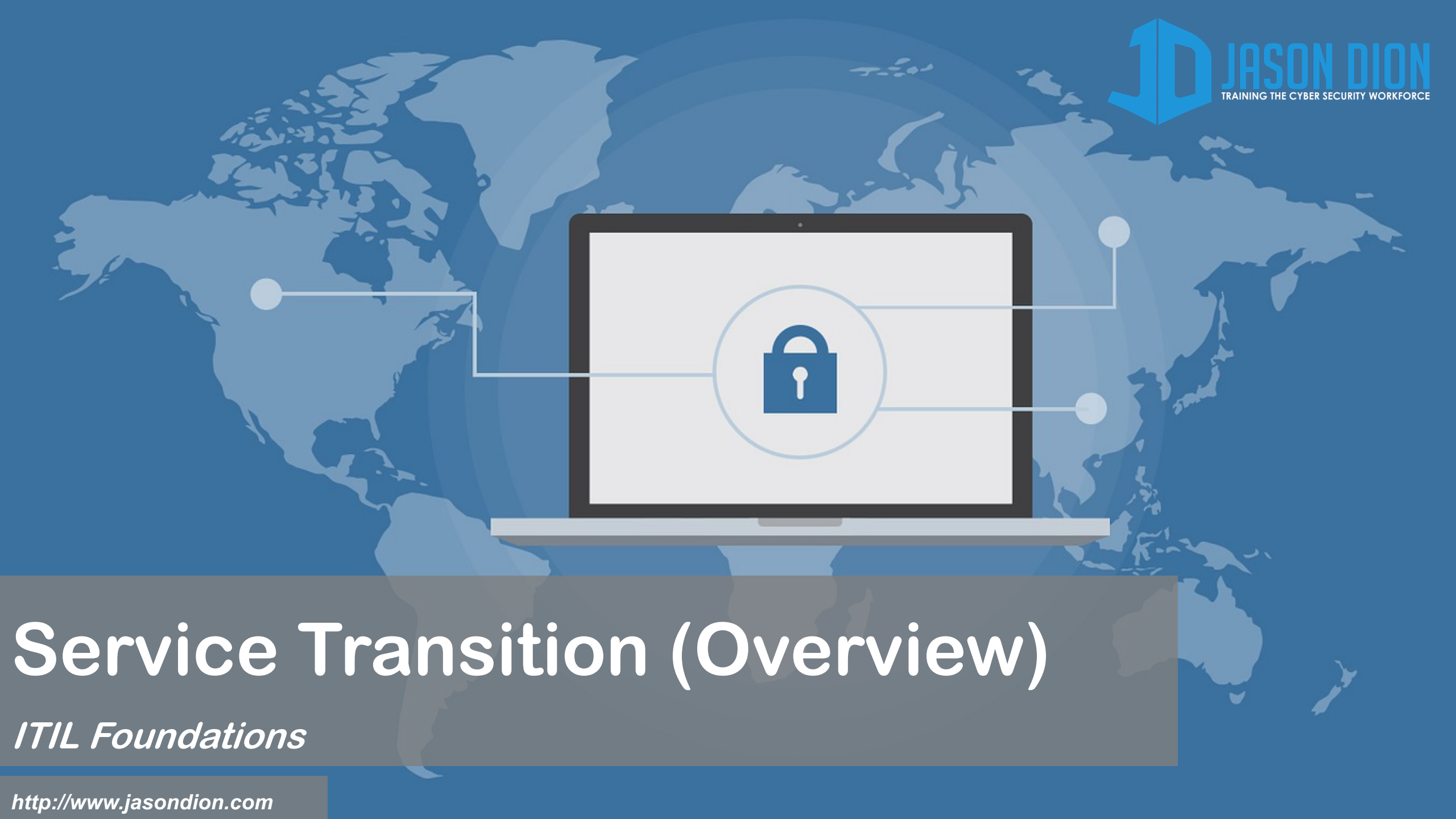
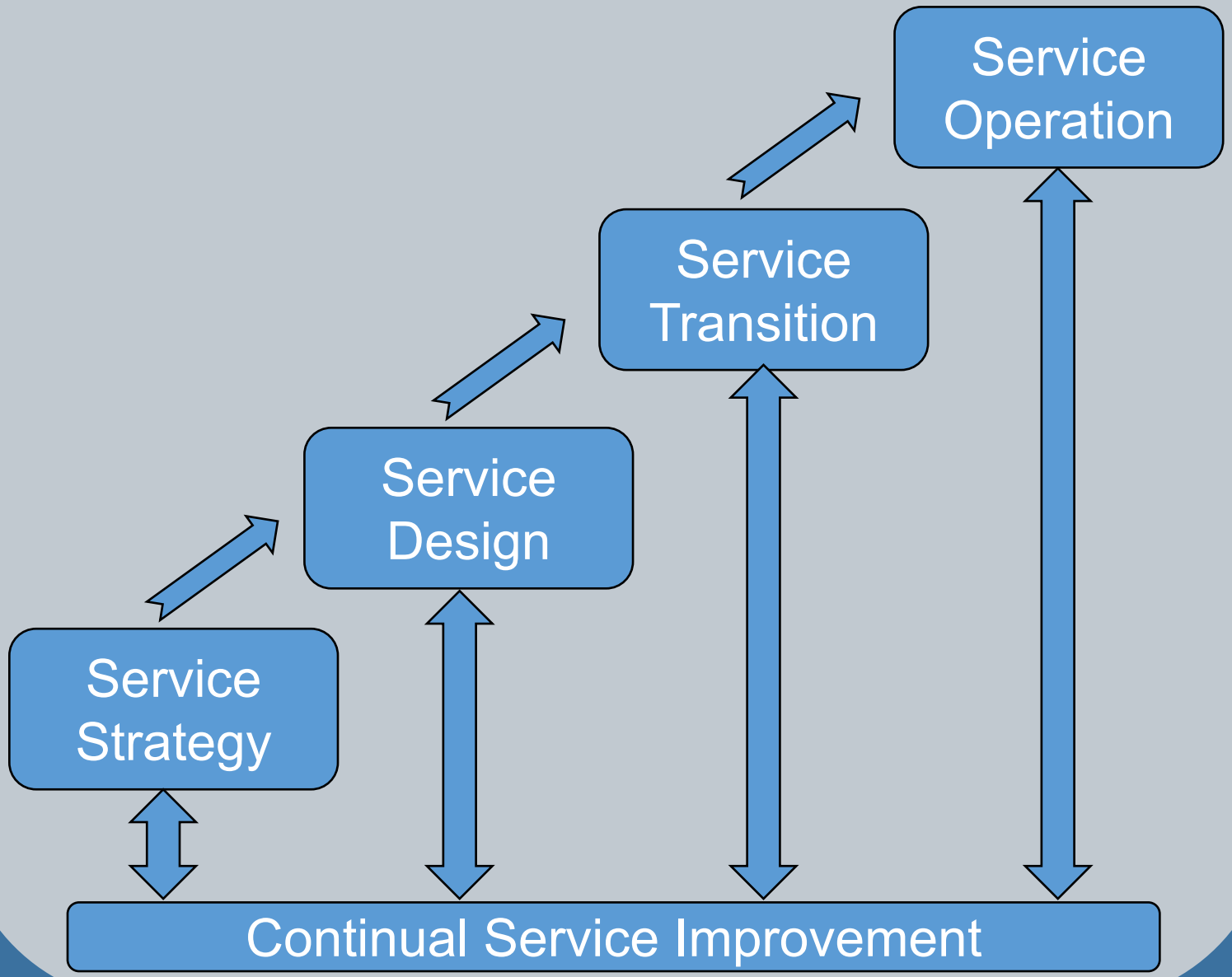


JASON DION
TRAINING THE CYBER SECURITY WORKFORCE

Service Transition (Overview)

ITIL Foundations

ITIL Lifecycle With Feedback



JASON DION
TRAINING THE CYBER SECURITY WORKFORCE

Service Transition

Stage when services are built

- Purchase
- Installation
- Configuration
- Testing
- Launch
- Operations begin

JASON DION
TRAINING THE CYBER SECURITY WORKFORCE

Coordination is Key!

Service Transition requires coordination:

- Stakeholders
- Customers
- Users
- Support Organizations

JASON DION
TRAINING THE CYBER SECURITY WORKFORCE

Testing of Service Transition

End to end testing to include

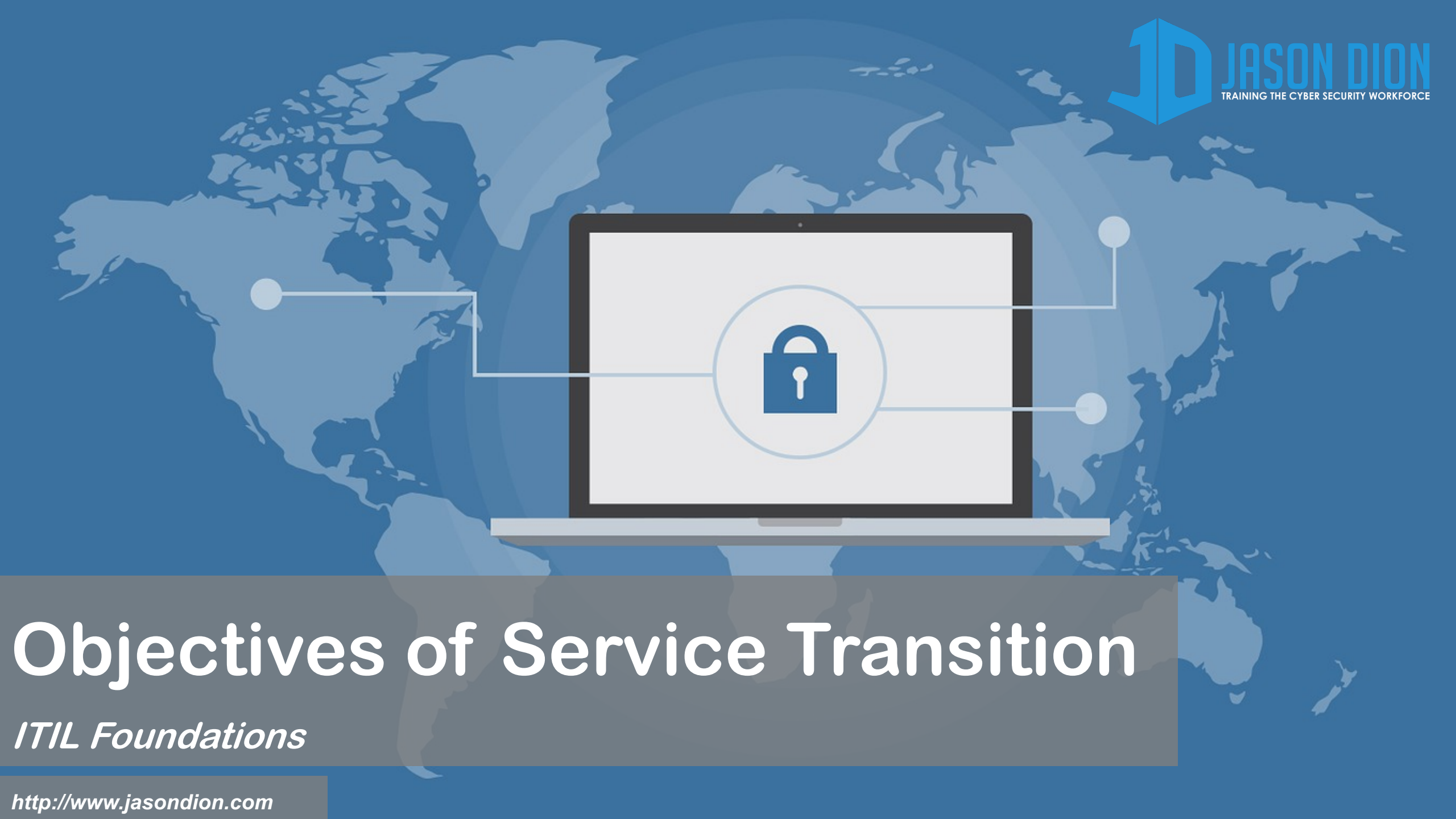
- Hardware
- Software
- Processes
- Procedures
- Support Agreements

JASON DION
TRAINING THE CYBER SECURITY WORKFORCE

Key Takeaways

- Physical development and implementation of service
- Thoroughly tested and fielded into a live environment with no shortcomings identified
- Configuration has been documented
- Operations has been trained and ready to receive the new service

JASON DION
TRAINING THE CYBER SECURITY WORKFORCE



JASON DION
TRAINING THE CYBER SECURITY WORKFORCE

Objectives of Service Transition

ITIL Foundations

Objective of Service Transition

- To plan and manage service changes while managing the risks involved in the transition

- To ensure the services meet the current and future needs of the business by creating value

JASON DION
TRAINING THE CYBER SECURITY WORKFORCE

Objectives of Service Transition

- Plan and manage service changes efficiently and effectively
- Manage risks
- Successful deploy versions into supported environments
- Expectation management
- Creation of business value
- Gain knowledge and understanding

JASON DION
TRAINING THE CYBER SECURITY WORKFORCE

Plan and manage service changes efficiently and effectively

- Utilizing the eight processes in Service Transition allows you to efficiently and effective plan, field, and manage new, changed, or retiring services

JASON DION
TRAINING THE CYBER SECURITY WORKFORCE

Manage Risks

- Change always involves some risk

- Imperative that Service Transition team understands the “uncertainty of outcome” and provide oversight, mitigations, and management to minimize those risks

JASON DION
TRAINING THE CYBER SECURITY WORKFORCE

Successful deploy versions into supported environments

- Team must ensure that extra resources, training, documentation, awareness, and understanding have been gained in order to successfully deploy new or changed services

- Should include both the operators of the service and the customers

JASON DION
TRAINING THE CYBER SECURITY WORKFORCE

Expectation Management

- Ensure that the customers are aware of the new or changed services and how the services are different
- How are they faster, slower, cheaper, better?
- Get the customer involved in pilots and acceptance testing

JASON DION
TRAINING THE CYBER SECURITY WORKFORCE

Creation of Business Value

- Services must provide business value

- Must ensure services have created the agreed-upon and documented business value before ending the Service Transition phase

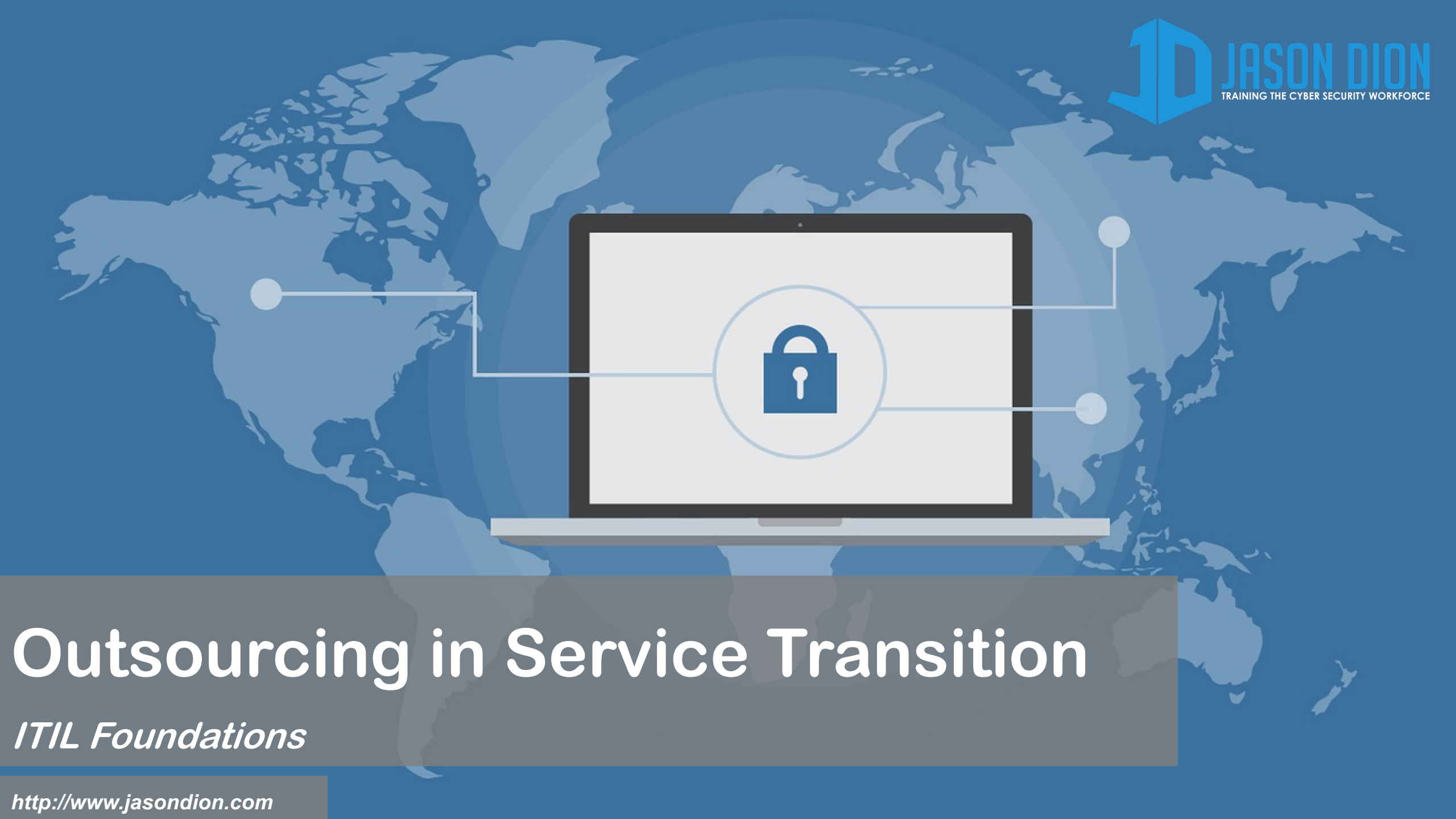
JASON DION
TRAINING THE CYBER SECURITY WORKFORCE

Gain Knowledge and Understanding

- Create an effective knowledge and information management system to ensure knowledge is gained and converted to understanding

- Tools can help with this but so must the customer and service providers

JASON DION
TRAINING THE CYBER SECURITY WORKFORCE



JASON DION
TRAINING THE CYBER SECURITY WORKFORCE

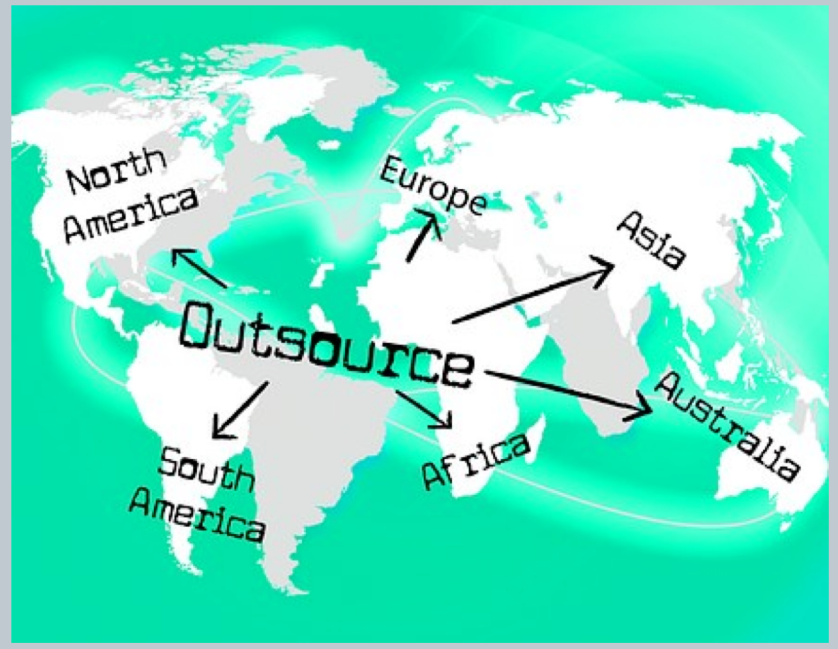
Outsourcing in Service Transition

ITIL Foundations

Outsourcing

- If you have chosen to outsource services or parts of a service, now is the time to setup the appropriate contracts

- If you do this, then have changed from being the provider to the customer



JASON DION
TRAINING THE CYBER SECURITY WORKFORCE

Outsourcing

- Outcomes are facilitated by the services without the specific detailed costs and risks

- Many ways to outsource services…

JASON DION
TRAINING THE CYBER SECURITY WORKFORCE

Traditional Outsourcing

- You transfer services from internal provisioning to an external supplier

- Example:

  Developed a website in house, but don't host it on your own architecture

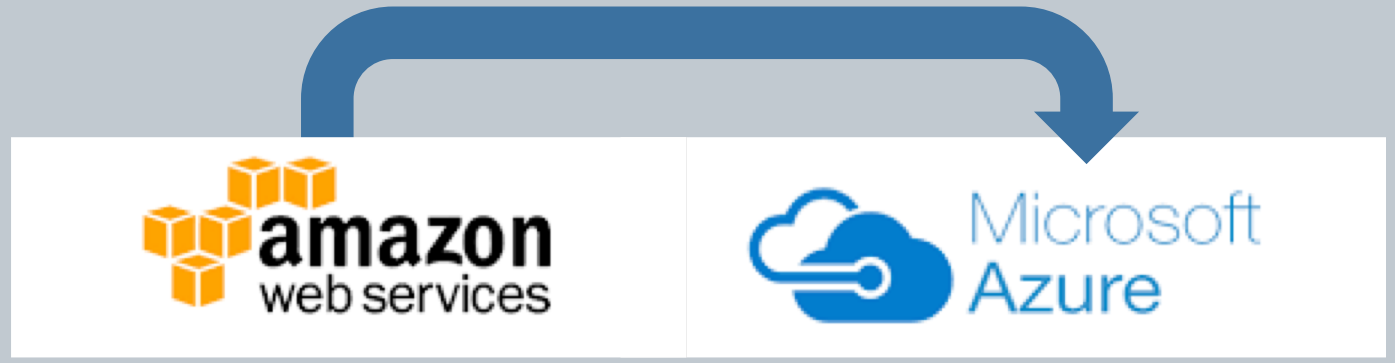
JASON DION
TRAINING THE CYBER SECURITY WORKFORCE

Changing Outsourcing

- You transfer services from one external supplier to another external supplier

- Example:

  Migrate your webserver from Amazon Web Services to Microsoft Azure



JASON DION
TRAINING THE CYBER SECURITY WORKFORCE

Re-Insourcing

- You transfer services from an external supplier to your in-house team

- Example:

  You hired a firm to build your new website, but decide to maintain it and update it yourself in the future

JASON DION
TRAINING THE CYBER SECURITY WORKFORCE

Partnership or Co-Sourcing

- You migrate to a partnership agreement where some pieces of the service are outsourced, but others remain in-house

- Example:

  You hired a firm to build your new website, but decide to host it on your own servers while they continue to maintain and update it

JASON DION
TRAINING THE CYBER SECURITY WORKFORCE

Co-Sourcing/Multi-sourcing

- Utilize multiple suppliers

- Note:

  Increases service level management and supplier management challenges

- Example:

  You hired a firm to build your new website, but decide to host it on a different firm's web servers

JASON DION
TRAINING THE CYBER SECURITY WORKFORCE

JASON DION
TRAINING THE CYBER SECURITY WORKFORCE

Transition Planning & Support

ITIL Foundations

Purpose

- Provide overall planning for the Service Transition stage and coordinate the required resources

- Planning occurs for all related projects and programs during this stage

JASON DION
TRAINING THE CYBER SECURITY WORKFORCE

Functions

- Plan and coordinate resources to ensure multiple concurrent transitions can occur seamlessly
- Lead major changes through the transition stage
- Migrate new or changed services to Service Operations within the agreed-upon time, cost, and quality

JASON DION
TRAINING THE CYBER SECURITY WORKFORCE

Functions

- Establish new or improved management systems and tools, technology and management architectures, processes, measurement methods, and metrics
  - 5 pieces of holistic Service Design
- Provide comprehensive transition plans to align business changes and the service transition

JASON DION
TRAINING THE CYBER SECURITY WORKFORCE

Functions

- Identify, manage, and control risks across the other seven (7) Service Transition processes

- Continually monitor and improve the Service Transition stage performance

7

JASON DION
TRAINING THE CYBER SECURITY WORKFORCE

Who Does The Planning?

- It's important to note that the Transition Planning and Support process doesn't do the planning itself

- It only ensures that planning is carried out per the service provider's policies

JASON DION
TRAINING THE CYBER SECURITY WORKFORCE

JASON DION
TRAINING THE CYBER SECURITY WORKFORCE

Knowledge Management

ITIL Foundations

http://www.jasondion.com

Purpose

- To share perspectives, ideas, experiences, and information
- To ensure these are available at the right time to make correct decisions
- To improve efficiency by reducing the need to rediscover knowledge

JASON DION
TRAINING THE CYBER SECURITY WORKFORCE

Functions

- Ensure that reliable and secure data, information, and knowledge are available to decision makers in order to improve quality and drive down cost

- Ensure service management data, information, and knowledge are collected, analyzed, stored, used, shared, and maintained

JASON DION
TRAINING THE CYBER SECURITY WORKFORCE

Functions

- Create and maintain an information management system to securely store data, information, and knowledge
  - Service Knowledge Management System (SKMS)

JASON DION
TRAINING THE CYBER SECURITY WORKFORCE

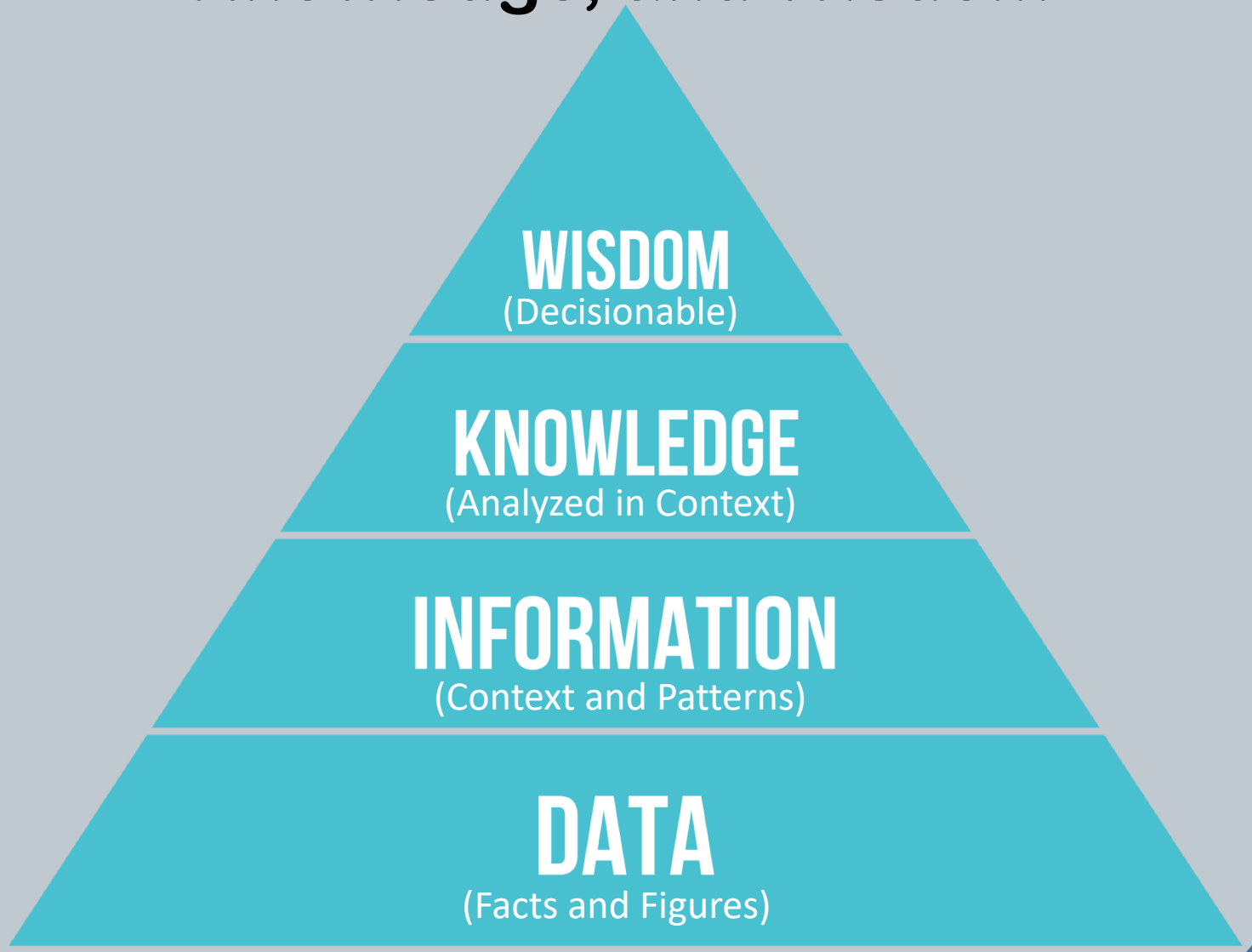
KM's Place in the Lifecycle

- KM really must occur in all stages of the ITIL lifecycle

- Your KM program is only as good as your ability to get people to use it…

JASON DION
TRAINING THE CYBER SECURITY WORKFORCE

Data, Information, Knowledge, and Wisdom



JASON DION
TRAINING THE CYBER SECURITY WORKFORCE

Service Knowledge Management System (SKMS)

- Data comes from many sources (config DBs, service management tools, and even open-sources)
- Contains all the data in a collection of repositories and systems
- Houses the Configuration Management System and in turn contains the Configuration Management Databases

JASON DION
TRAINING THE CYBER SECURITY WORKFORCE

Service Knowledge Management System (SKMS)

JASON DION
TRAINING THE CYBER SECURITY WORKFORCE

Service Knowledge Management System (SKMS)

Contains CMS, service portfolios, service level agreements, capacity plan, user skill levels, technical documentation, and more

Configuration Management System (CMS)

Contains CMDBs and the tools used to manage themselves, the CMDBs, and the knowledge derived from these different tools

Configuration Management Database (CMDB)

Contains configuration item records for incidents, service requests, problems, known errors, changes, released, and more

JASON DION
TRAINING THE CYBER SECURITY WORKFORCE

Service Asset and Configuration Management

ITIL Foundations

Purpose

- Ensures assets needed to deliver services are managed and accurate/reliable information is available for those assets

- *Service Asset and Configuration Management (SACM) is vital to knowledge management*

JASON DION
TRAINING THE CYBER SECURITY WORKFORCE

SACM Considerations

- Don’t start SACM until change control and change management are in place
- Relationships between configuration items is what makes the SACM powerful instead of a simple asset list
- Identify, control, record, report, audit, and verify services and configuration items (CIs) including their relationships to each other

JASON DION
TRAINING THE CYBER SECURITY WORKFORCE

Functions

- Accurate information on configuration items is essential
- Historical information on configuration items is necessary
- SACM ensures only authorized components are utilized in architecture

JASON DION
TRAINING THE CYBER SECURITY WORKFORCE

Functions

- SACM ensures only authorized changes occur in the architecture
- SACM supports other processes in all stages of the lifecycle
- SACM may seem boring but it is crucial to your organizational success across various other processes

JASON DION
TRAINING THE CYBER SECURITY WORKFORCE

SACM Definitions

- Configuration items
- Categories
- Levels
- Naming
- Labels
- Attributes
- Configurations
- Baselines
- Configuration Management System
- Definitive Media Library (DML)

JASON DION
TRAINING THE CYBER SECURITY WORKFORCE

JASON DION
TRAINING THE CYBER SECURITY WORKFORCE

SACM Definitions and Concepts

ITIL Foundations

SACM Definitions

- Configuration items
- Categories
- Levels
- Naming
- Labels
- Attributes
- Configurations
- Baselines
- Configuration Management System
- Definitive Media Library (DML)

JASON DION
TRAINING THE CYBER SECURITY WORKFORCE

Configuration Items (CIs)

- CIs are the individual records in your Configuration Management Database (CMDB)

- CIs are components or service assets that need to be identified and managed

JASON DION
TRAINING THE CYBER SECURITY WORKFORCE

Categories

- Hardware
  - Workstations, servers, switches, …
- Software
  - OS, productivity, in-house built, …
- People
  - Users, customers, technical staff, …
- Documentation
  - End user, admin guides, plans, …
- Physical locations
  - Server rooms, buildings, …

JASON DION
TRAINING THE CYBER SECURITY WORKFORCE

Levels

- How detailed does your CIs need to be to support your service needs?
- Do you need to know every CPU in every workstation or just how many workstations?
- Depends on your organizations role and any outsourcing being conducted

JASON DION
TRAINING THE CYBER SECURITY WORKFORCE

Naming

- Utilize a uniform naming convention
- Do we call all mobile devices one thing, or break them into Laptops, Tablets, Smartphones, and PDAs?
- Do we break them down based on their Operating Systems (Android, iOS, Windows)?

JASON DION
TRAINING THE CYBER SECURITY WORKFORCE

Labels

- How are you going to label assets?
- Workstations are easy
  - Use a barcoding system

- People and electronic software are harder
  - Unique employee identifier
  - Electronic tracking of software by virtual asset tags

JASON DION
TRAINING THE CYBER SECURITY WORKFORCE

Attributes

- What information do you want to know about the Configuration Item (CI)?
- Universal attributes:
  - Description, Unique ID, Location
- Other attributes can be customized based on the type of asset
- CMDBs are relational databases
  - Don’t repeat information multiple times, instead just link to it

JASON DION
TRAINING THE CYBER SECURITY WORKFORCE

Configurations

- Group of CIs to makeup a specific build or architecture
- Created by linking several CIs in a relationship
- KM system may be one configuration which is made up of numerous assets (servers, software, people) from various CIs

JASON DION
TRAINING THE CYBER SECURITY WORKFORCE

Baselines

- Snapshot of a particular configuration at a moment in time
- Starting point when equipment arrives
- Must document any changes from the baseline to account for the difference between the design and operation
- Most common baselines used are for workstations and servers

JASON DION
TRAINING THE CYBER SECURITY WORKFORCE

Configuration Management System

- Essential set of tools, data, and information on configurations
- Part of the Service Knowledge Management System (SKMS) and each SKMS can only have one CMS
- Includes information on incidents, service requests, changes, problems, releases, errors, and more

JASON DION
TRAINING THE CYBER SECURITY WORKFORCE

Definitive Media Library (DML)

- Secure storage area for authorized software versions for every CI
- Includes the licensing information and documentation
- Everything must be quality checked before being put into the DML
- *We will cover this more in the Release and Deployment Management lesson*

JASON DION
TRAINING THE CYBER SECURITY WORKFORCE

JASON DION
TRAINING THE CYBER SECURITY WORKFORCE

SACM's 5 Principles

ITIL Foundations

Five Principles of SACM

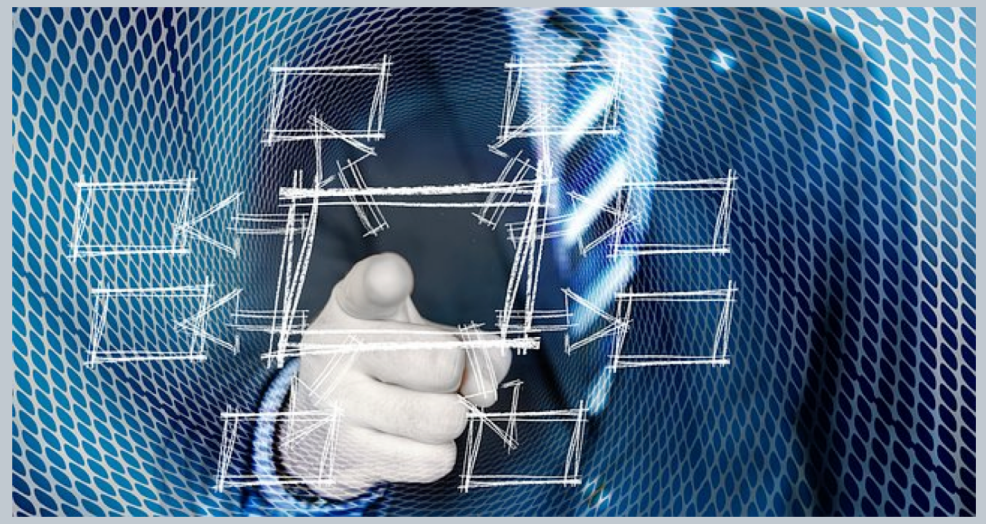
- Planning and Management
- Identification
- Control
- Status Accounting
- Verification and Audit

JASON DION
TRAINING THE CYBER SECURITY WORKFORCE

Planning and Management

- First major activity is planning

- Must plan to introduce/develop SACM, including resources required, size of CI types, CI levels, and the management tools needed



JASON DION
TRAINING THE CYBER SECURITY WORKFORCE

Identification

- Designate the CI types
- Agree on naming conventions
- Decide on unique identifiers for assets
- Choose proper CI attributes

JASON DION
TRAINING THE CYBER SECURITY WORKFORCE

Control

- Integrate SACM into the processes that produce changes to keep CI information up to date:
  - Change Management
  - Release and Deployment Management
  - Incident Management

JASON DION
TRAINING THE CYBER SECURITY WORKFORCE

Status Accounting

- Status of a CI changes over time

- Create standard status codes (Example for computers):
  - Ordered
  - Received
  - Configured
  - Installed
  - Repaired
  - Retired
  - Disposed

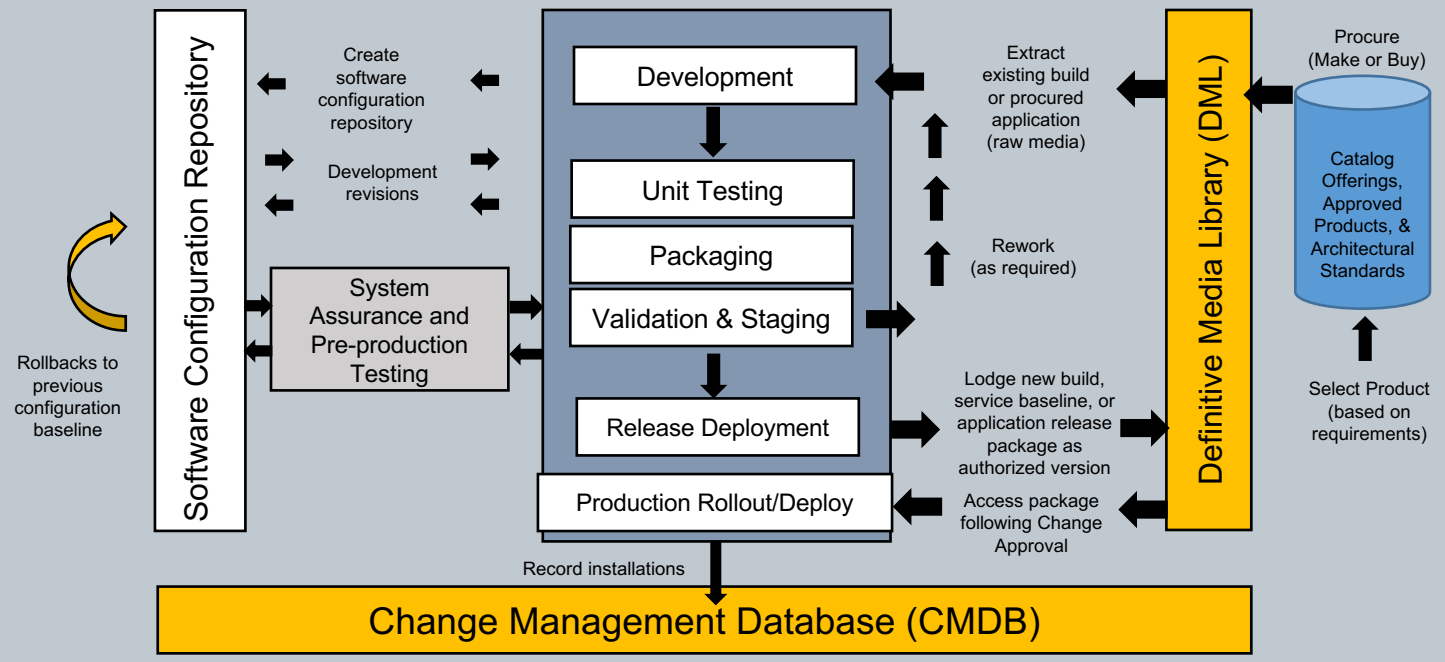
JASON DION
TRAINING THE CYBER SECURITY WORKFORCE

Verification and Audit

- Verify and audit SACM to determine if it is effective
- Are users and employees using it?
- Is it up to date?
- Don’t try to do 100% validation
- Spot check it periodically and investigate when a problem is found

JASON DION
TRAINING THE CYBER SECURITY WORKFORCE

Relationships in the Processes



Service Asset and Configuration Management,
Change Management, and
Release and Deployment Management
all work together!

JASON DION
TRAINING THE CYBER SECURITY WORKFORCE

Change Management

ITIL Foundations

http://www.jasondion.com

What is Change?

- Addition, modification, or removal of anything that could have an effect on IT services

JASON DION
TRAINING THE CYBER SECURITY WORKFORCE

Purpose

- To control the lifecycle of all changes, enabling beneficial changes to be made with a minimal disruption of IT services

JASON DION
TRAINING THE CYBER SECURITY WORKFORCE

Purpose

- To ***control*** the lifecycle of all changes, enabling beneficial changes to be made with a minimal disruption of IT services

- *Have a clear change policy and roles/responsibilities to allow for the control of change*

- *Not just administration of change*

JASON DION
TRAINING THE CYBER SECURITY WORKFORCE

Purpose

- To control the ***lifecycle*** of all changes, enabling beneficial changes to be made with a minimal disruption of IT services

- *Changes have their own lifecycle*

- *Some are short and quick*

- *Others take months or years to finish*

Purpose

- To control the lifecycle of all changes, enabling ***beneficial changes*** to be made with a minimal disruption of IT services

- *Don't want to change for change sake*

- *Need a beneficial reason to change*
  - *Compliance*
  - *Make more money*
  - *Drive down costs*

JASON DION
TRAINING THE CYBER SECURITY WORKFORCE

Purpose

- To control the lifecycle of all changes, enabling beneficial changes to be made with a ***minimal disruption*** of IT services

- *Changes cause disruption*

- *Change management focuses on creating the minimal impact to the service*

JASON DION
TRAINING THE CYBER SECURITY WORKFORCE

Functions

- Respond to change initiating triggers
  - New business requirements
  - Operational failures
  - Improvements and additions

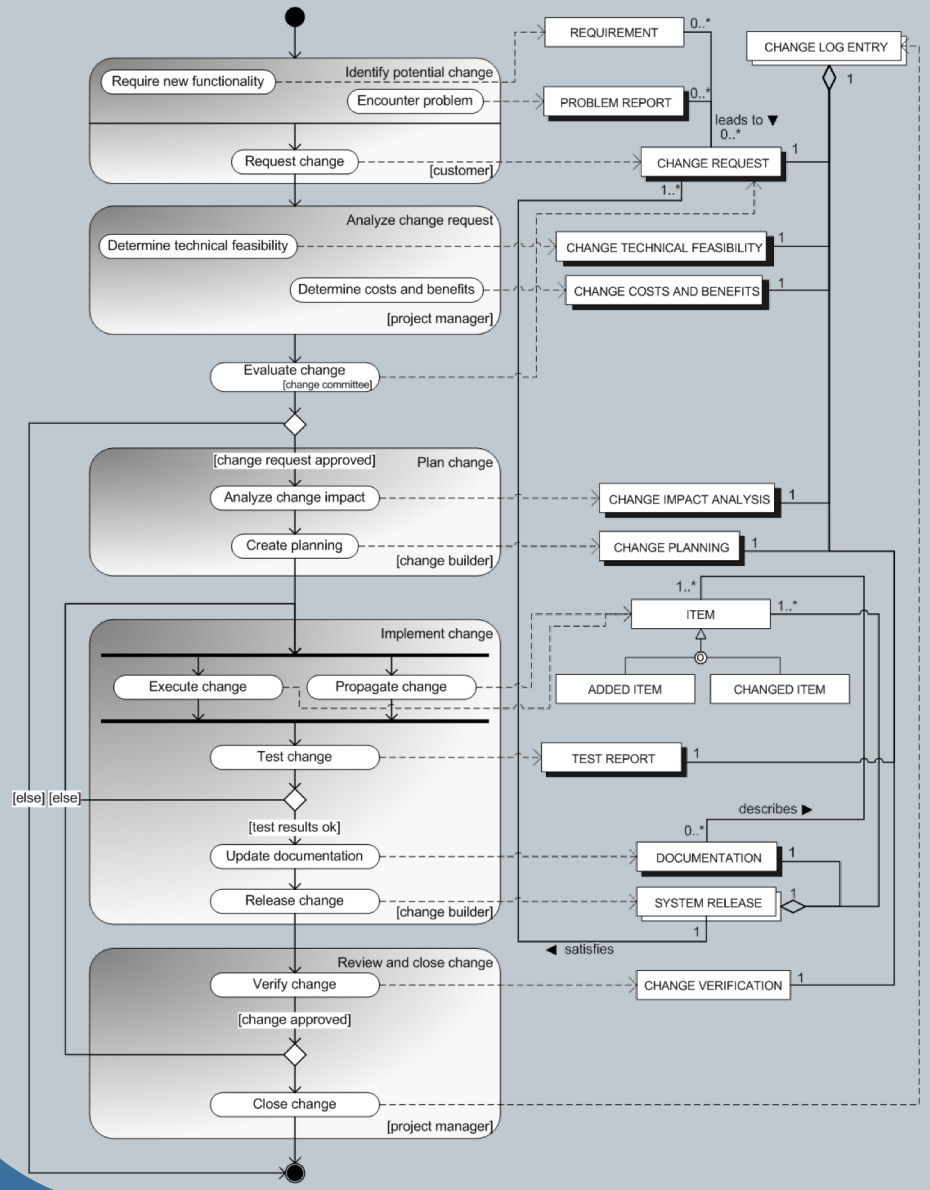
- Record, evaluate, authorize/reject, prioritize, plan, test, implement, document, and review changes

When Does Change Occur?

- Changes happen at every stage
- Changes happen to the Service Portfolio, Service Catalog, Service Level Agreements, and processes
- Change management needs to be involved with all of these processes

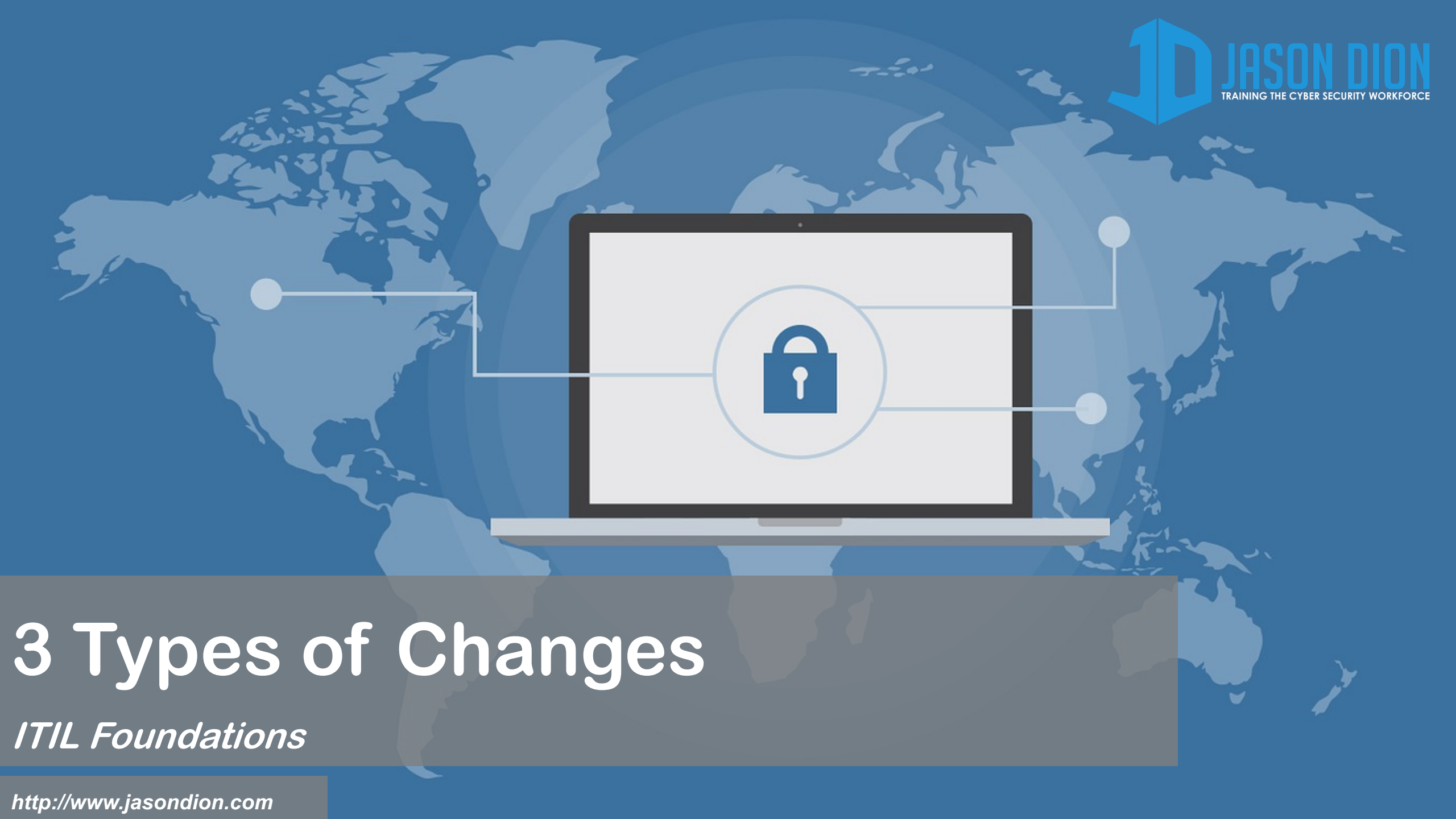
JASON DION
TRAINING THE CYBER SECURITY WORKFORCE

Change Management Process



Change is Updated/ Recorded in CMS

JASON DION
TRAINING THE CYBER SECURITY WORKFORCE



JASON DION
TRAINING THE CYBER SECURITY WORKFORCE

3 Types of Changes

ITIL Foundations

Three Types of Changes

- Emergency changes
- Normal changes
- Standard changes

JASON DION
TRAINING THE CYBER SECURITY WORKFORCE

Emergency Changes

- Address unforeseen operational issues, such as failures, security threats, and vulnerabilities
- Rapid change is required to continue the business operations
- Emergency changes should still follow the documented procedures, but they just happen much quicker

JASON DION
TRAINING THE CYBER SECURITY WORKFORCE

Emergency Change Procedures

- Clearly define who can declare an emergency change
- Emergency Change Advisory Board (ECAB) can be called in after hours for decisions
- Testing may be modified or removed
- RFC and documentation are often done after the issue is resolved

JASON DION
TRAINING THE CYBER SECURITY WORKFORCE

Normal Changes

- Change that has a uniqueness to them that represents a higher risk or uncertainty of outcome
- Default type of change that occurs
- Emergency and Standard are variations on Normal Change procedures
- Example:
  - Adding a new server or service

JASON DION
TRAINING THE CYBER SECURITY WORKFORCE

Standard Changes

- Typical day-to-day changes that are low-risk and well understood
- Utilizes a shorter version of the Normal Change procedures
- Minimizes bureaucracy and quickly satisfies customer needs
- Example:
  - Moving a workstation to another office

JASON DION
TRAINING THE CYBER SECURITY WORKFORCE

Standard Change Procedures

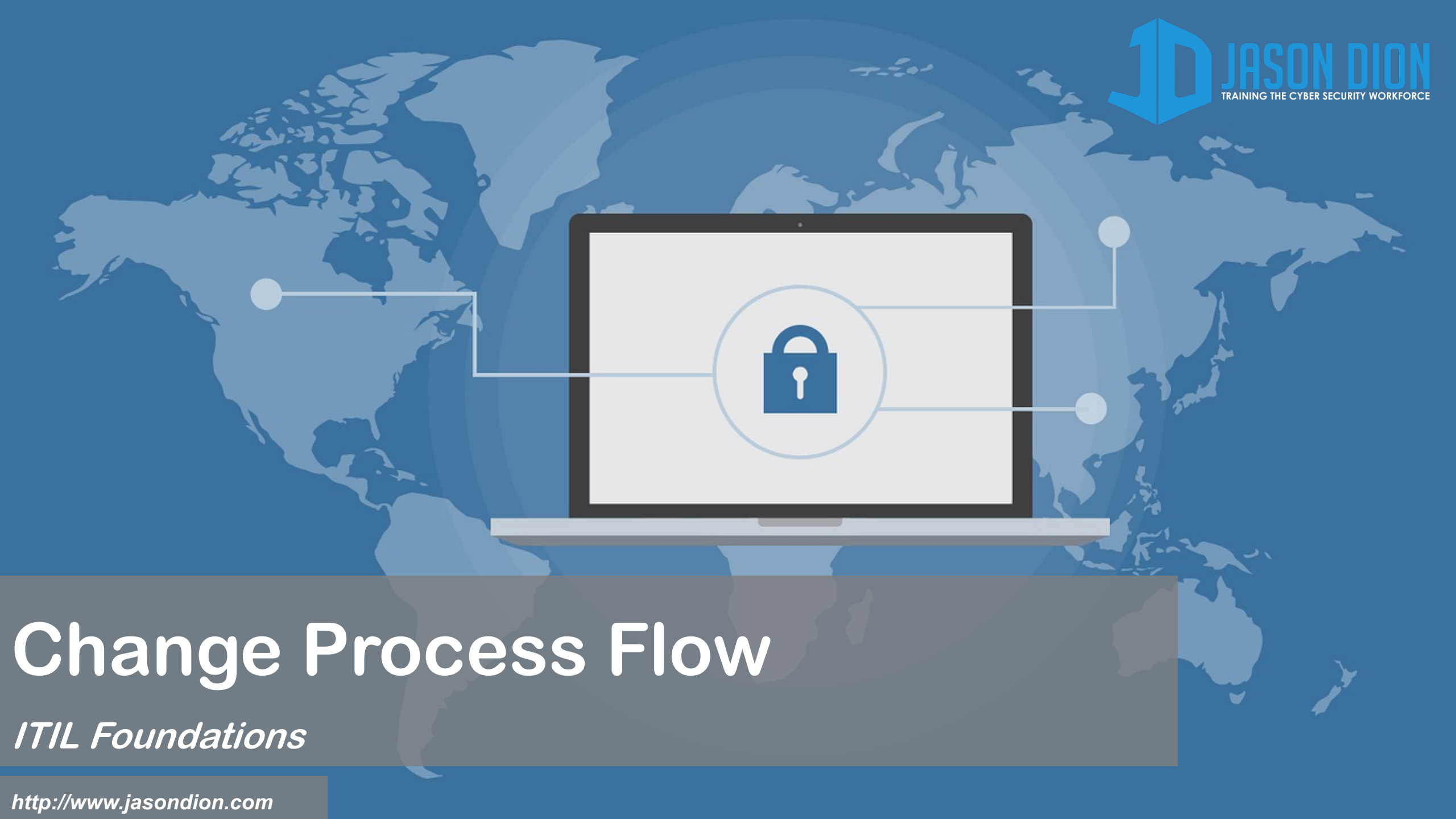
- Generally follow a predefined workflow controlled by automation
- Usually an automated system checks initiator has permission to start the process and technicians just work the change ticket to resolution
- Don’t need CAB approval since it is approved as part of normal service management (request fulfillment)

JASON DION
TRAINING THE CYBER SECURITY WORKFORCE

Why Do Changes Fail?

- Wider impact than originally thought
- Insufficient resources (time, money)
- Stakeholder disagreements on who can authorize the change
- Poorly planned or conducted testing
- Users were not ready for change
- Support organizations were not ready
- Change rolled out prematurely due to management pressures
- Two incompatible changes at once

JASON DION
TRAINING THE CYBER SECURITY WORKFORCE



JASON DION
TRAINING THE CYBER SECURITY WORKFORCE

Change Process Flow

ITIL Foundations

Change Management is a Process

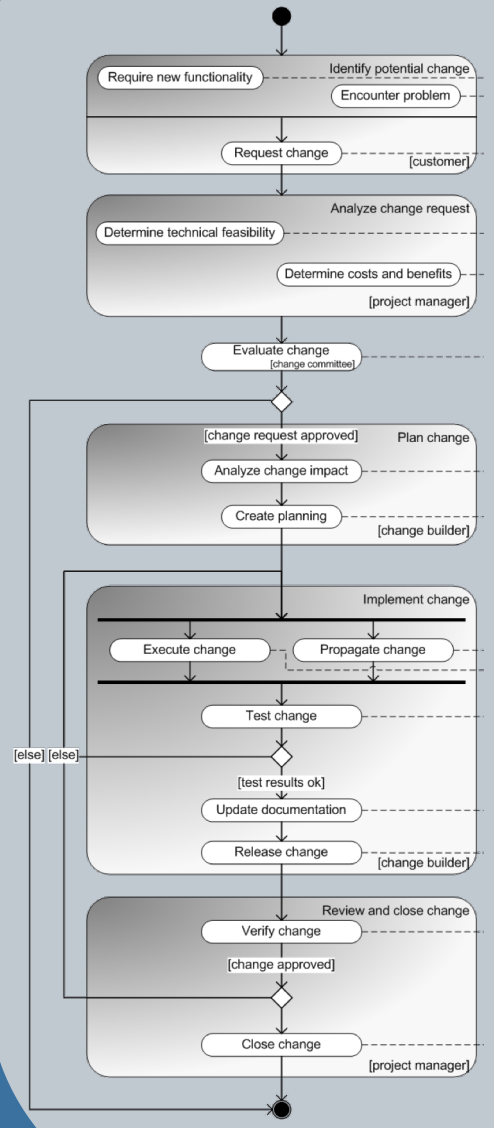
- A process is a set of coordinated activities combining resources and capabilities to produce an outcome that creates value for the customer

- Processes respond to a trigger, are measurable, produce specific results, and deliver the results to a defined customer

Review of a Process from Earlier Lessons

JASON DION
TRAINING THE CYBER SECURITY WORKFORCE

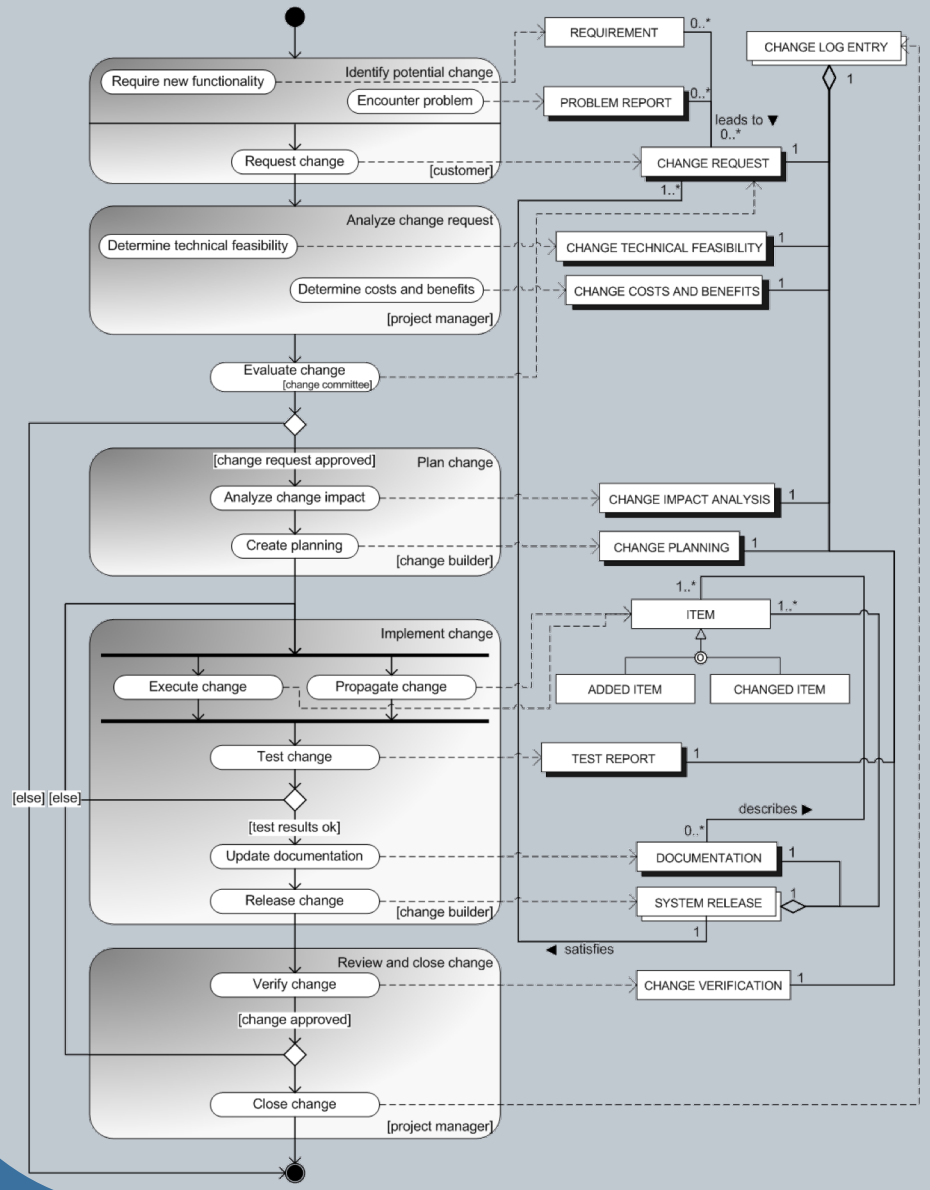
Change Process Flow



- Initiation
- Initial Review
- Raise RFC
- Assess and Evaluate
- Authorization to Proceed
- Build and Test
- Authorization to Implement
- Implementation
- Remediation
- Review
- Closure

JASON DION
TRAINING THE CYBER SECURITY WORKFORCE

Change Process Flow

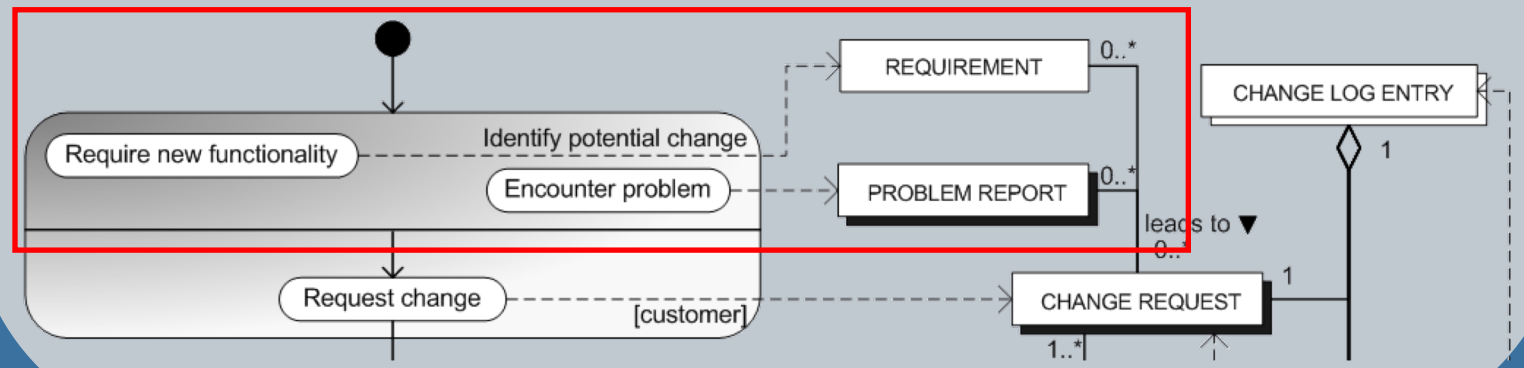


Change is Updated/ Recorded in CMS

JASON DION
TRAINING THE CYBER SECURITY WORKFORCE

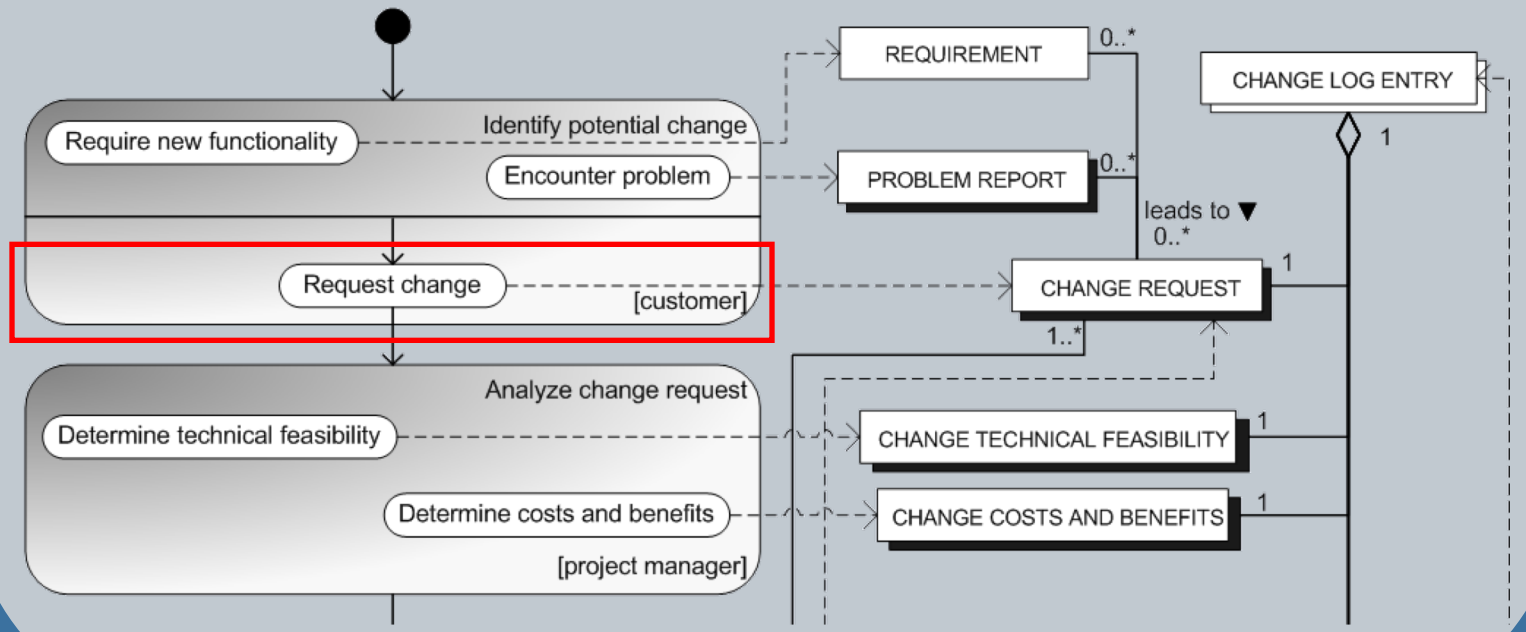
Initiation

- Change is initiated by a trigger:
  - Service request, continual service improvement, program/project, new legal/compliance requirements, better technology, service failures, etc.
- Change priority must be determined
  - Transition Planning and Support does it



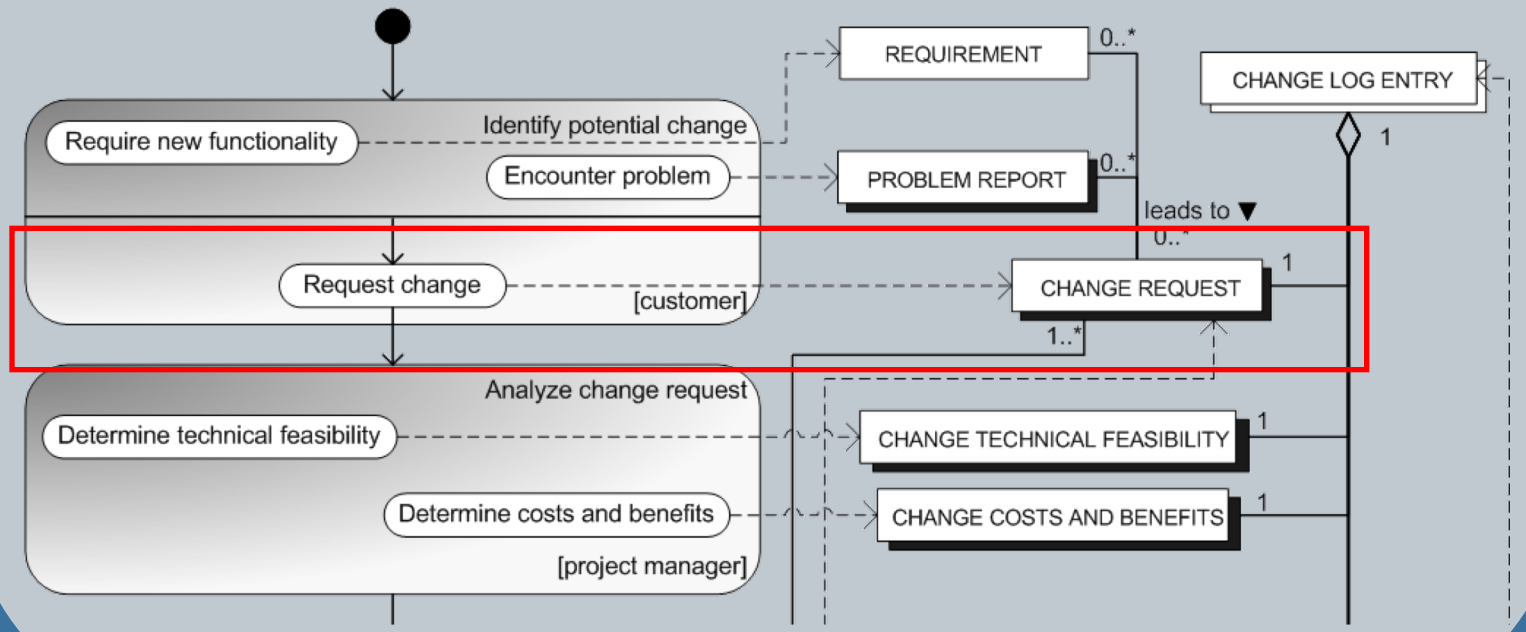
Initial Review

- Determine if proposed change is realistic and check the priority
- Record this step into CMS



Raise RFC

- Formal Change Request or “Move, Add, Change” in some organizations
- ITIL uses Request for Change (RFC)



JASON DION
TRAINING THE CYBER SECURITY WORKFORCE

The Seven (7) R's of RFCs

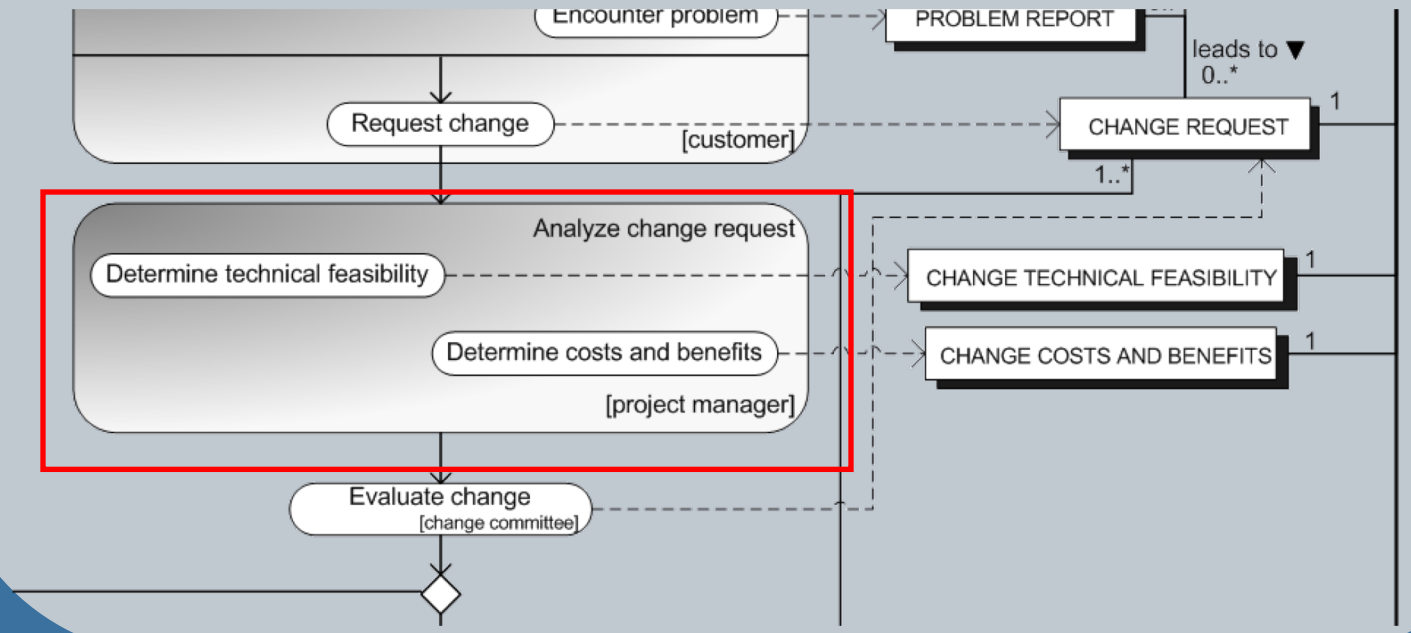
Raised	Who request the change?
Reason	Why is it needed?
Return	What benefits do we get?
Risks	What are the uncertainties?
Resources	What does it cost?
Responsible	Who's owner/sponsor?
Relationship	Any with other changes we can leverage or deconflict?

Answered by owner/sponsor, not CM

JASON DION
TRAINING THE CYBER SECURITY WORKFORCE

Assess and Evaluate

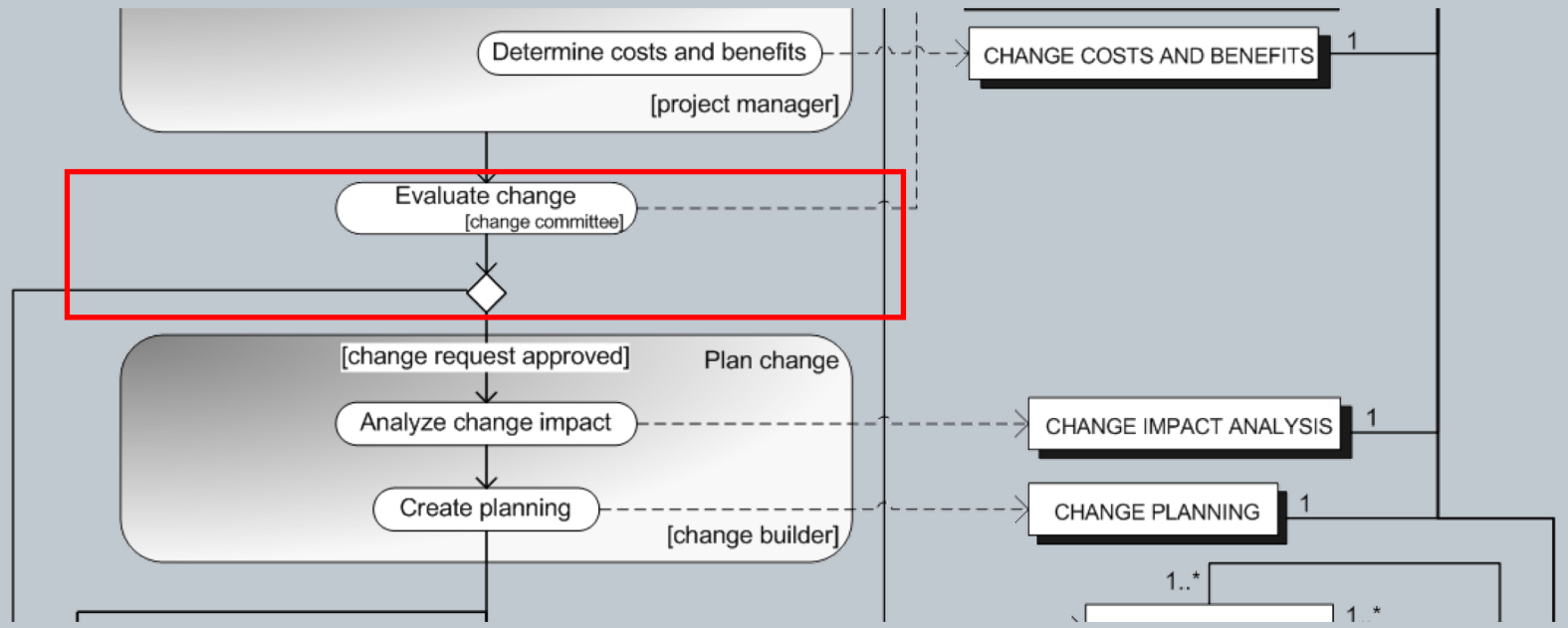
- Analyze change and get recommendations from stakeholders
- If your service is being changed, you get a veto!



JASON DION
TRAINING THE CYBER SECURITY WORKFORCE

Authorization to Proceed

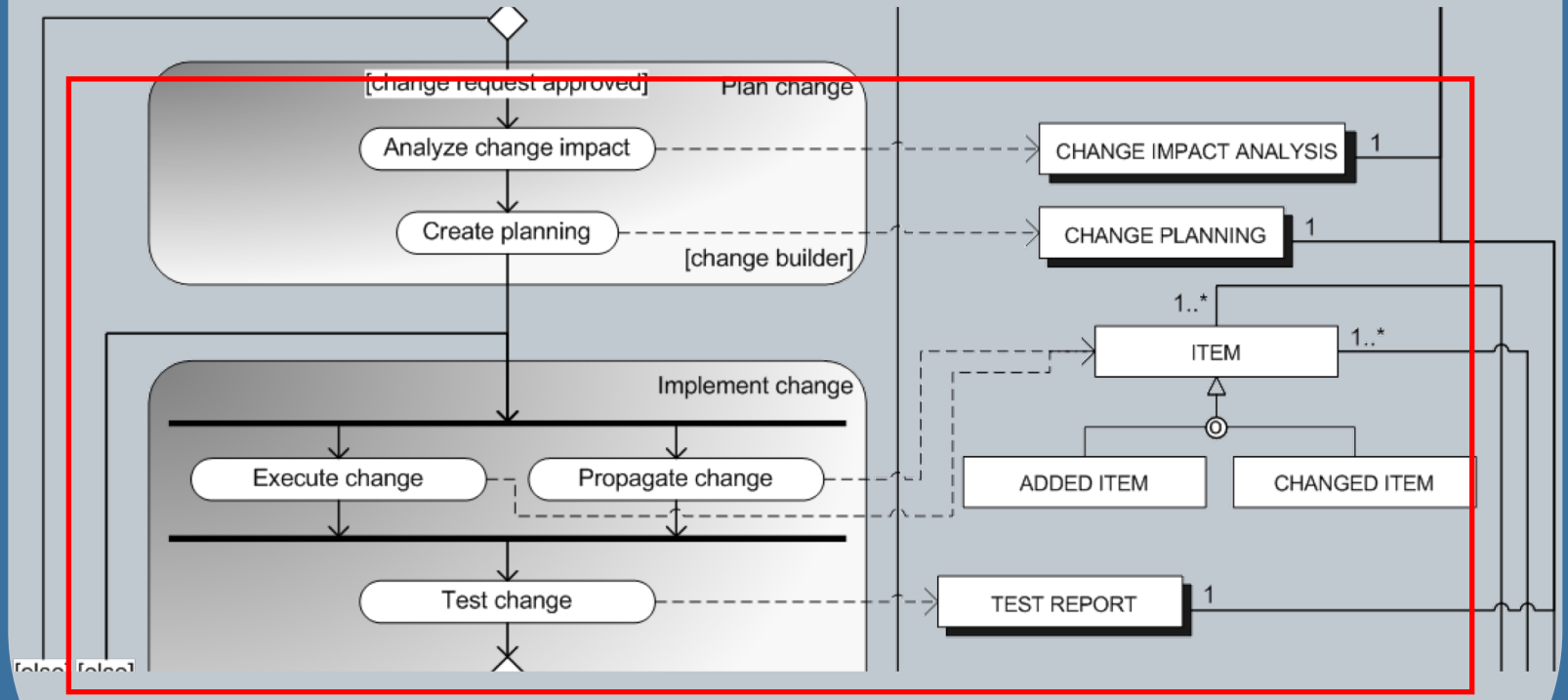
- Results of evaluation are presented to the Change Advisory Board (CAB) for approval or rejection of the change



JASON DION
TRAINING THE CYBER SECURITY WORKFORCE

Build and Test

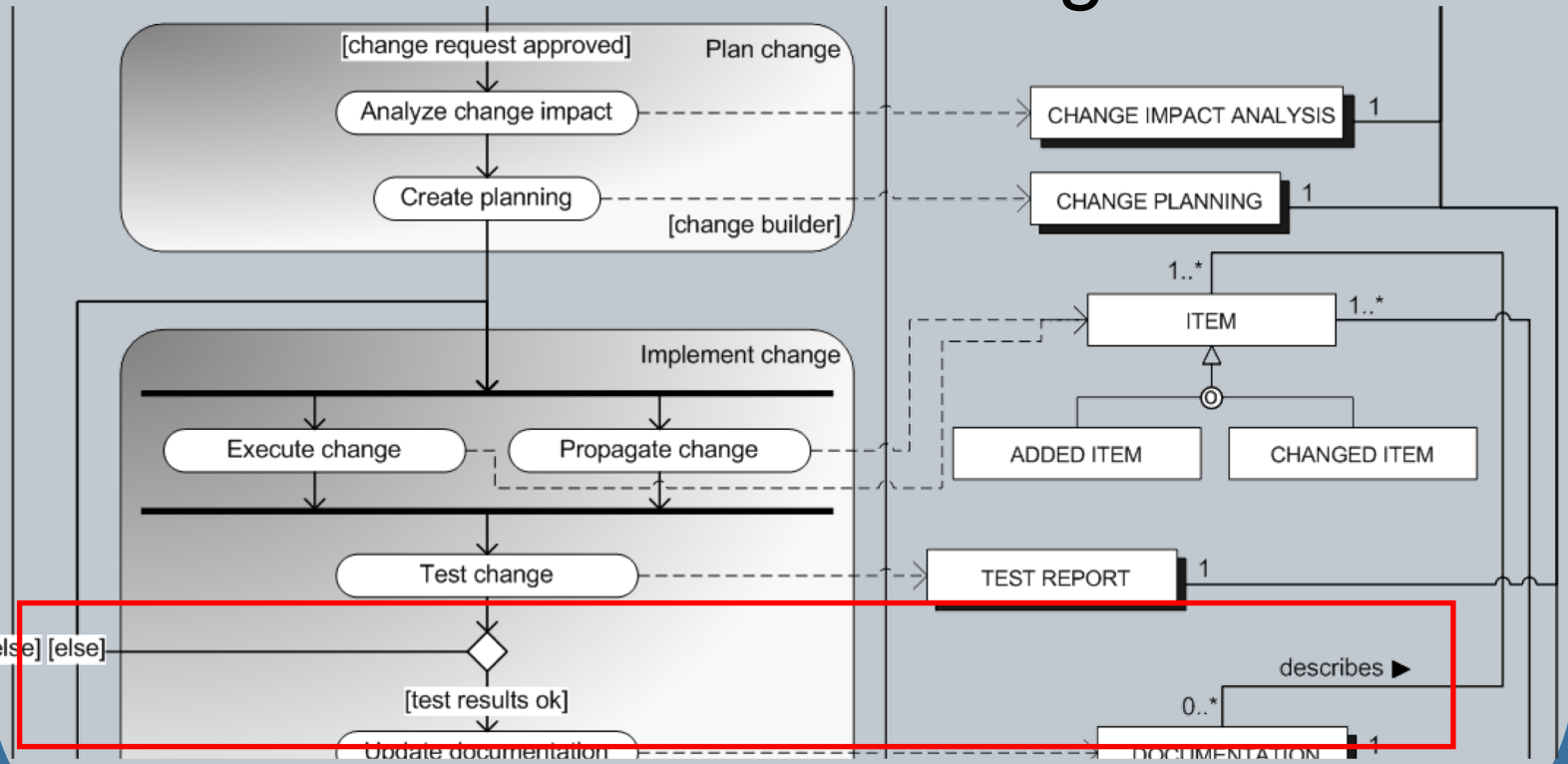
- Owner/Sponsor builds the service, then Service Validation and Testing will test it (CM only tracks progress)



JASON DION
TRAINING THE CYBER SECURITY WORKFORCE

Authorization to Implement

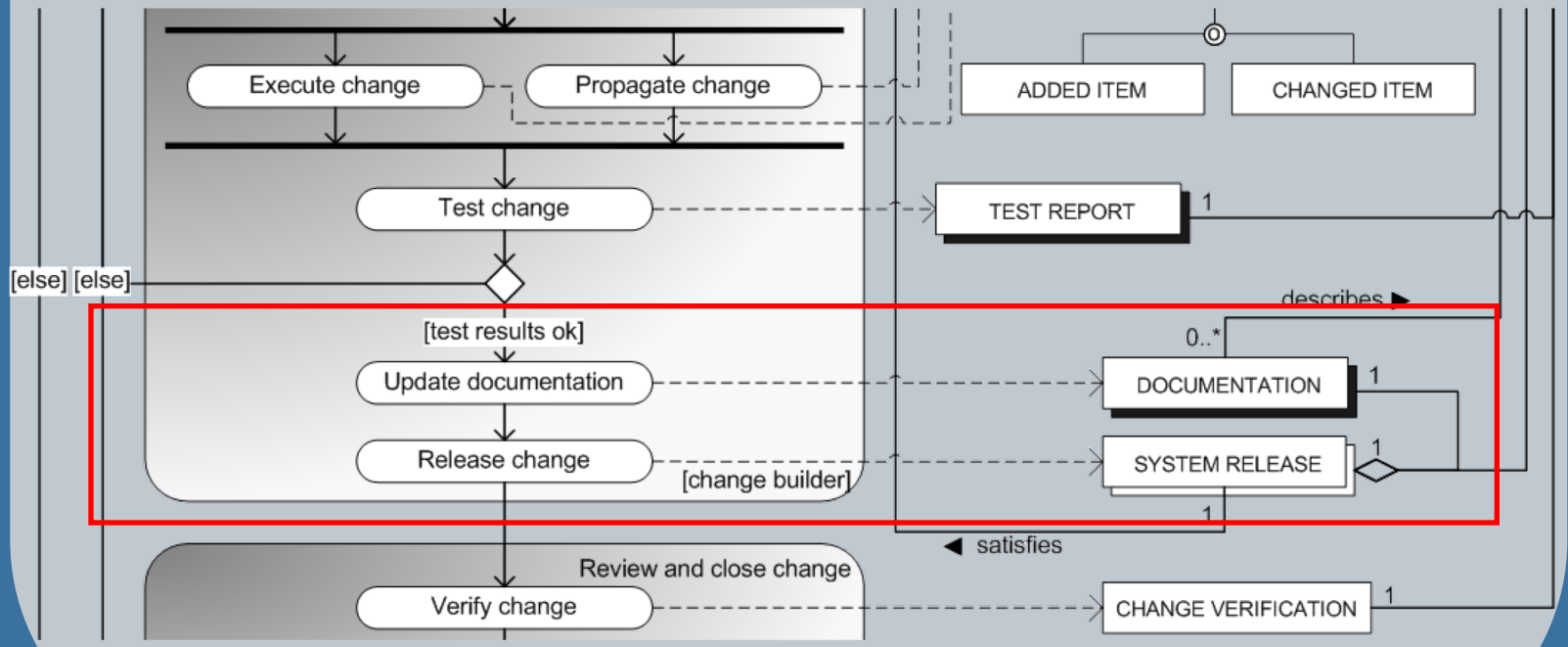
- Initial test results are presented to the CAB then approval to implement can be obtained and scheduling occurs



JASON DION
TRAINING THE CYBER SECURITY WORKFORCE

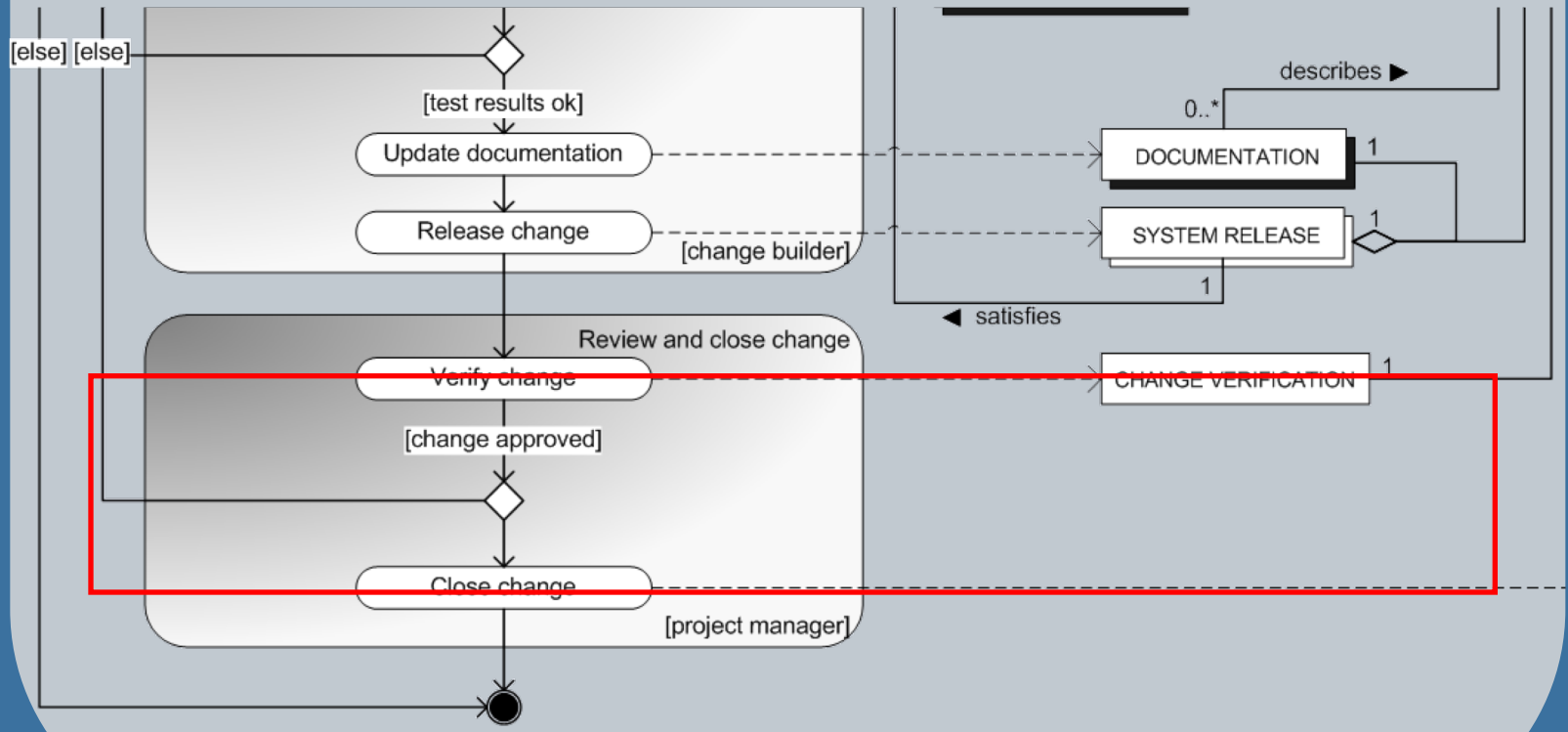
Implementation

- Release and Deployment are brought in to implement the change into the production environment



Remediation

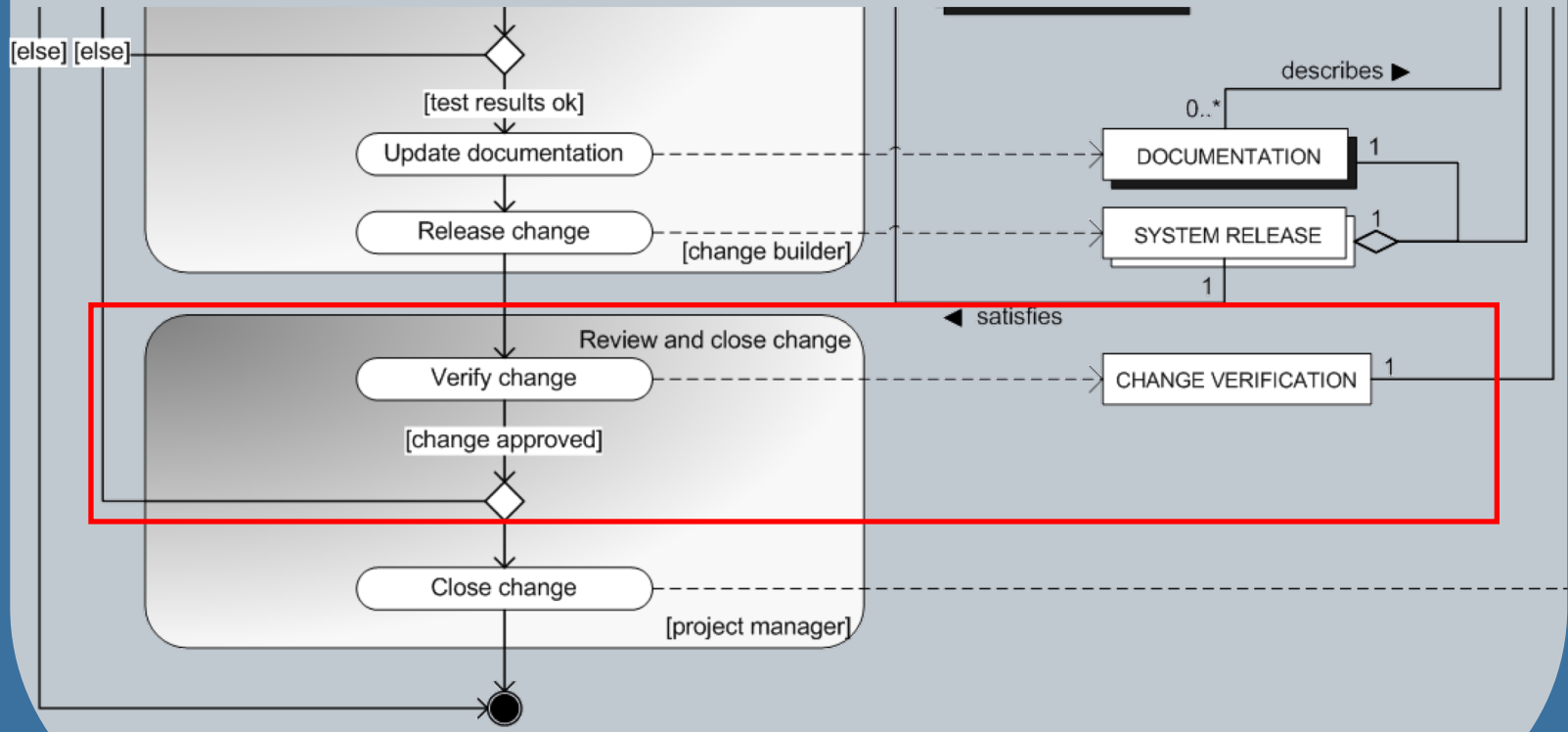
- Back out plan if the change release doesn't work properly or a point of no return identified



JASON DION
TRAINING THE CYBER SECURITY WORKFORCE

Review

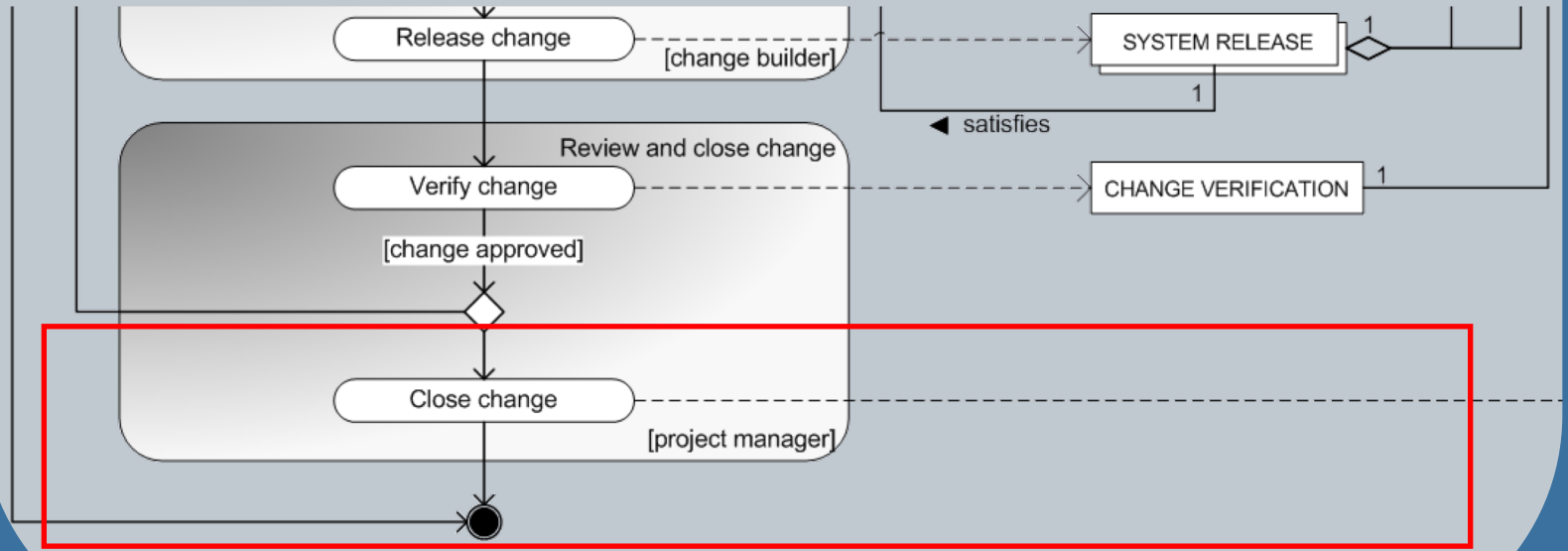
- If implementation is considered successful then review occurs based upon accepted timeline after change



Closure

- Results of review are recorded in change record, lessons learned identified, and change pushed to CSI

- Authority for closure is the CAB



JASON DION
TRAINING THE CYBER SECURITY WORKFORCE

Change Advisory Board (CAB)

ITIL Foundations

Change Advisory Board (CAB)

- Focused on providing a go/no-go decision for all changes
- Meet on a regular basis (i.e. weekly)
- In large organizations there may be many smaller CABs, but one is always the final decision maker

JASON DION
TRAINING THE CYBER SECURITY WORKFORCE

CAB Members

- Change Manager (Chairman)
- Service Desk Manager
- Capacity Manager
- IT Security Manager

…other members as appropriate

JASON DION
TRAINING THE CYBER SECURITY WORKFORCE

CAB Meeting Inputs

- Minutes of previous CAB meeting
- Any Emergency CAB activity
- New changes for decision
- Changes ready for implementation
- Change reviews completed since last meeting
- Any improvement initiatives

JASON DION
TRAINING THE CYBER SECURITY WORKFORCE

CAB Meeting Outputs

- Minutes of this CAB meeting
- Authorized new changes
- Rejected changes

- Updated change schedule
- Update PSO (Project Service Outage)

JASON DION
TRAINING THE CYBER SECURITY WORKFORCE

CAB Chairman's Role

- Protector and enforcer of the standards and processes to ensure positive change
- Ensures all change authorities have approved the changes before he does
- Ensures good governance
- Provides final approval on RFC

JASON DION
TRAINING THE CYBER SECURITY WORKFORCE

JASON DION
TRAINING THE CYBER SECURITY WORKFORCE

Change Authority

ITIL Foundations

Change Authority

- CAB is actually not the change authority but serves as an advisory body making *recommendations*
- Change Authority comprise a role, a person, or a group/team
- Change Authority is the stakeholder for a given change

JASON DION
TRAINING THE CYBER SECURITY WORKFORCE

Who is the Change Authority?

- RFC documents the change authority for a given change
- Change Management Team notates this during the “raising of an RFC” in the workflow activity
- Change Authorities are often in the management level, executive board, or IT steering group

JASON DION
TRAINING THE CYBER SECURITY WORKFORCE

Delegation

- Delegation of the Change Authority often occurs to the CAB or Change Manager

- Routine changes can be delegated down to junior management such as during Standard Changes

JASON DION
TRAINING THE CYBER SECURITY WORKFORCE

JASON DION
TRAINING THE CYBER SECURITY WORKFORCE

Change Models

ITIL Foundations

Change Models

- Predefined steps taken to handling a certain category of change

- Numerous change models exist with one for each configuration item

JASON DION
TRAINING THE CYBER SECURITY WORKFORCE

Simple or Complex?

- Change models can be simple or complex

- Simple
  Used for tasks like change a password or moving a workstation

- Complex
  Used for tasks like major system rollouts or configuration changes

JASON DION
TRAINING THE CYBER SECURITY WORKFORCE

Standard Change Model

- Detailed model covering all the technical details and angles of the proposed changes

- Routine tasks can be covered by incorporation into the Standard Operating Procedures

JASON DION
TRAINING THE CYBER SECURITY WORKFORCE

Normal Change Model

- Not as detailed because each change being proposed has unique qualities

JASON DION
TRAINING THE CYBER SECURITY WORKFORCE

Usefulness of Change Models

- Change models are useful when emergency changes are proposed

- Provides guidance and useful checklists when limited time is available

JASON DION
TRAINING THE CYBER SECURITY WORKFORCE

JASON DION
TRAINING THE CYBER SECURITY WORKFORCE

Change Documents

ITIL Foundations

Change Documents

- Request for Change
- Change Record
- CAB Minutes
- Change Schedule
- Projected Service Outage

JASON DION
TRAINING THE CYBER SECURITY WORKFORCE

Request for Change (RFC)

- Formal change proposal
- Manages change throughout the process

CHANGE REQUEST 24093-D

Type: AZB → vehicle interior → air bags **ID**: 24093-D
Deadline: ASAP **Priority**: high
Customer:
*__direct__: customer service (internal)
*__indirect__: (future) owners of car type AZB (external)

Abstract: Air bags of car type AZB automatically inflate on long distances. This is a severe issue that must be repaired at all cost. Probable cause is a misconfiguration of the car's electric circuit on Board 13-C. A repair plan for dealers should be created and the production department needs an updated design.

Related documents:
*Problem report C253087
*Lab test AE13

JASON DION
TRAINING THE CYBER SECURITY WORKFORCE

Change Record

- Gives additional details to the RFC and records the relevant information about the change throughout the workflow and its lifecycle

JASON DION
TRAINING THE CYBER SECURITY WORKFORCE

CAB Minutes

- Record of the CAB meetings
- Documentation of members present
- Documents what was discussed
- Documents reasoning used to make decisions

JASON DION
TRAINING THE CYBER SECURITY WORKFORCE

Change Schedule

- States changes to be implemented
- Scheduled dates
- Other pertinent information useful to the IT staff, users, Service Desk, and the customers

JASON DION
TRAINING THE CYBER SECURITY WORKFORCE

Projected Service Outage (PSO)

- Notifies IT staff, users, Service Desk, and the customers of any changes to normal service availability resulting from impending changes that have been approved for implementation

JASON DION
TRAINING THE CYBER SECURITY WORKFORCE

JASON DION
TRAINING THE CYBER SECURITY WORKFORCE

Release & Deployment Management

ITIL Foundations

http://www.jasondion.com

Definition of a Release

- One or more changes to an IT service that are built, tested, and deployed together

- *Releases consist of software, hardware, configurations, or a combination of these*

JASON DION
TRAINING THE CYBER SECURITY WORKFORCE

Purpose

- Plans, schedules, and controls the build, test, and deployment of releases, as well as to deliver new functionality required by the business while protecting the integrity of existing services

JASON DION
TRAINING THE CYBER SECURITY WORKFORCE

Purpose

- ***Plans, schedules***, and controls the build, test, and deployment of releases, as well as to deliver new functionality required by the business while protecting the integrity of existing services

Crucial to a successful release and controlled by higher-level guidance of the Change Management process

JASON DION
TRAINING THE CYBER SECURITY WORKFORCE

Purpose

- Plans, schedules, and ***controls*** the build, test, and deployment of releases, as well as to deliver new functionality required by the business while protecting the integrity of existing services

Signifies governance and not just the administration of releases and deployments

JASON DION
TRAINING THE CYBER SECURITY WORKFORCE

Purpose

- Plans, schedules, and controls the ***build, test***, and deployment of releases, as well as to deliver new functionality required by the business while protecting the integrity of existing services

Each component of the release has been built and tested separately and as an entire system to ensure a successful integration

Purpose

- Plans, schedules, and controls the build, test, and ***deployment*** of releases, as well as to deliver new functionality required by the business while protecting the integrity of existing services

Release is placed into the live environment using your deployment mechanisms

JASON DION
TRAINING THE CYBER SECURITY WORKFORCE

Purpose

- Plans, schedules, and controls the build, test, and deployment of releases, as well as to ***deliver new functionality*** required by the business while protecting the integrity of existing services

Provide enhanced utility in the production environment to enable more effective customer outcomes

JASON DION
TRAINING THE CYBER SECURITY WORKFORCE

Purpose

- Plans, schedules, and controls the build, test, and deployment of releases, as well as to deliver new functionality required by the business while ***protecting*** the integrity of ***existing services***

Rollout of the new changes cannot negatively impact the existing services (other than as specified in PSO)

JASON DION
TRAINING THE CYBER SECURITY WORKFORCE

Scope/Span of the Process

- Physical assets (servers, networks,…)
- Virtual assets (VMs, cloud)
- Application/System software
- Relevant documentation
- Training for users and IT staff
- Supporting services, including all related contracts and agreements
- Ensuring appropriate testing is completed (per Service Validation and Testing process)

JASON DION
TRAINING THE CYBER SECURITY WORKFORCE

Functions

- Produce\maintain R&D policy
- Produce\maintain individual R&D plans
- Define\create\test release packages
- Maintain integrity of live environment
- Deploy software from DML only

JASON DION
TRAINING THE CYBER SECURITY WORKFORCE

Functions

- Track progress of releases with SACM process
- Ensure each release has a test plan for backout
- Manage organizational and stakeholder change
- Ensure services deployed deliver agreed-upon utility and warranty

JASON DION
TRAINING THE CYBER SECURITY WORKFORCE

Functions

- Record and manage deviations, risks, and issues
- Ensure successful transfer of skills and knowledge to users, customers, and Service Operation functions

JASON DION
TRAINING THE CYBER SECURITY WORKFORCE

Release & Deployment Assets

ITIL Foundations

Secure Repositories

- All assets being deployed (hardware or software) need to come from a trusted, quality-assured source

- Two main ones:
  - Definitive Media Library (DML)
  - Definitive Spares

JASON DION
TRAINING THE CYBER SECURITY WORKFORCE

Definitive Media Library

- Secure storage of master copies of all software
- Access to DML is controlled
- DML is physical, electronic, or both
- All software is quality-checked for completeness and viruses prior to entering the DML

JASON DION
TRAINING THE CYBER SECURITY WORKFORCE

Definitive Media Library

- Software remains in the DML until it is no longer useful
  - Older versions can prove useful in legacy systems and during troubleshooting
- Many organizations also keep copies of licenses in the DML for tracking and safekeeping

JASON DION
TRAINING THE CYBER SECURITY WORKFORCE

Definitive Spares

- Unallocated items of hardware
- *Float* is unallocated but configured hardware ready to be swapped into the network for broken assets
- Definitive spares are controlled like the DML and each item is quality-checked to ensure it is ready for use when needed

JASON DION
TRAINING THE CYBER SECURITY WORKFORCE

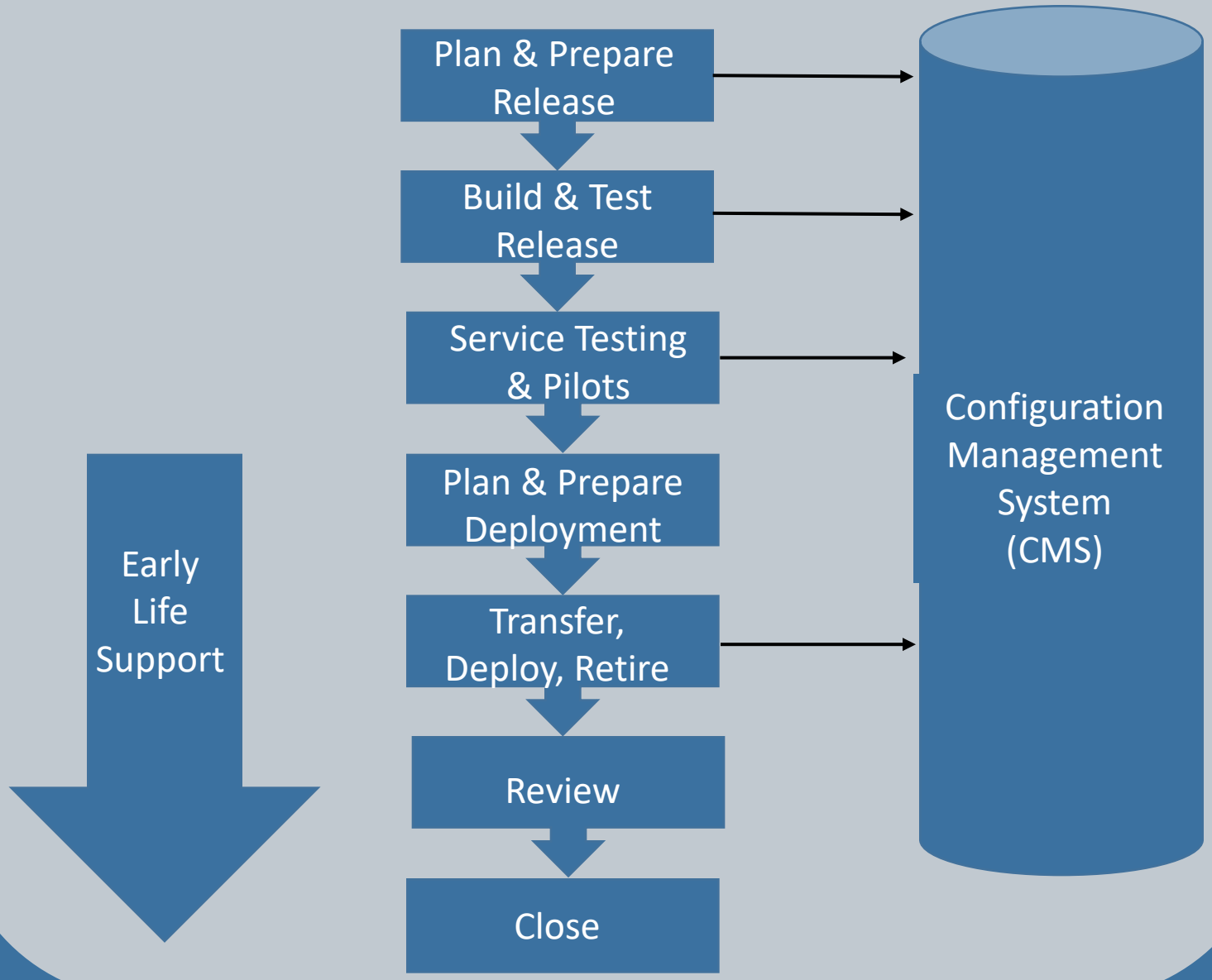
JASON DION
TRAINING THE CYBER SECURITY WORKFORCE

Release & Deployment Process

ITIL Foundations

http://www.jasondion.com

Workflow: Release & Deployment



JASON DION
TRAINING THE CYBER SECURITY WORKFORCE

Plan and Prepare

- In accordance with policy, determine RFCs for the release candidate
- Check authorization on RFCs for implementation
- Check resource availability
- Publish the plan for release
- Ensure organization/users are ready to receive release (training)

JASON DION
TRAINING THE CYBER SECURITY WORKFORCE

Build and Test

- Combine all components (even across multiple RFCs) that comprise release
  - Sometimes RFCs will be from different projects, but release as a single release to maximize the maintenance window
- Testing ensure no incompatibility in the mixture of the RFCs
- Testing of the deployment mechanism should also occur in this phase

JASON DION
TRAINING THE CYBER SECURITY WORKFORCE

Service Testing and Pilots

- Ensures that the release, as a whole, will provide the agreed upon utility and warranty

- Often includes a Pilot test in the live environment across a limited number of live users such as a one department or single geographic region

JASON DION
TRAINING THE CYBER SECURITY WORKFORCE

Plan and Prepare Deployment

- Usually uses automated deployment for software products
- Software originates from the DML
- Hardware requires physical deployment and coordination with the software deployment

JASON DION
TRAINING THE CYBER SECURITY WORKFORCE

Transfer, Deploy, Retire

- It is time to put our plan into effect!
- Service is transferred from one service provider to the next
- Hardware/software are deployed
- Redundant services, hardware, software are retired and their resources are made available to resource pool

JASON DION
TRAINING THE CYBER SECURITY WORKFORCE

Early Life Support

- Additional highly skilled specialists may augment the operational teams during the initial roll out of the new or changed services

- Goal:

  Bring operational staff up to speed and allow them to takeover the operations fully

JASON DION
TRAINING THE CYBER SECURITY WORKFORCE

Review and Close

- Once everything is “done”, it is time to review and close out the deployment

- Includes a review to confirm success has been achieved and to collect the lessons learned

JASON DION
TRAINING THE CYBER SECURITY WORKFORCE

A Note on Phased Releases

- In large organizations, releases are done in a phased approach based on time and/or geography

- Planning, preparation, and control are essential to the success of a phased release and good configuration management is essential to understand your ever changing services!

JASON DION
TRAINING THE CYBER SECURITY WORKFORCE

JASON DION
TRAINING THE CYBER SECURITY WORKFORCE

Service Validation & Testing

ITIL Foundations

http://www.jasondion.com

Service Validation & Testing Process

JASON DION
TRAINING THE CYBER SECURITY WORKFORCE

Ensures the service that has been built meets the specifications and will provide the agreed upon utility and warranty to the customer

Note: Service Validation & Testing Process is not covered by the ITIL Foundation exam

Important Considerations

- Testing is performed under both the Change Management process and the Release & Deployment process

- Different testers than the Release & Deployment personnel conduct the testing to ensure compliance and proper validation

JASON DION
TRAINING THE CYBER SECURITY WORKFORCE

Service Validation & Testing Process

JASON DION
TRAINING THE CYBER SECURITY WORKFORCE

Process is not covered by the ITIL Foundation exam, but it is necessary to fully understand the lifecycle

Note: Service Validation & Testing Process is not covered by the ITIL Foundation exam

JASON DION
TRAINING THE CYBER SECURITY WORKFORCE

Change Evaluation

ITIL Foundations

Change Evaluation Process

- To assess the likely performance of the new or changed service
- To compare predicted performance against actual performance
- To identify and manage risk and issues

Note: Change Evaluation Process is not covered by the ITIL Foundation exam

JASON DION
TRAINING THE CYBER SECURITY WORKFORCE

Important Considerations

- Helps to set stakeholder expectations

- Valuable in providing guidance to the Change Management team on whether to allow a change to proceed to next phase of the change process workflow

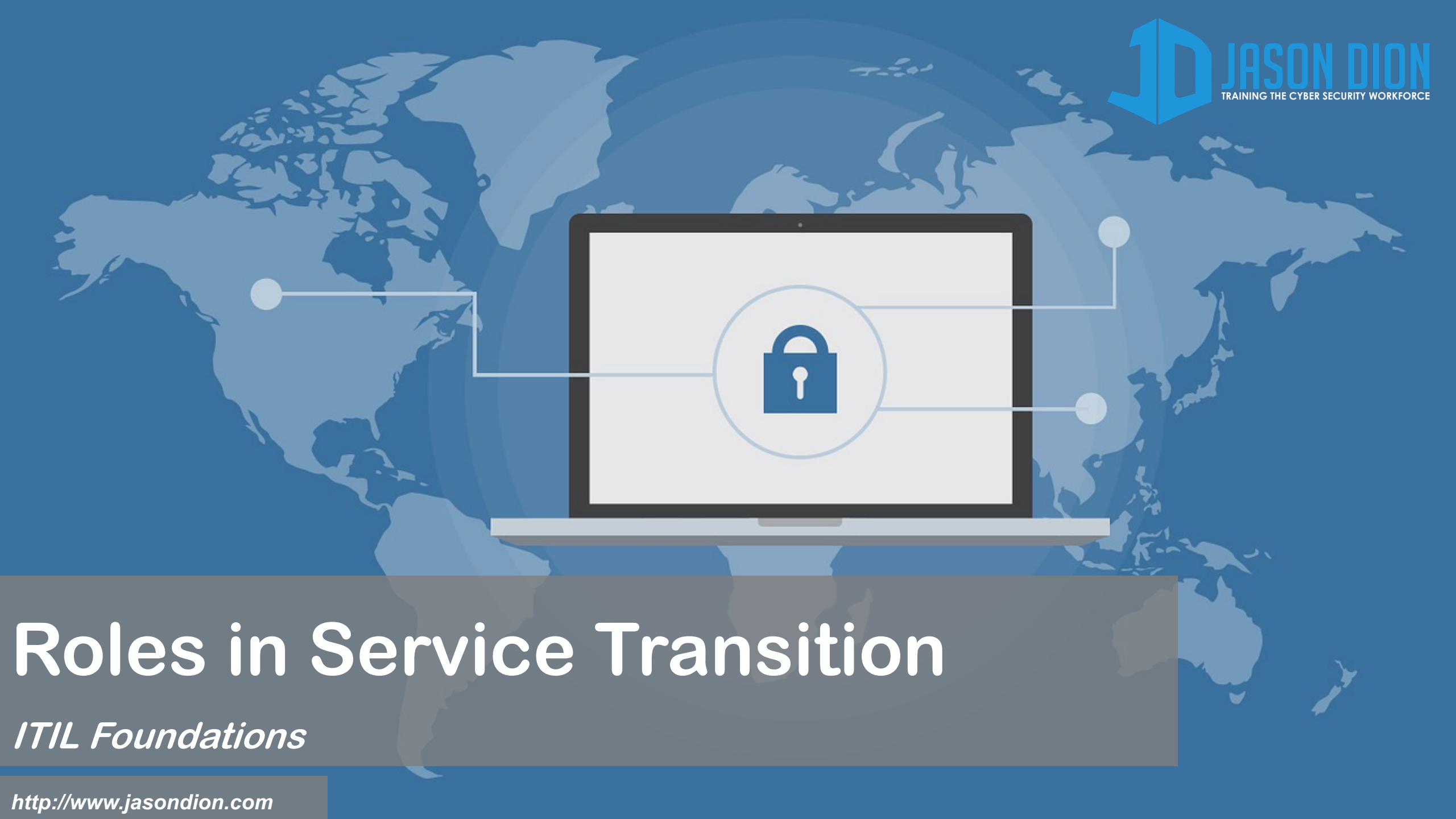
JASON DION
TRAINING THE CYBER SECURITY WORKFORCE

Change Evaluation Process

JASON DION
TRAINING THE CYBER SECURITY WORKFORCE

Process is not covered by the ITIL Foundation exam, but it is necessary to fully understand the lifecycle

Note: Service Validation & Testing Process is not covered by the ITIL Foundation exam



JASON DION
TRAINING THE CYBER SECURITY WORKFORCE

Roles in Service Transition

ITIL Foundations

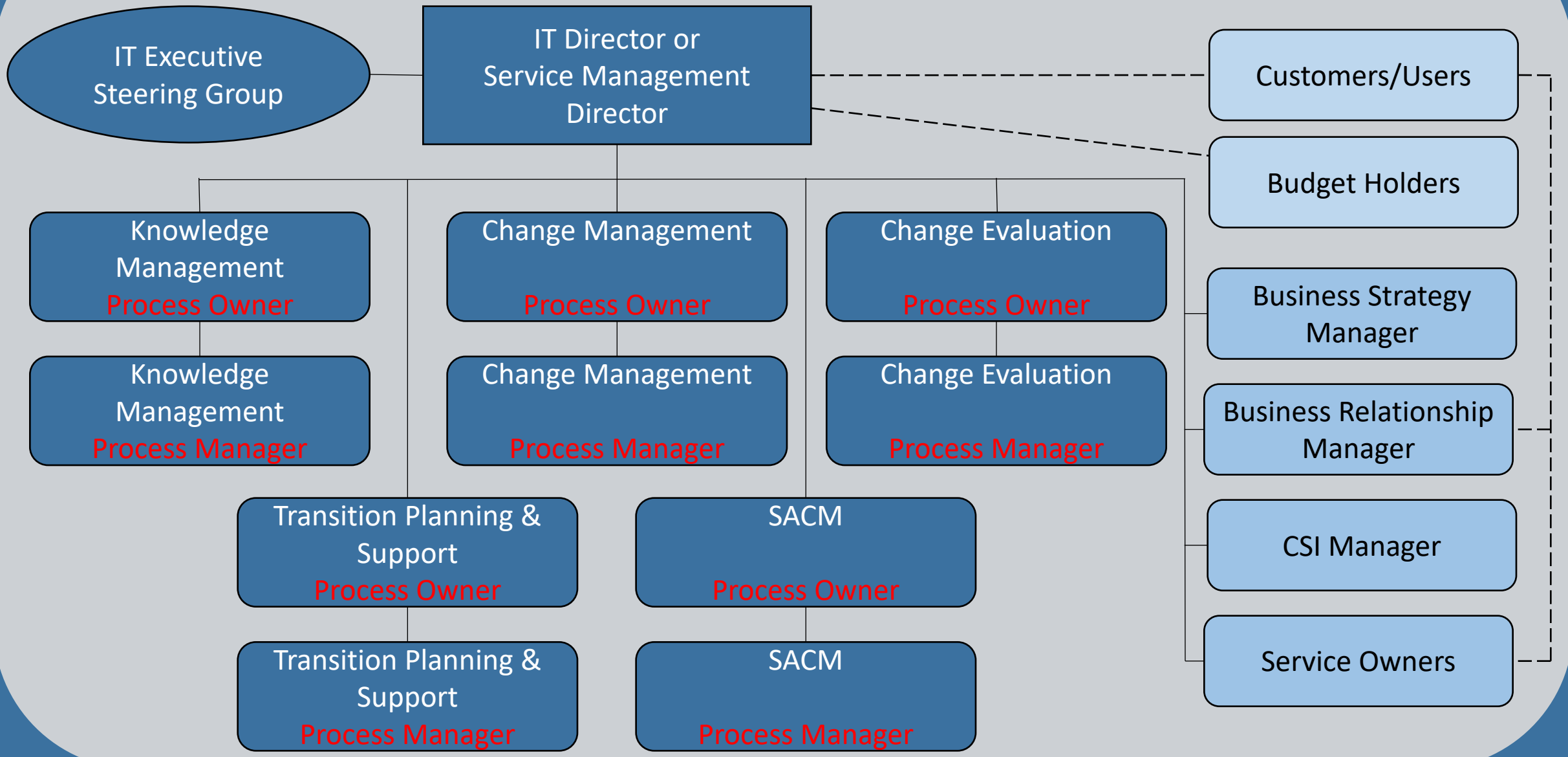
Roles in Service Transition

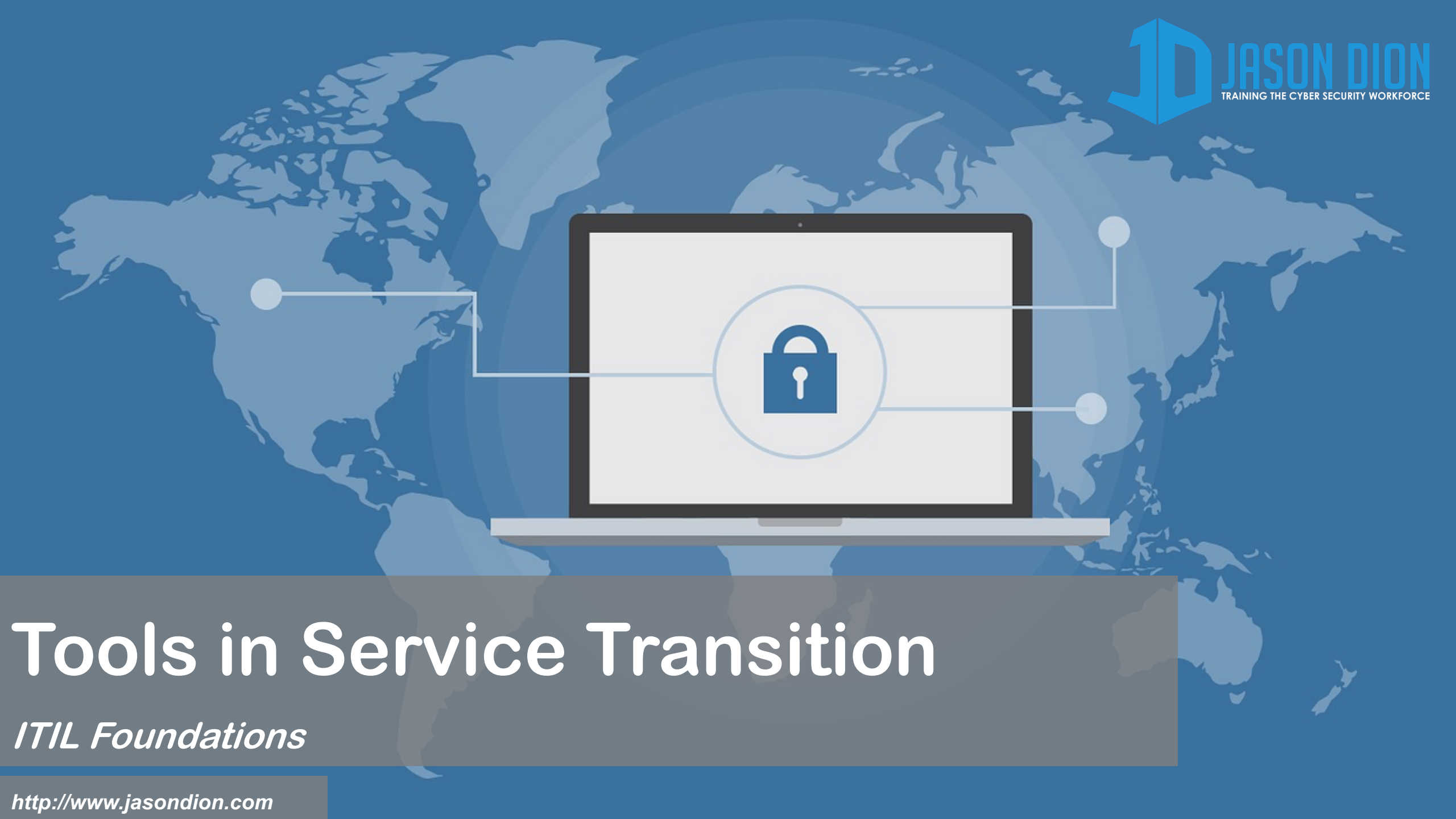
- ITIL doesn't dictate how an organization should be organized

- ITIL does recommends roles:
  - Service Owner
  - Process Owner
  - Process Manager

JASON DION
TRAINING THE CYBER SECURITY WORKFORCE

Roles in Service Transition





JASON DION
TRAINING THE CYBER SECURITY WORKFORCE

Tools in Service Transition

ITIL Foundations

Tools in Service Transition

- Many of the same tools from the Service Strategy stage are useful in Service Transition

- Many different areas in Service Transition can be benefited by the use of technology

JASON DION
TRAINING THE CYBER SECURITY WORKFORCE

Areas Where Tools Help

- System, network, and application management
- Integrated ITSM tools for configuration, change, and release & deployment
- Discovery and auditing tools
- Software distribution and management

JASON DION
TRAINING THE CYBER SECURITY WORKFORCE

Areas Where Tools Help

- Service dashboards and reporting
- Document and records management
- Collaboration tools
- Test and test management tools

JASON DION
TRAINING THE CYBER SECURITY WORKFORCE