- DRP is traditionally defined as recovery of IT systems after a major failure



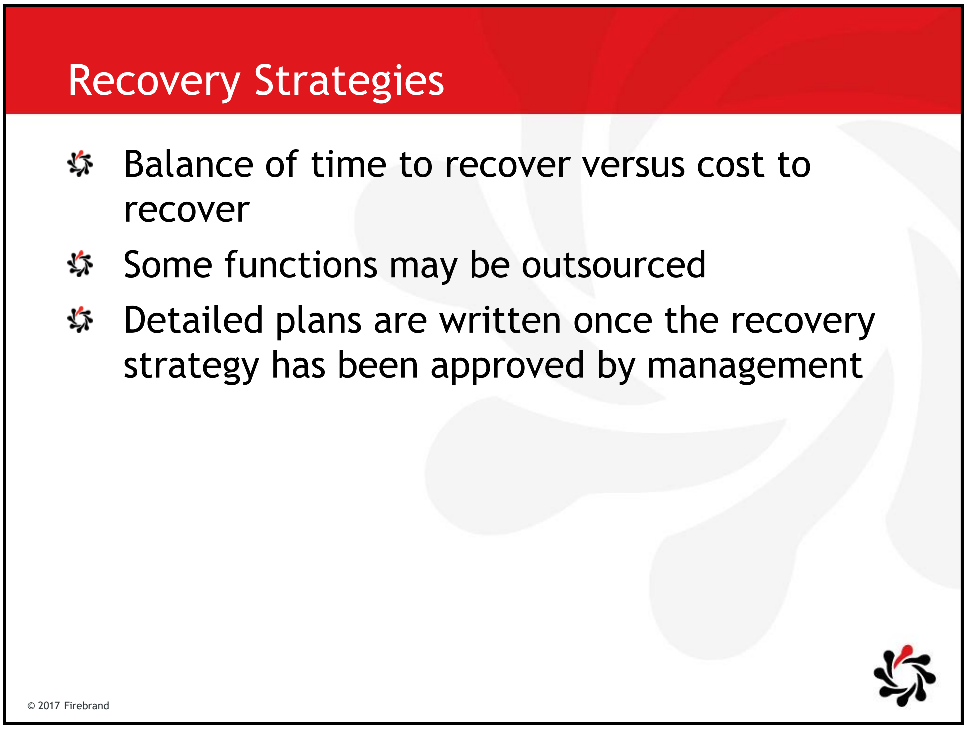
## BCP and DRP Planning

- Typical planning phases include:
  - Conducting a risk assessment and BIA
  - Defining a response and recovery strategy
  - Documenting response and recovery plans
  - Training on response procedures
  - Updating plans
  - Testing plans
  - Auditing plans



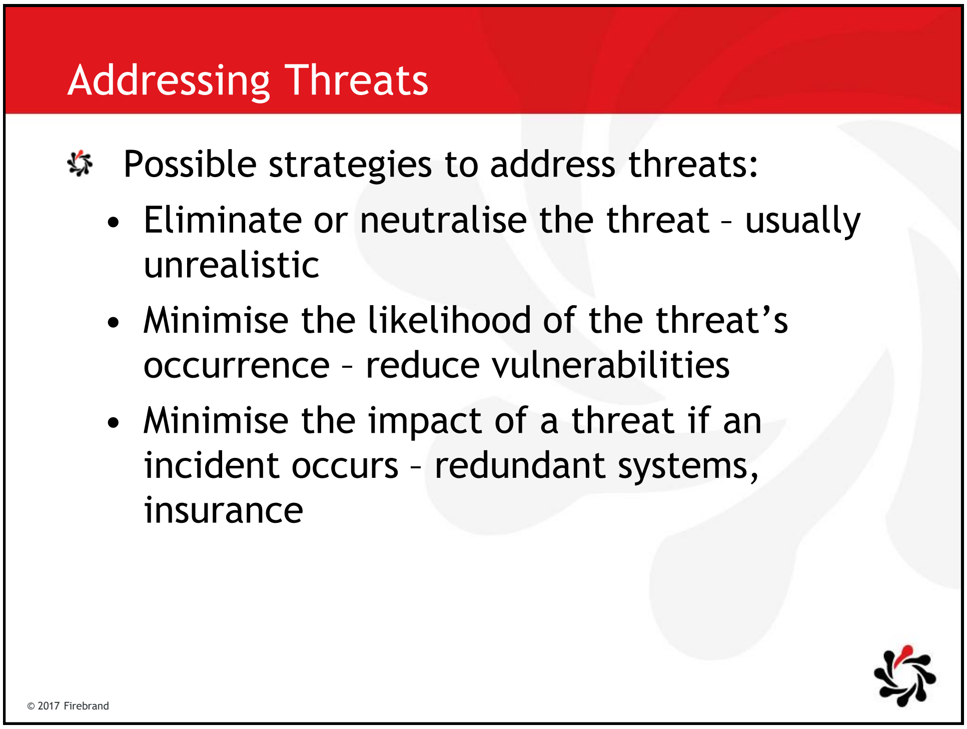
## Recovery Operations

- Recovery mode – running at the alternate site
- Restoration of primary site – when safe to return
  - In some cases the organisation will never return to the original primary site
- Define processes for both recovery and restoration
- Information resources must still be protected during the chaos of the crisis



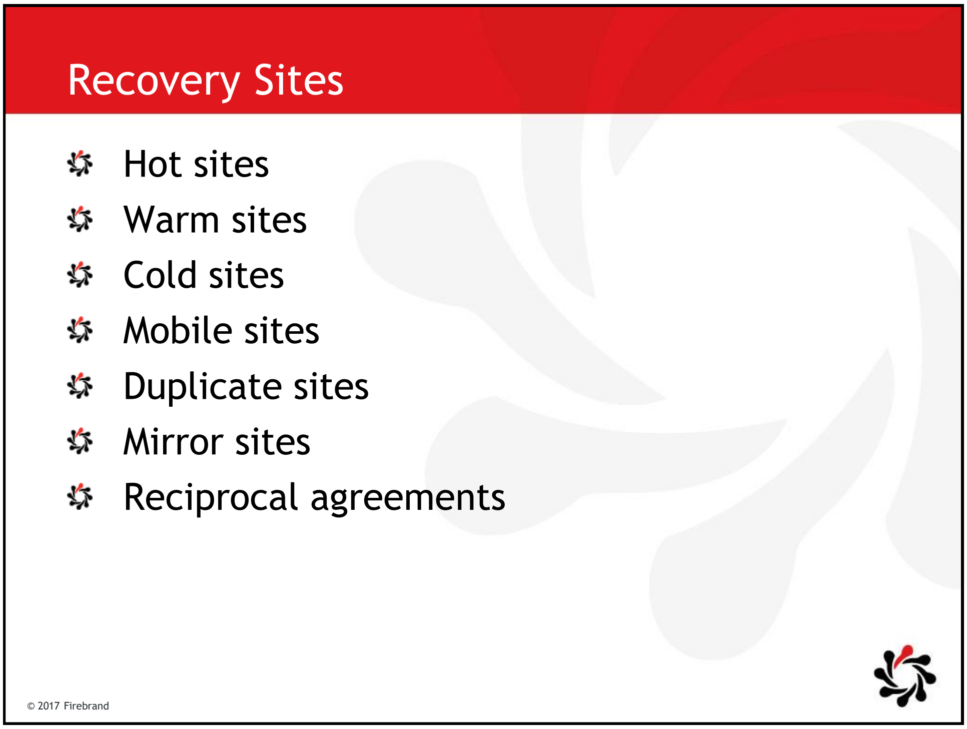
## Recovery Strategies

- Balance of time to recover versus cost to recover
- Some functions may be outsourced
- Detailed plans are written once the recovery strategy has been approved by management



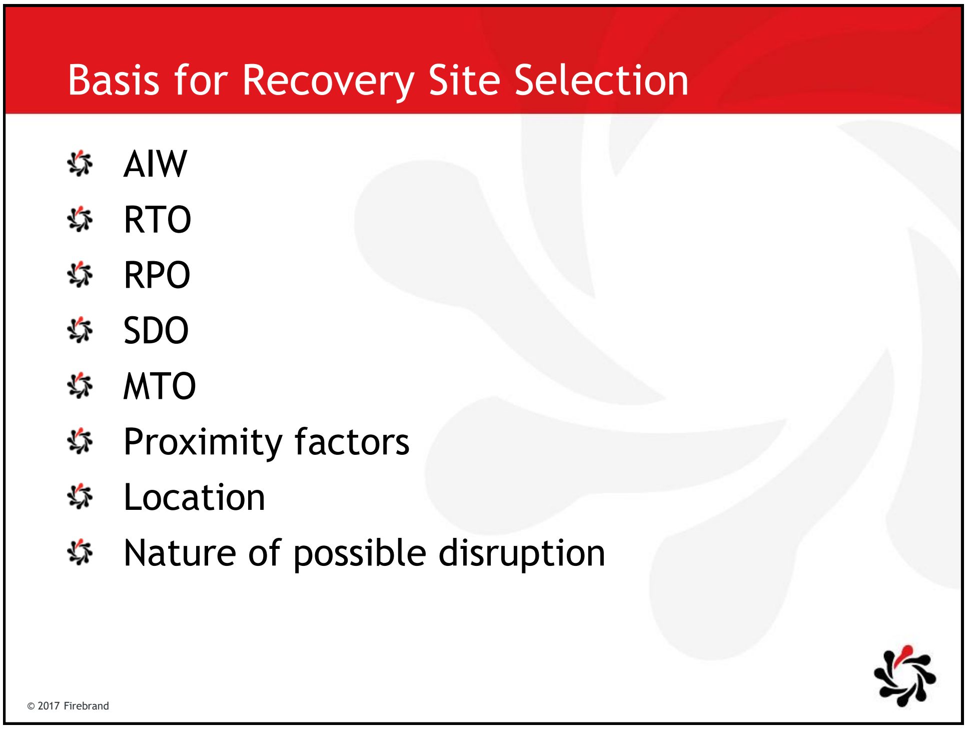
## Addressing Threats

- Possible strategies to address threats:
  - Eliminate or neutralise the threat – usually unrealistic
  - Minimise the likelihood of the threat’s occurrence – reduce vulnerabilities
  - Minimise the impact of a threat if an incident occurs – redundant systems, insurance



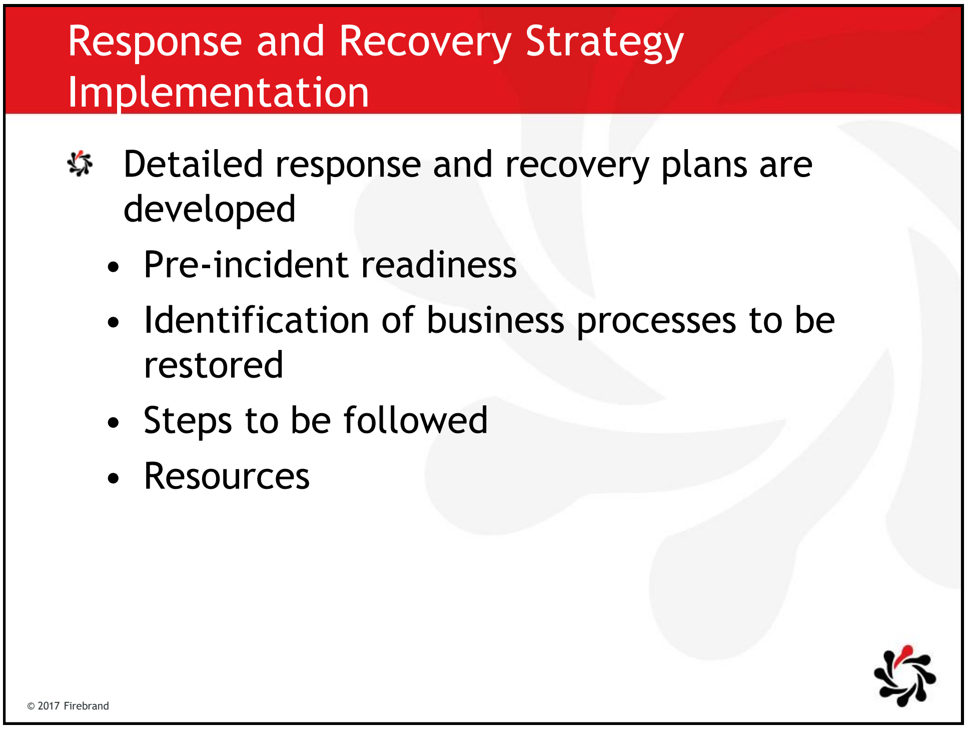
## Recovery Sites

- Hot sites
- Warm sites
- Cold sites
- Mobile sites
- Duplicate sites
- Mirror sites
- Reciprocal agreements



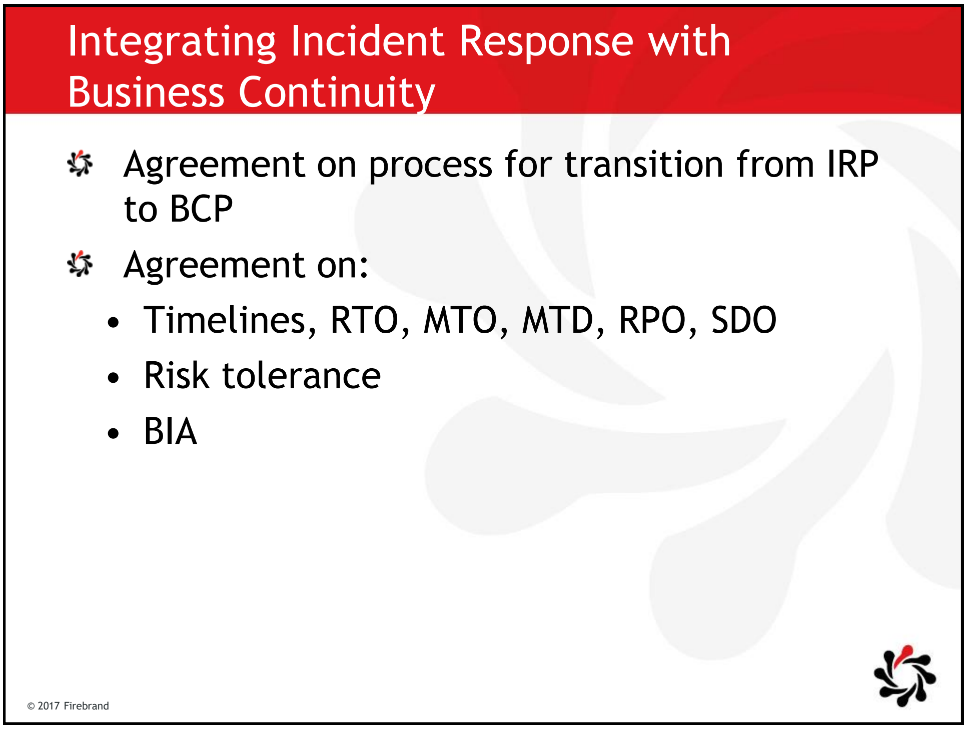
## Basis for Recovery Site Selection

- AIW
- RTO
- RPO
- SDO
- MTO
- Proximity factors
- Location
- Nature of possible disruption



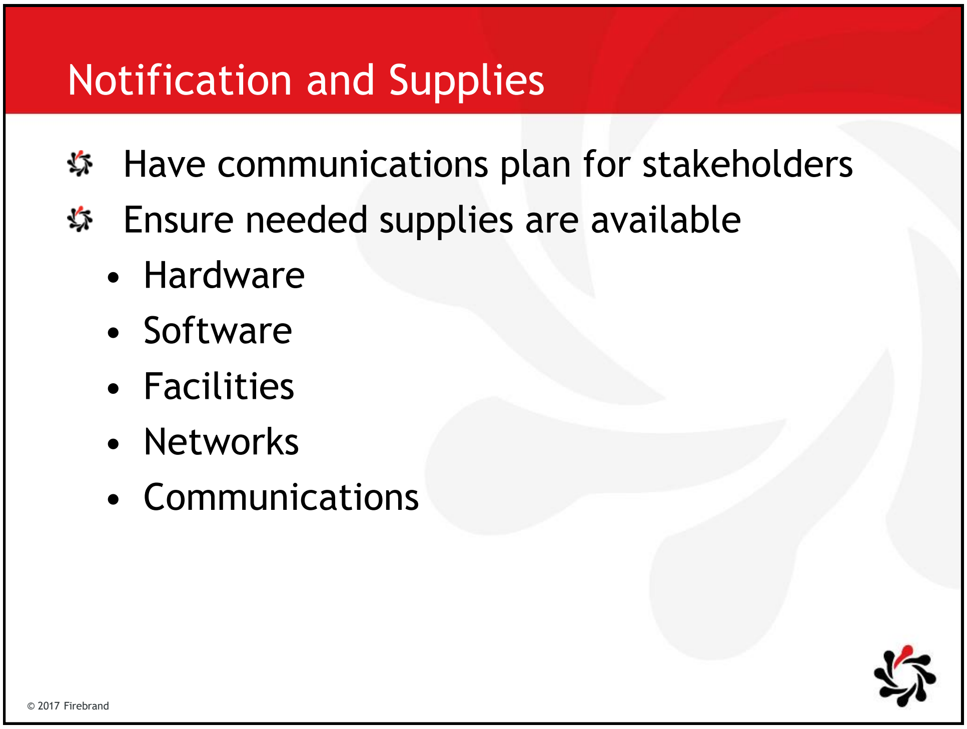
## Response and Recovery Strategy Implementation

- Detailed response and recovery plans are developed
  - Pre-incident readiness
  - Identification of business processes to be restored
  - Steps to be followed
  - Resources



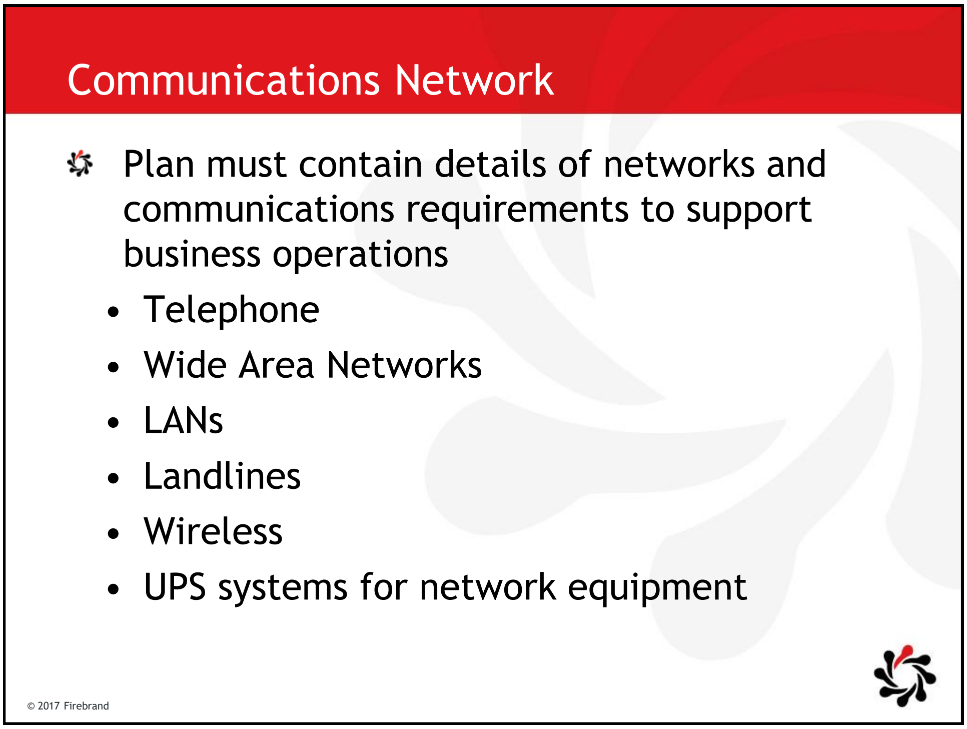
## Integrating Incident Response with Business Continuity

- Agreement on process for transition from IRP to BCP
- Agreement on:
  - Timelines, RTO, MTO, MTD, RPO, SDO
  - Risk tolerance
  - BIA



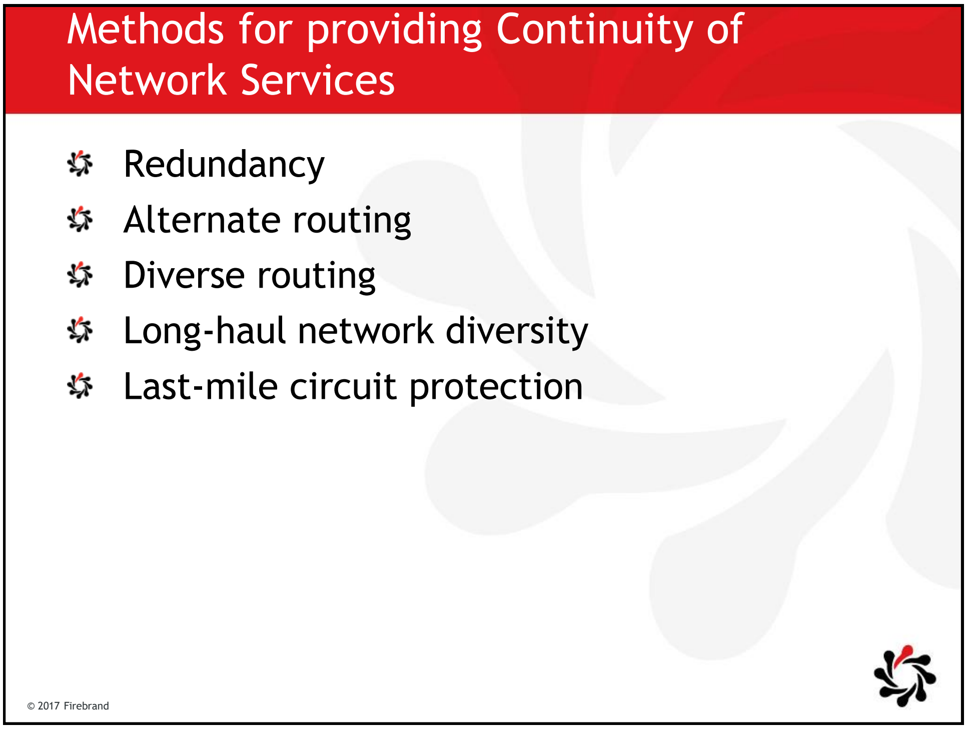
## Notification and Supplies

- Have communications plan for stakeholders
- Ensure needed supplies are available
  - Hardware
  - Software
  - Facilities
  - Networks
  - Communications



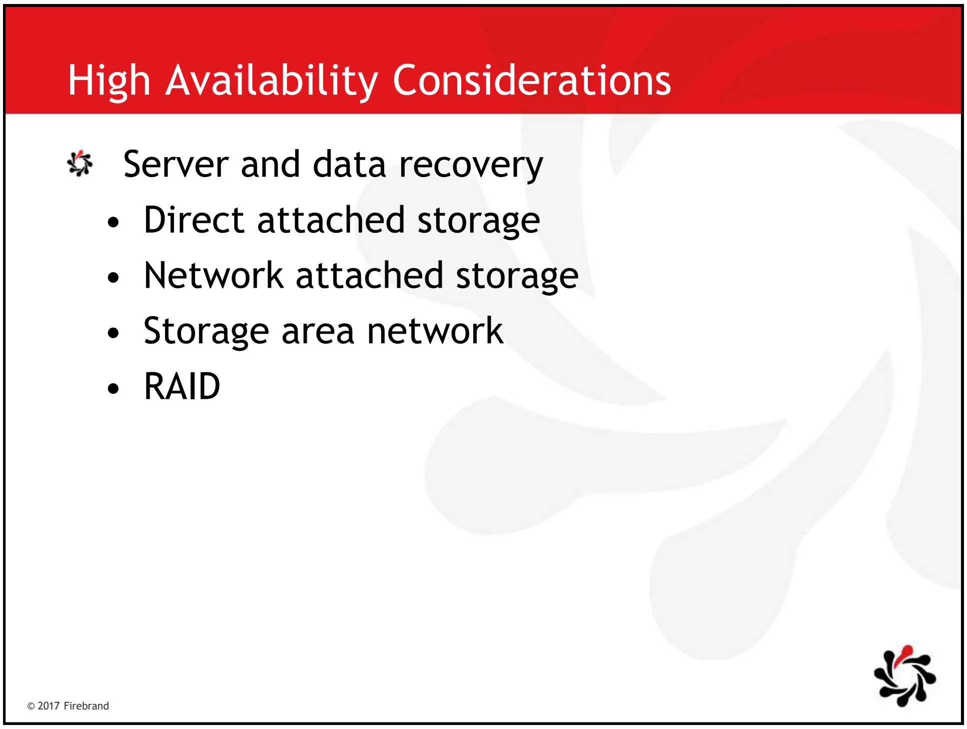
## Communications Network

- Plan must contain details of networks and communications requirements to support business operations
  - Telephone
  - Wide Area Networks
  - LANs
  - Landlines
  - Wireless
  - UPS systems for network equipment



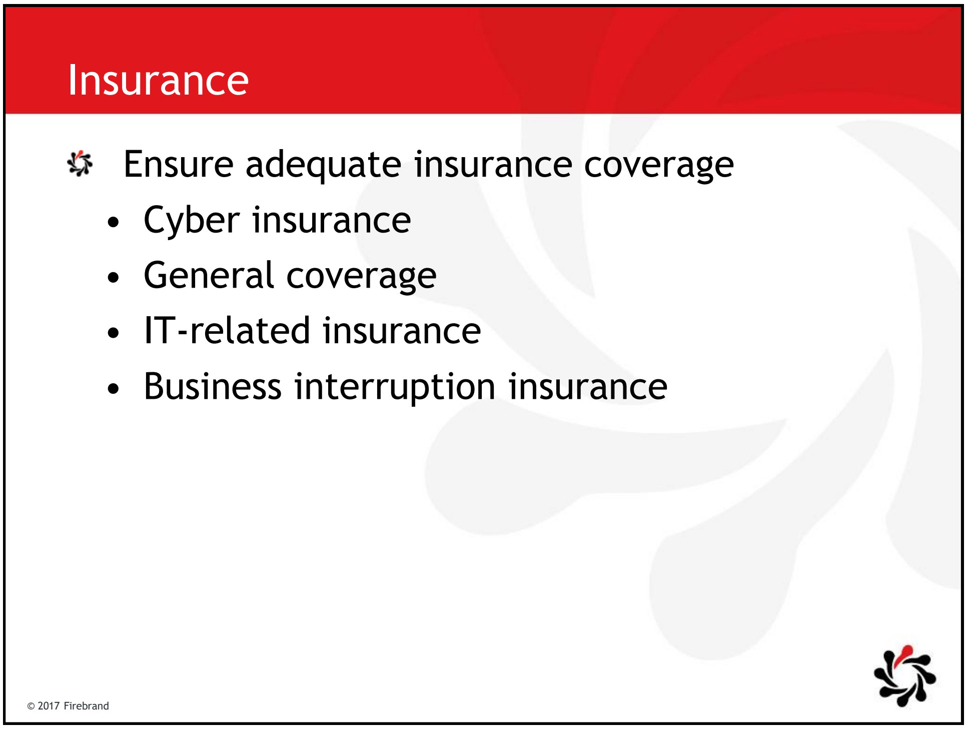
## Methods for providing Continuity of Network Services

- Redundancy
- Alternate routing
- Diverse routing
- Long-haul network diversity
- Last-mile circuit protection



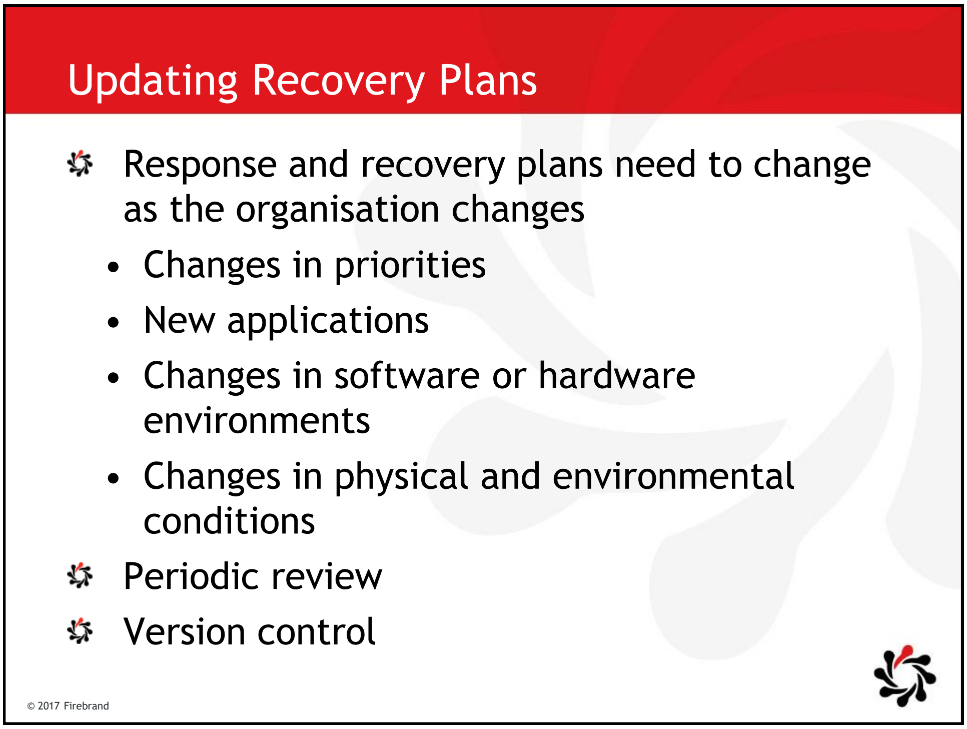
## High Availability Considerations

- Server and data recovery
  - Direct attached storage
  - Network attached storage
  - Storage area network
  - RAID



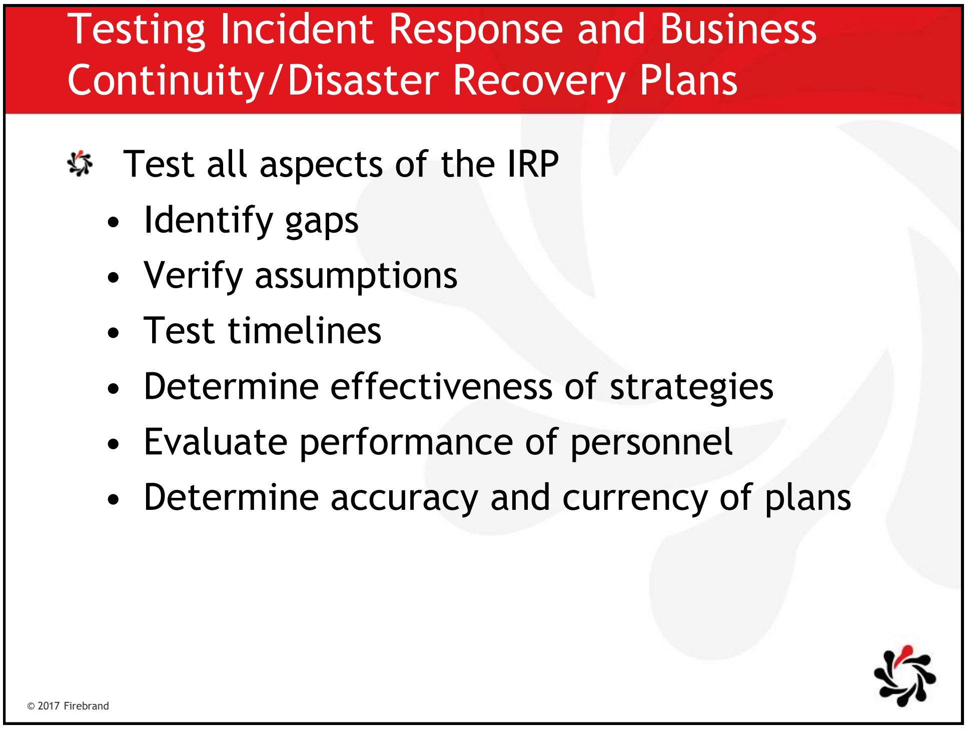
## Insurance

- Ensure adequate insurance coverage
  - Cyber insurance
  - General coverage
  - IT-related insurance
  - Business interruption insurance



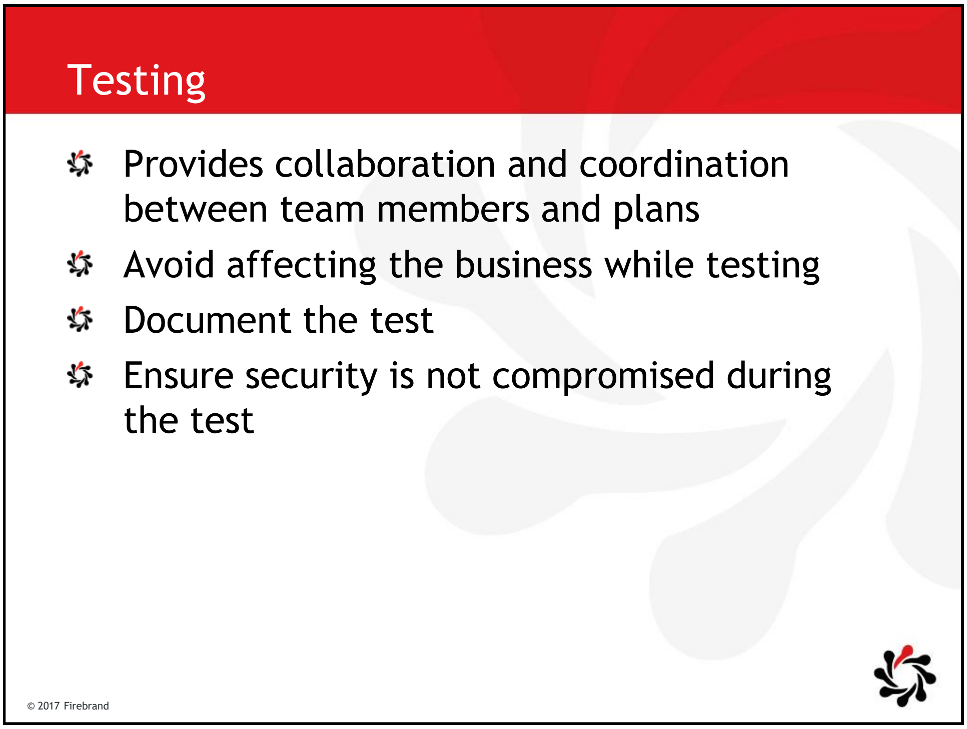
## Updating Recovery Plans

- Response and recovery plans need to change as the organisation changes
  - Changes in priorities
  - New applications
  - Changes in software or hardware environments
  - Changes in physical and environmental conditions
- Periodic review
- Version control



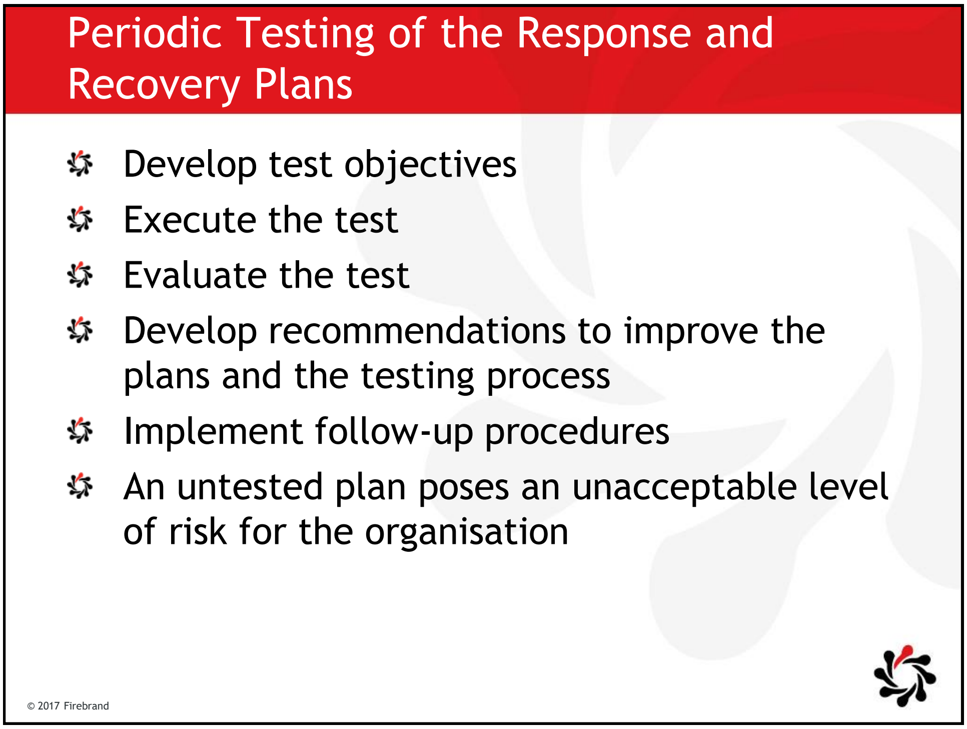
## Testing Incident Response and Business Continuity/Disaster Recovery Plans

- Test all aspects of the IRP
  - Identify gaps
  - Verify assumptions
  - Test timelines
  - Determine effectiveness of strategies
  - Evaluate performance of personnel
  - Determine accuracy and currency of plans



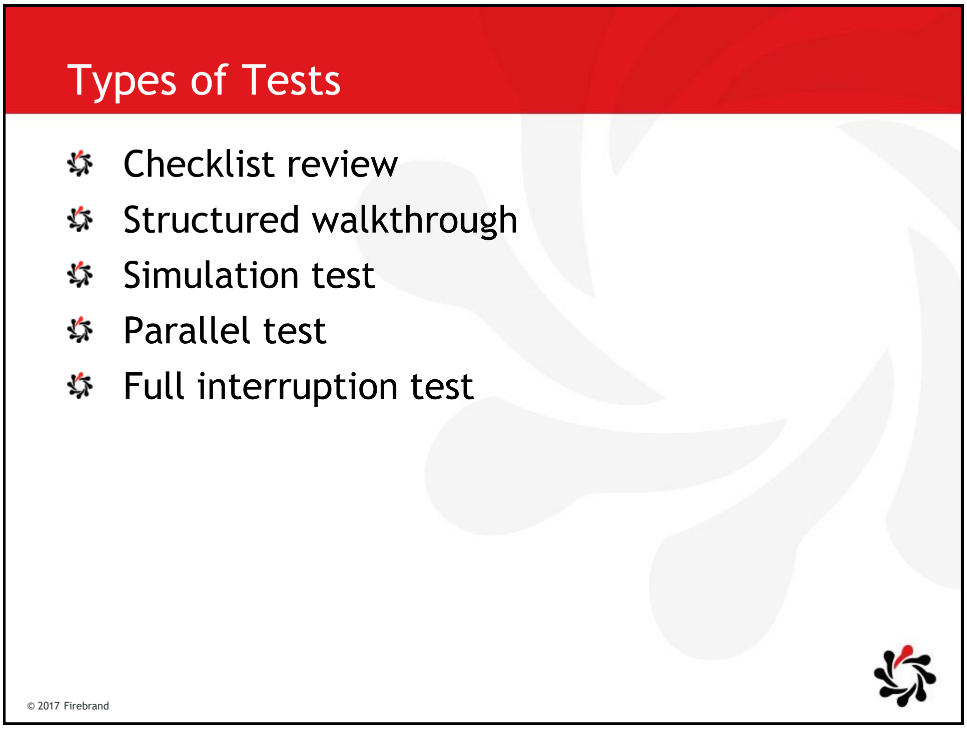
## Testing

- Provides collaboration and coordination between team members and plans
- Avoid affecting the business while testing
- Document the test
- Ensure security is not compromised during the test



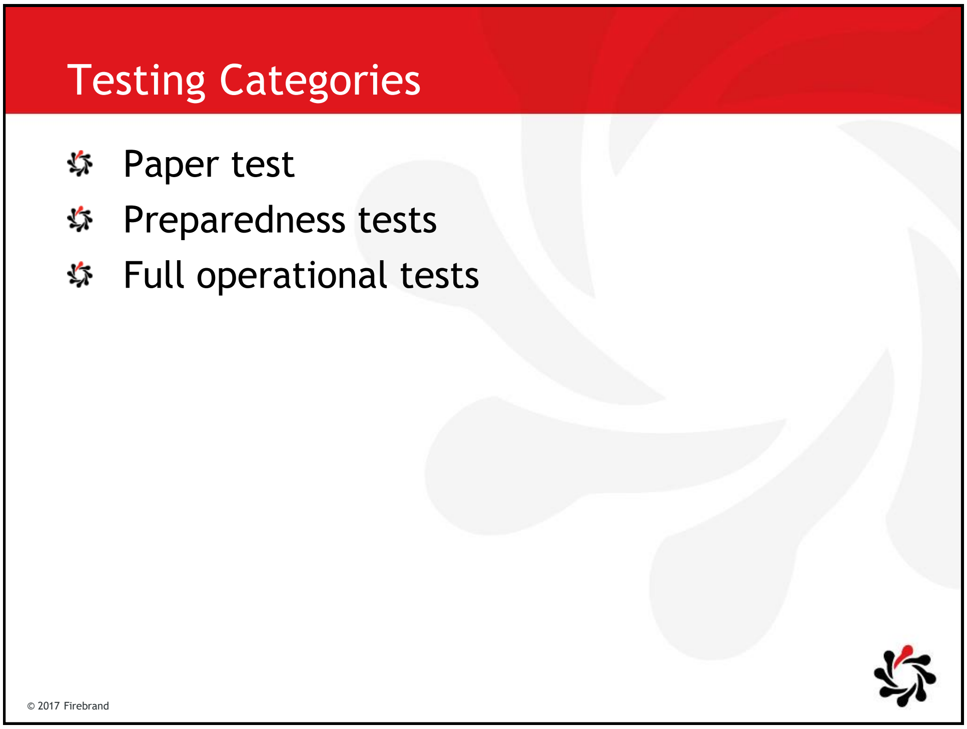
## Periodic Testing of the Response and Recovery Plans

- Develop test objectives
- Execute the test
- Evaluate the test
- Develop recommendations to improve the plans and the testing process
- Implement follow-up procedures
- An untested plan poses an unacceptable level of risk for the organisation



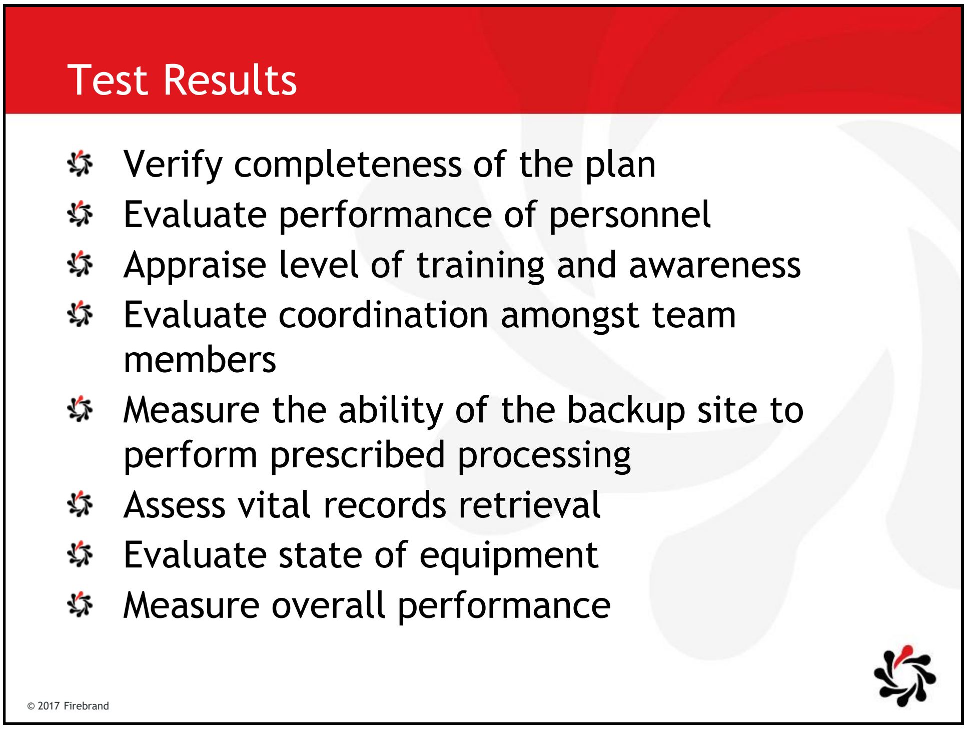
## Types of Tests

- Checklist review
- Structured walkthrough
- Simulation test
- Parallel test
- Full interruption test



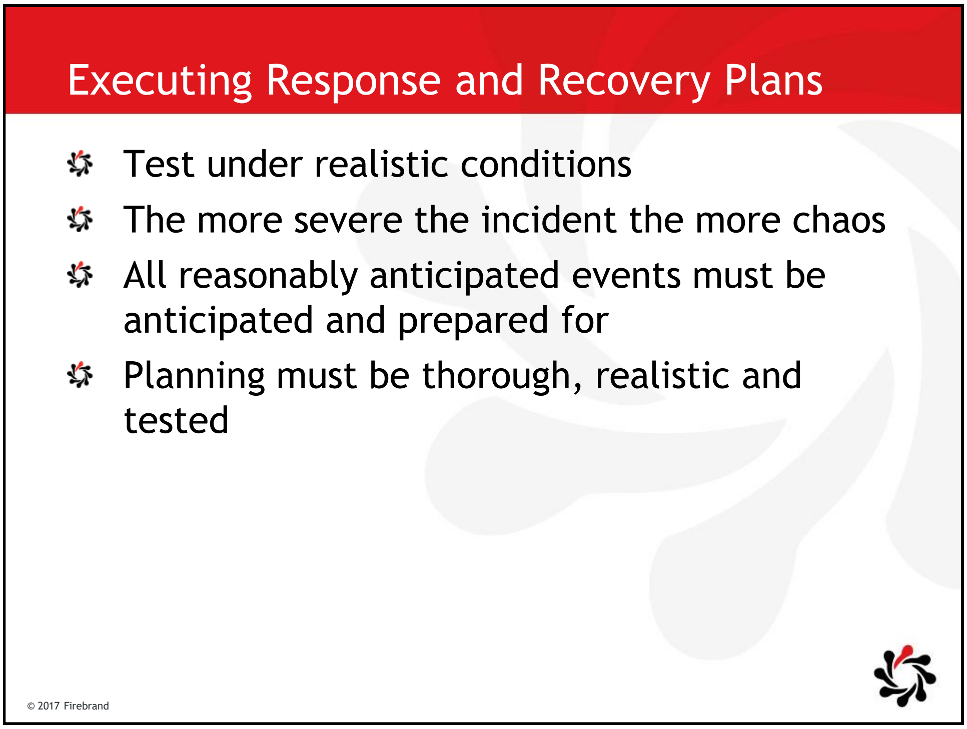
## Testing Categories

- Paper test
- Preparedness tests
- Full operational tests



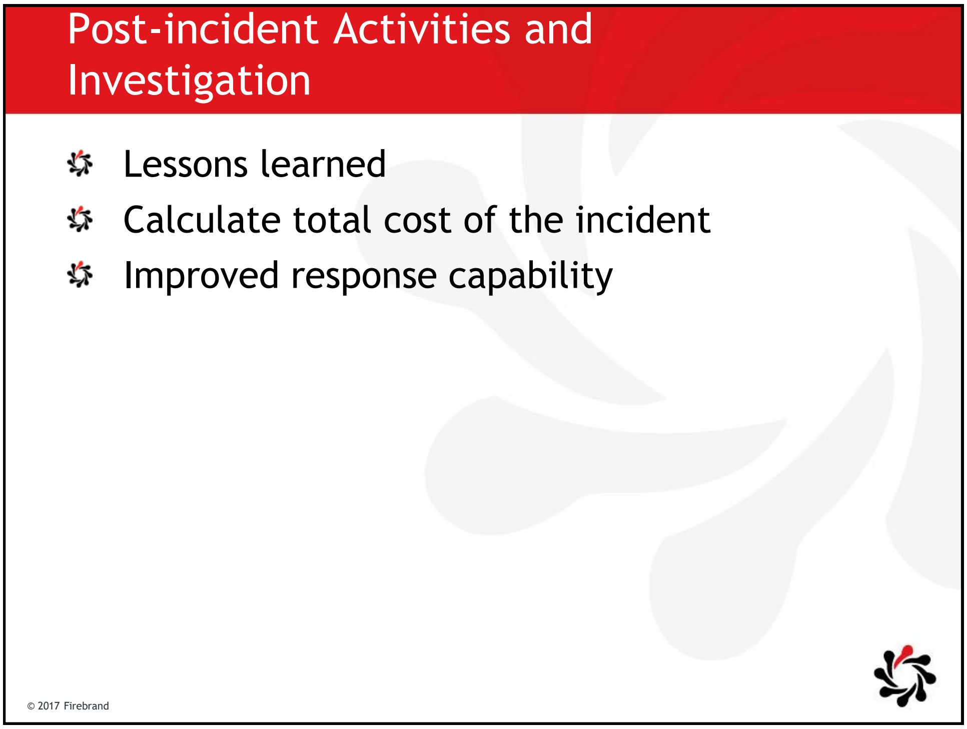
## Test Results

- Verify completeness of the plan
- Evaluate performance of personnel
- Appraise level of training and awareness
- Evaluate coordination amongst team members
- Measure the ability of the backup site to perform prescribed processing
- Assess vital records retrieval
- Evaluate state of equipment
- Measure overall performance



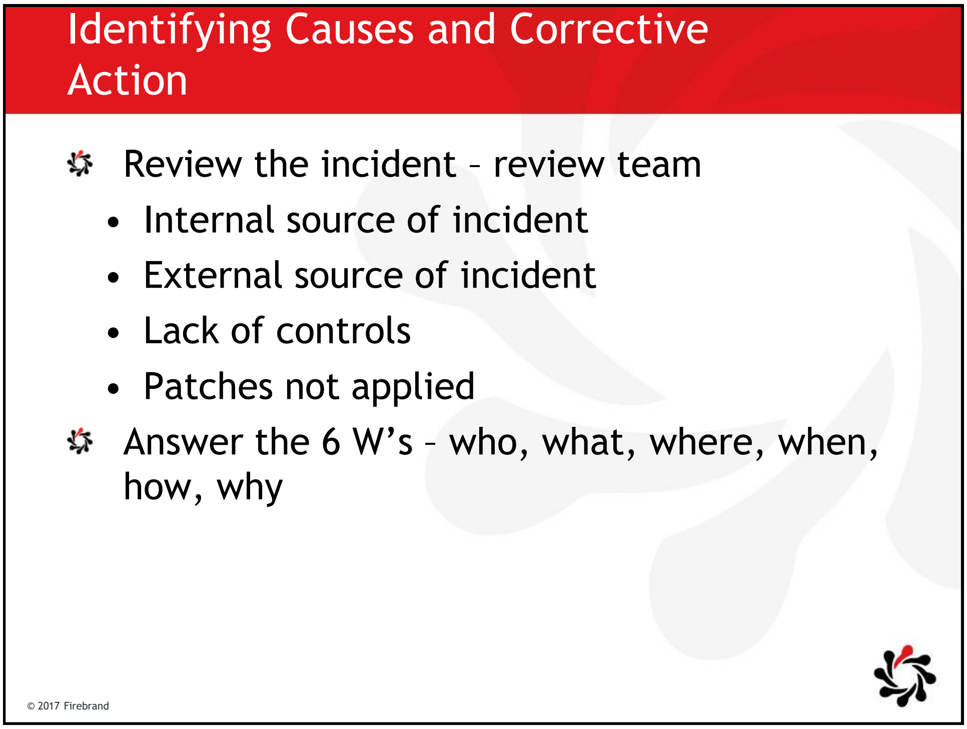
## Executing Response and Recovery Plans

- Test under realistic conditions
- The more severe the incident the more chaos
- All reasonably anticipated events must be anticipated and prepared for
- Planning must be thorough, realistic and tested



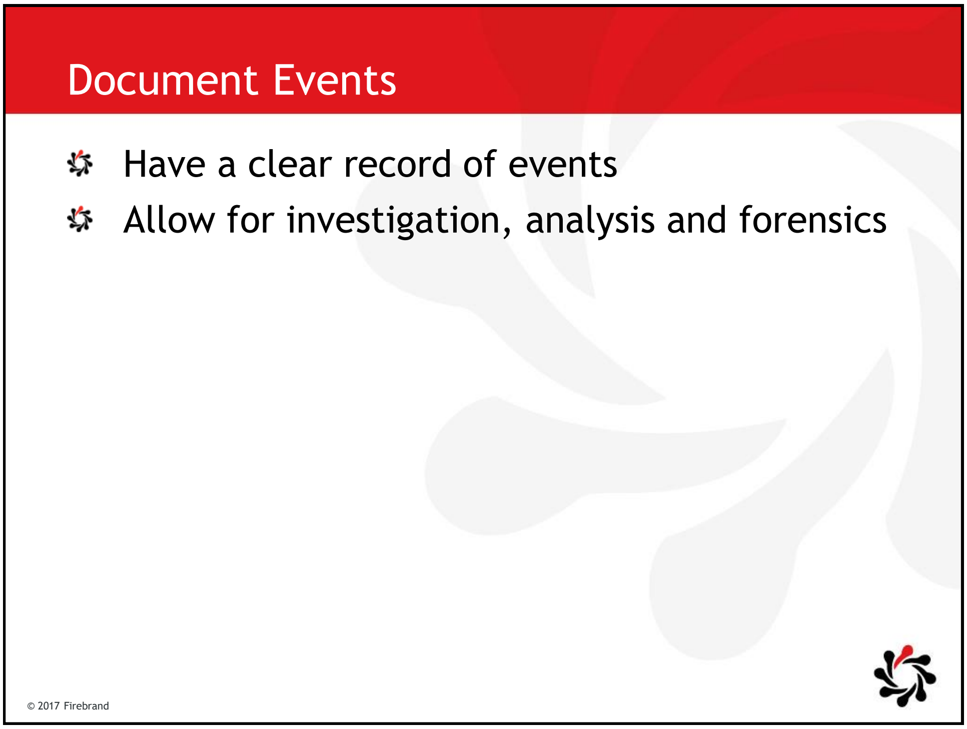
## Post-incident Activities and Investigation

- Lessons learned
- Calculate total cost of the incident
- Improved response capability



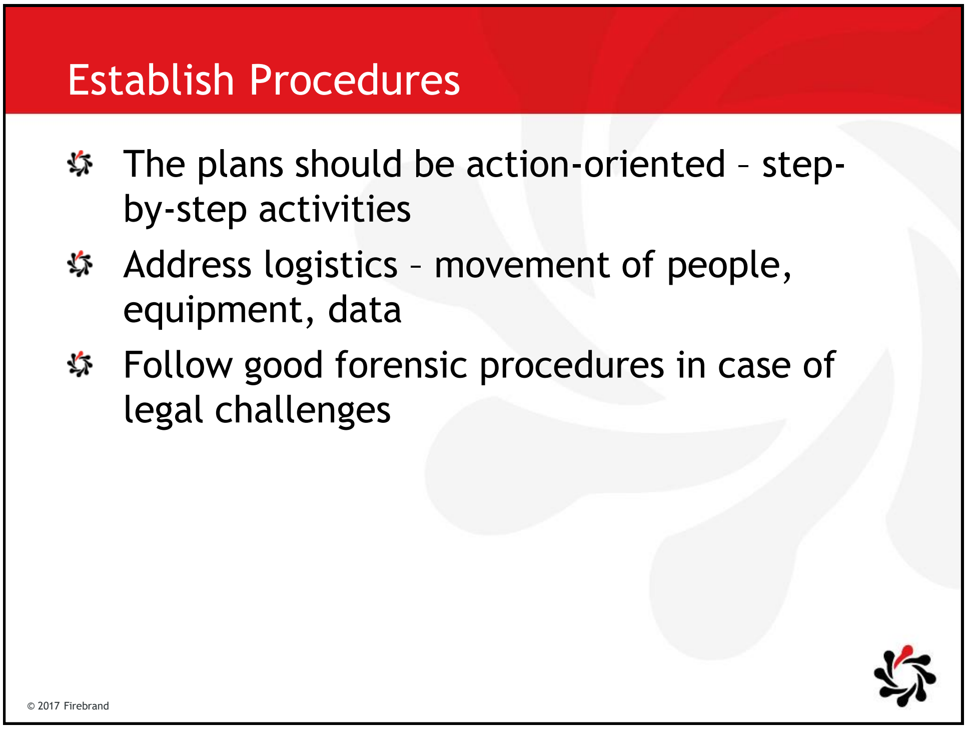
## Identifying Causes and Corrective Action

- Review the incident – review team
  - Internal source of incident
  - External source of incident
  - Lack of controls
  - Patches not applied
- Answer the 6 W’s – who, what, where, when, how, why



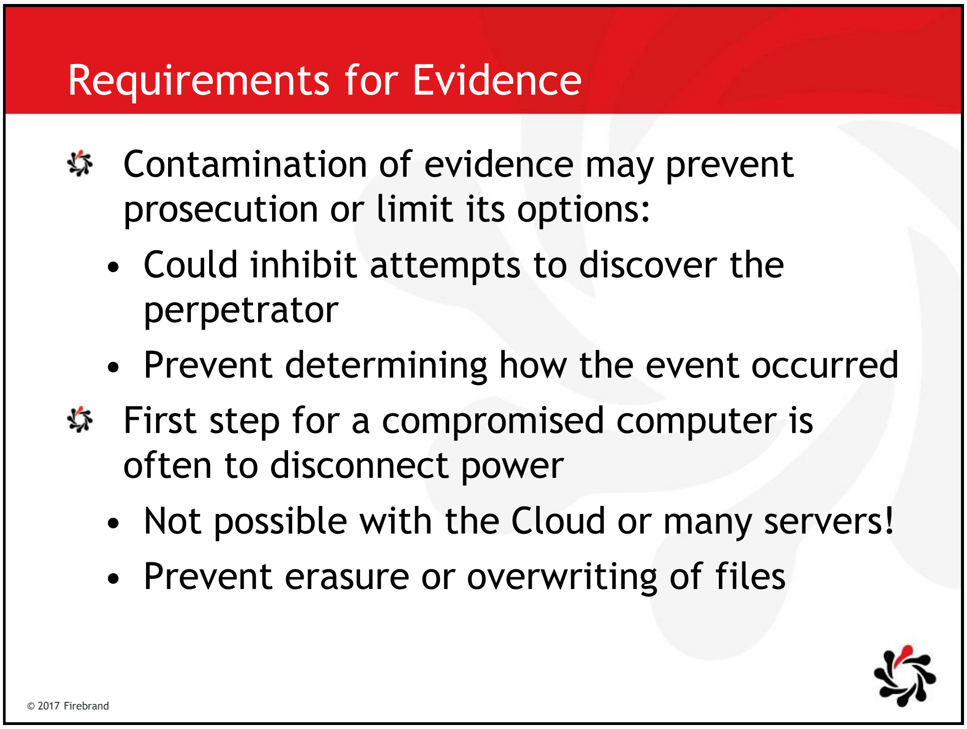
## Document Events

- Have a clear record of events
- Allow for investigation, analysis and forensics



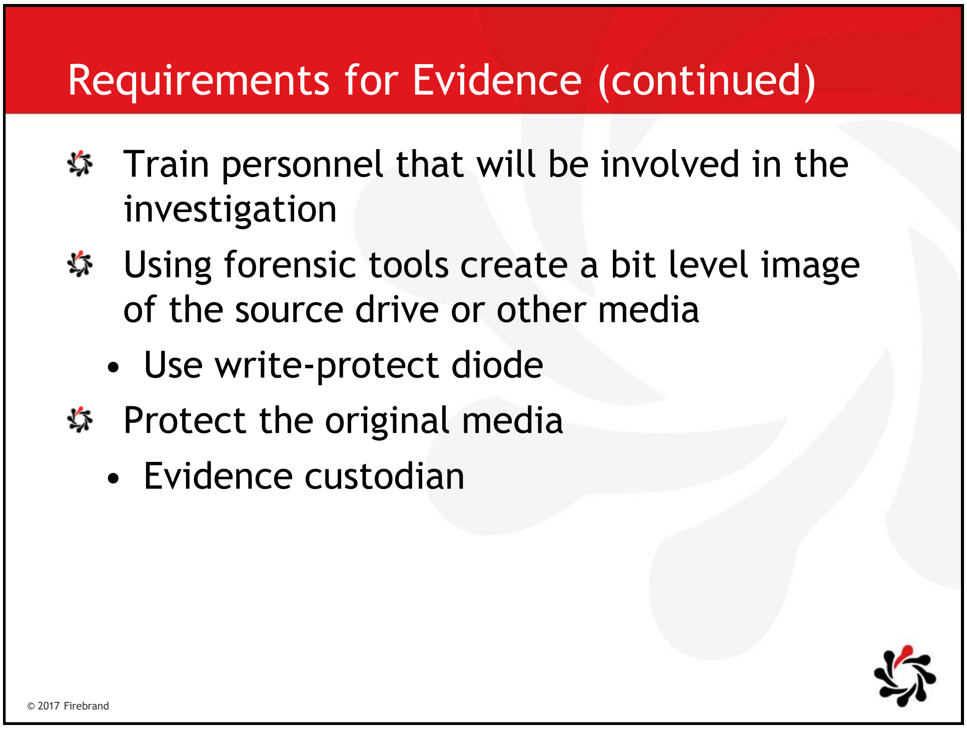
## Establish Procedures

- The plans should be action-oriented – step-by-step activities
- Address logistics – movement of people, equipment, data
- Follow good forensic procedures in case of legal challenges



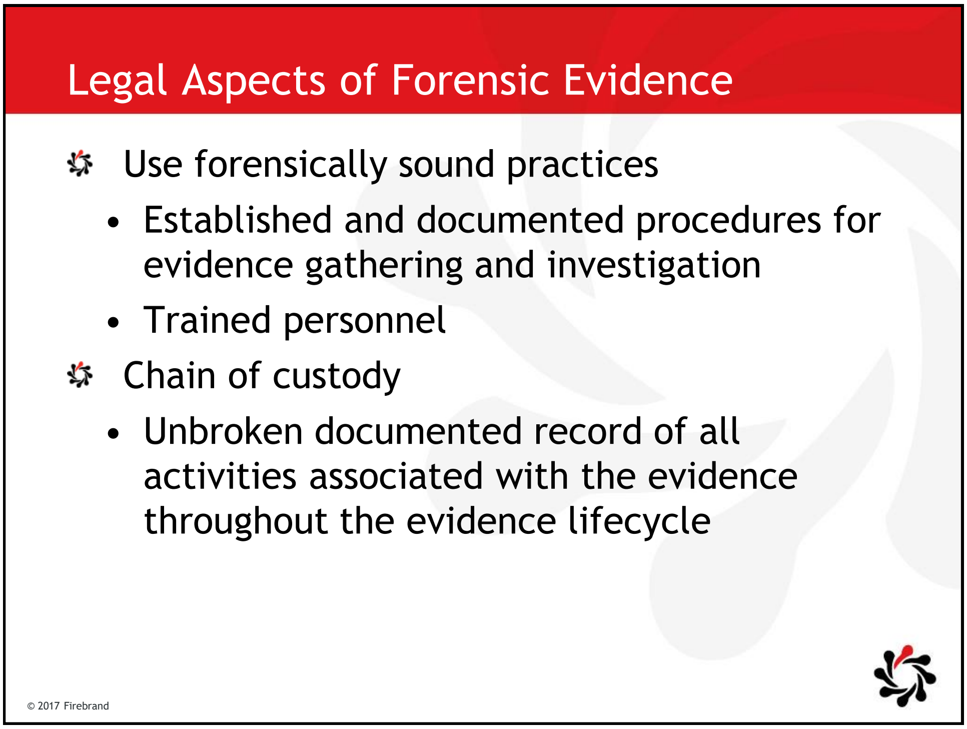
## Requirements for Evidence

- Contamination of evidence may prevent prosecution or limit its options:
  - Could inhibit attempts to discover the perpetrator
  - Prevent determining how the event occurred
- First step for a compromised computer is often to disconnect power
  - Not possible with the Cloud or many servers!
  - Prevent erasure or overwriting of files



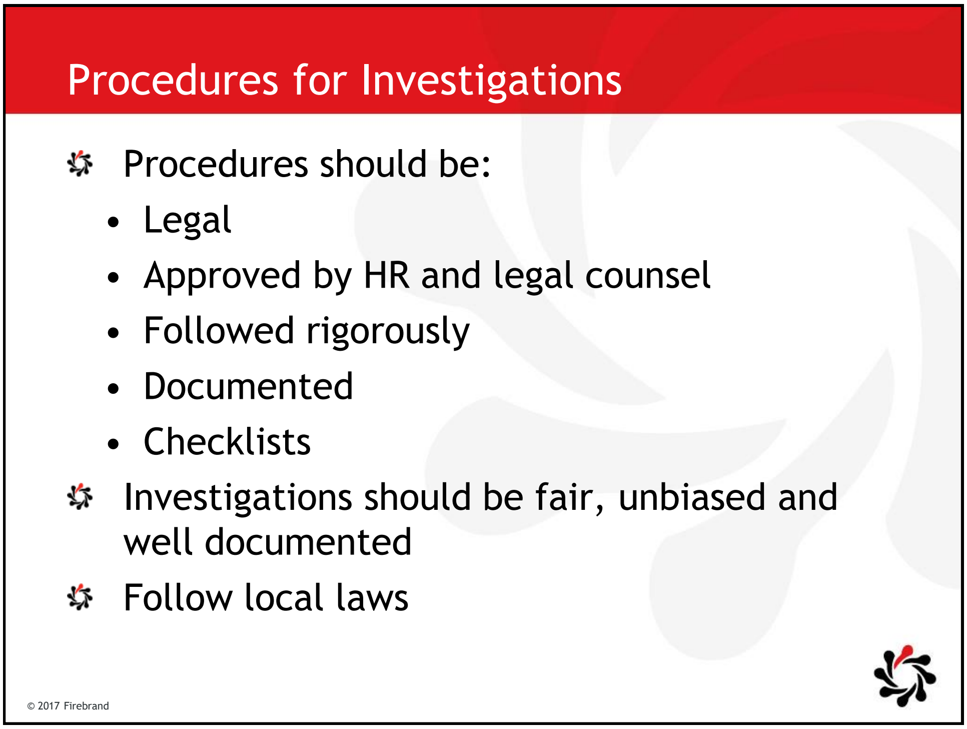
## Requirements for Evidence (continued)

- Train personnel that will be involved in the investigation
- Using forensic tools create a bit level image of the source drive or other media
  - Use write-protect diode
- Protect the original media
  - Evidence custodian



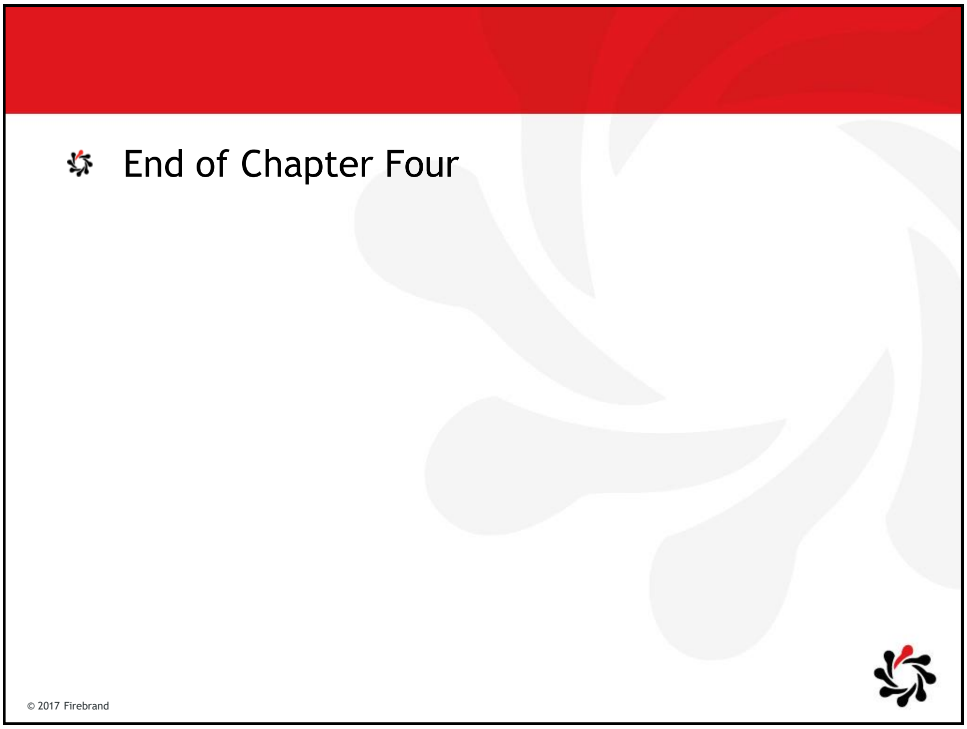
## Legal Aspects of Forensic Evidence

- Use forensically sound practices
  - Established and documented procedures for evidence gathering and investigation
  - Trained personnel
- Chain of custody
  - Unbroken documented record of all activities associated with the evidence throughout the evidence lifecycle



## Procedures for Investigations

- Procedures should be:
  - Legal
  - Approved by HR and legal counsel
  - Followed rigorously
  - Documented
  - Checklists
- Investigations should be fair, unbiased and well documented
- Follow local laws



- End of Chapter Four