Cyber Resilience Toolkit

Index & Controls Reference

Cyber Resilience

A canonical reference for cyber resilience terminology, structures, and control alignment.

by Blake Wiltshire

Cyber Resilience Tools — Index & Controls Reference

By Blake Wiltshire

Published independently by Blake Wiltshire

Part of the **Cyber Resilience Toolkit (CRT)**

This reference forms part of a modular decision-support framework designed to strengthen structured reasoning, architectural governance, and control interpretation across cybersecurity and digital-risk ecosystems.
It supports the Cyber Resilience in the Information Age guide and the wider Cyber Resilience Toolkit (CRT) environment — providing the shared language, structural definitions, and technical-control mappings that connect guides, modular tools, and AI-assisted reasoning into a unified analytical system.

Copyright © 2026

Published independently • Printed in the United Kingdom

Trademarks

Table of Contents

Disclaimer

Important Notice

This reference forms part of the Cyber Resilience Toolkit (CRT) and the companion guide Cyber Resilience in the Information Age — Strategic Foundations for Risk and Adaptation.

It is designed to support structured reasoning, control interpretation, and system-level analysis across cybersecurity and governance environments.

It does not constitute security advice, professional assurance, or compliance certification.

Risk Disclosure

All frameworks, indices, and control classifications described herein are designed for architectural reasoning — not prescriptive implementation.

Cyber-risk conditions evolve continuously, and outcomes may vary by organisation, sector, or jurisdiction. Readers should apply independent judgment, conduct verification, and consult qualified professionals before acting on any interpretation or mapping.

Examples and references are illustrative only and not tailored to specific infrastructures.

Limitation of Liability

The CRT framework and associated references are intended to inform reflection and structured decision-support — not to replace institutional governance, regulatory obligation, or professional judgment.

All actions and interpretations remain solely the responsibility of the reader.

Personal Responsibility

The CRT and its companion references are intended to support structured exploration, reflective assessment, and decision-support design — not to replace institutional policy, regulatory obligation, or human oversight.

AI Personas and Role-Based Interaction

AI-linked personas, prompts, and integrations referenced within the CRT environment are conceptual scaffolds for exploration and analysis.

They do not represent real individuals, certified experts, or deterministic systems.

All AI interactions are illustrative, probabilistic, and context-dependent, designed to augment reasoning — never to prescribe outcome or action.

About This Series

The Cyber Resilience Toolkit (CRT) extends the Blake Wiltshire System into the domains of cybersecurity, governance, and digital continuity.

It provides a modular architecture for interpreting how technical controls, human factors, and governance structures combine to form adaptive resilience across interconnected systems.

Structured around the Cyber Resilience in the Information Age guide, the CRT includes catalogues, control mappings, and decision-support modules that link conceptual foundations to operational application.

Together they form a unified environment for reasoning about exposure, governance, and strategic control within the Information Age.

This reference acts as the linguistic and architectural layer for that environment — linking foundational terminology with technical control definitions and the broader CRT Decision-Support System.

About This Reference

The Cyber Resilience Tools — Unified Index & Glossary Reference consolidates the key terms, control families, and system definitions that underpin the Cyber Resilience Toolkit (CRT) and its companion guide.

It bridges three interpretive layers:

1. **Foundational Concepts** — governance, resilience, trust, and structural design principles.
2. **Technical Controls** — baseline architectural mechanisms across prevent, detect, respond, and recover domains.
3. **Integrative Mappings** — cross-references to CRT modules and decision-support schemas.

Each entry defines a term or control class, identifies its structural purpose, and notes linkages to the relevant CRT catalogue (C, F, N series).

The content is non-prescriptive, platform-agnostic, and suitable for conceptual, audit, and analytical use alike.

Reference Governance and Currency

All entries in this reference align with the CRT structural architecture at the time of publication.

Canonical control catalogues, schemas, and reference datasets are maintained within the Cyber Resilience Toolkit (CRT) framework and its associated repositories. This document functions as a consolidated interpretive layer, not as a live configuration source.

Updates, schema expansions, and versioned releases are published through the official CRT distribution channels and reflected within the CRT application, including the Index & Controls Viewer.

How to Use This Document

This document provides the canonical reference index for the Cyber Resilience Toolkit (CRT).

It is designed to support structural orientation, terminology alignment, and cross-domain reasoning across the CRT ecosystem.

Entries are arranged alphabetically (A—Z).

Each entry may include:

- □ **Term / Control Family** — the defined structural concept, domain, or control grouping.
- □ **Structural Context** — the primary resilience domain or architectural concern the term relates to (e.g. data, identity, governance, monitoring).
- □ **Definition** — a concise, non-prescriptive description of function, scope, and intent.
- □ **CRT Controls / Families (where applicable)** — associated control identifiers or catalogue groupings (CRT-C, CRT-F, CRT-N, CRT-G).
- □ **CRT Modules (illustrative touchpoints)** — environments within the CRT where the concept is commonly surfaced or referenced.

Interpretive Note — Illustrative Touchpoints

Touchpoints indicate where a concept is typically expressed or examined within the CRT environment.

They do not imply workflow, execution order, dependency, or required module usage.

Cross-references indicate conceptual alignment, not operational linkage or enforcement. They serve as interpretive anchors, allowing readers to trace how terminology, architecture, and structural logic connect across the CRT framework without implying configuration or action.

This index functions as a reference layer, not a configuration guide, maturity model, or implementation manual.

Its purpose is to preserve terminological coherence and structural clarity across guides, supplemental references, and the CRT application.

For the most recent reference datasets and updates, visit: blakewiltshire.com

Cyber Resilience Toolkit — Structural Module Index

This section provides a structural overview of the primary CRT environments and reasoning surfaces. It is intended to orient readers to the conceptual role of each module within the CRT ecosystem.

It does not describe workflows, execution order, configuration steps, or required usage. Module capabilities evolve over time; the CRT application and Index & Controls Viewer remain the authoritative sources for current functionality.

🏠 CRT Home

Structural Function

Provides orientation to the CRT environment, framing resilience as a system of structured reasoning surfaces rather than tools or tasks.

🎛️ Programmes & Outputs

Structural Function

Forms governance, architecture, metrics, and scenario artefacts from structured CRT catalogues and contextual bundles.

This is where reasoning is externalised into reviewable, traceable forms.

🎛️ Programme Builder Export

Structural Function

Assembles decision artefacts (manifests and bundles) that externalise how an organisation is reasoning about resilience at a point in time.

🎛️ Task Builder

Structural Function

Frames reasoning tasks across governance, architecture, metrics, and simulation without prescribing outcomes or execution paths.

Governance — policy drafts, standards, risk briefs, questionnaires, narratives

Architecture — structural views, zoning, data-flow summaries

Metrics — resilience briefs, coverage summaries

Simulation — playbooks, scenario summaries, “what-if” structural exploration

🧱 User Templates

Structural Function

Provides reusable reasoning scaffolds for artefact articulation, not executable playbooks.

🔍 Verify

Structural Function

Confirms structural completeness and coherence of a reasoning artefact prior to downstream interpretation.

🧠 AI Prompt & Response

Structural Function

Supports bounded AI articulation within explicit governance and interpretive constraints.

🧹 Maintenance

Structural Function

Manages versioned artefacts, profiles, and structural hygiene across the CRT environment.

📁 Structural Controls & Frameworks

Structural Function

Org Governance Profile (Org & Scope)

CRT Defaults Browser

Governance Setup (Framework Onboarding)

Operational Extensions (Org-Specific)

Mapping Explorer

🔎 Structural Lenses

Structural Function

Provide read-only structural views that surface exposure, dependency, and constraint without implying action or optimisation.

🧮 Data Classification Registry

Structural Function

Surfaces data sensitivity, propagation rules, and handling constraints as governance context.

🧩 Attack Surface Mapper

Structural Function

Represents exposure pathways across users, systems, services, and dependencies.

🔐 Identity & Access Lens

Structural Function

Frames identity, privilege, and trust boundaries as architectural structure.

🛰️ Supply-Chain Exposure Scanner

Structural Function

Surfaces transitive dependency and vendor-propagation risk across ecosystems.

📡 Telemetry & Signal Console

Structural Function

Aggregates operational signals as interpretive inputs, not automated decisions.

📚 Reference & Integration

Structural Function

Provides canonical reference layers and integration utilities that stabilise interpretation across the CRT.

📚 Reference Data & Trusted Sources

Structural Function

Anchors reasoning in external frameworks, indices, taxonomies, and CRT reference catalogues.

🌐 Cyber Resilience Reference Directory

Structural Function

Presents curated structural references supporting governance and architectural reasoning.

🧠 AI Persona Reference

Structural Function

Defines bounded analytical framings for AI-assisted articulation (non-agent, non-advisory).

🗃️ Index & Controls Viewer

Structural Function

Provides the authoritative index of controls, concepts, and mappings used throughout the CRT.

🔄 System Integrator Hub

Structural Function

Maintains schema coherence, entity relationships, and interoperability across CRT modules.

Catalogue health

Catalogue explorer

Entity & relationship probe

Note — Structural Index, Not Workflow

This index reflects structural surfaces, not user journeys, task sequences, or operational flows.

Presence in the index does not imply required usage, execution order, or maturity expectation.

Index & Glossary (Concepts)

This section consolidates the core concepts, structural terminology, and analytical language used throughout the Cyber Resilience Toolkit (CRT) ecosystem and the *Cyber Resilience in the Information Age* volume.

Entries are arranged alphabetically (A—Z). Each term includes a concise definition and, where relevant, cross-references to the guide and chapter in which the concept is discussed.

This index serves as a conceptual anchor, supporting interpretation across CRT modules, scenario analysis, governance frameworks, and architectural discussions.

A

Acceleration Vector — A structural driver (compute, latency, abstraction, tooling) that compresses decision cycles and increases operational tempo.
→ *Cyber Resilience in the Information Age* — Chapter 6 — Acceleration Vectors & Strategic Asymmetries

Accelerated Adversarial Operations — Attacks amplified by automation, leveraging speed, scale, and unpredictability to overwhelm manual defence cycles.
→ *Cyber Resilience in the Information Age* — Chapter 6 — Rise of Autonomous Threats & Defences

Adaptive Continuity — The capacity to anticipate, absorb, and respond to disruption without systemic failure.
→ *Cyber Resilience in the Information Age* — Chapter 2 — Core Principles of Cybersecurity

Adaptive Memory — Retention of validated interpretations and decisions as organisational context, enabling continuity without automation of judgement.
→ *Cyber Resilience in the Information Age* — Chapter 5 — Platform Architecture for AI-Augmented Resilience

Adaptive Readiness — The capacity to re-align response posture dynamically under uncertainty and partial information.
→ *Cyber Resilience in the Information Age* — Chapter 5 — Incident Readiness and Adaptive Containment

Alignment Risk — Divergence between autonomous system outcomes and organisational intent, constraints, or governance expectations.
→ *Cyber Resilience in the Information Age* — Chapter 6 — Rise of Autonomous Threats & Defences

Anomaly Framing — Treating deviation as a structural signal indicating early disruption geometry.
→ *Cyber Resilience in the Information Age* — Chapter 4 — Adaptive Monitoring & AI-Augmented Detection

Architectural Continuity — Embedding control logic directly into operational workflows rather than separating protection from process.
→ *Cyber Resilience in the Information Age* — Chapter 4 — Layered Defence — Continuity Across Functions

Architectural Sovereignty — The ability to maintain control over data, logic, and infrastructure across jurisdictions without isolation.
→ *Cyber Resilience in the Information Age* — Chapter 6 — Strategic Imperatives for the Next Information Age

Attack Surface — The cumulative set of pathways through which systems or data may be accessed, manipulated, or disrupted.
→ *Cyber Resilience in the Information Age* — Chapter 1 — The Rise of the Information Age

Autonomous Agents — Self-directed systems that execute and adapt actions based on environmental input and embedded decision logic.
→ *Cyber Resilience in the Information Age* — Chapter 6 — Rise of Autonomous Threats & Defences

Autonomy Preservation — Designing systems that retain meaningful human or institutional control under distributed automation.
→ *Cyber Resilience in the Information Age* — Chapter 6 — Strategic Imperatives for the Next Information Age

B

Behavioural Mimicry — Adaptive imitation of legitimate patterns to evade detection and exploit contextual trust.
→ *Cyber Resilience in the Information Age* — Chapter 6 — Rise of Autonomous Threats & Defences

C

Commons-Aligned Control Models — Structural governance extended into shared infrastructures where collective continuity is essential.
→ *Cyber Resilience in the Information Age* — Chapter 6 — Strategic Imperatives for the Next Information Age

Commons Resilience Architecture — Mechanisms embedding integrity, continuity, and traceable accountability into open digital ecosystems.
→ *Cyber Resilience in the Information Age* — Chapter 6 — Future of the Commons

Connectivity — Seamless transfer of information across individuals, systems, and jurisdictions.
→ *Cyber Resilience in the Information Age* — Chapter 1 — The Rise of the Information Age

Consensus Fragility — Vulnerability of distributed validation to manipulation, latency, or coordinated failure.
→ *Cyber Resilience in the Information Age* — Chapter 6 — Open Systems & Decentralised Trust

Containment Architecture — Recovery designed as a pre-engineered capability rather than emergency improvisation.
→ *Cyber Resilience in the Information Age* — Chapter 4 — Embedded Recovery & Systemic Containment

Continuity by Design — Engineering continuity as a condition embedded in system behaviour, not post-incident recovery.
→ *Cyber Resilience in the Information Age* — Chapter 6 — Strategic Imperatives for the Next Information Age

Continuity Threshold — The point where controlled degradation becomes loss of coherence.
→ *Cyber Resilience in the Information Age* — Chapter 5 — Scenario Analysis and Structural Stress Testing

Control Absolutism (Limitations) — Recognition that perfect defence is unattainable; resilience depends on adaptability and recovery logic.
→ *Cyber Resilience in the Information Age* — Chapter 2 — Core Principles of Cybersecurity

Control Assertion — Ability to enforce governance across systems not under direct ownership.
→ *Cyber Resilience in the Information Age* — Chapter 6 — Data Sovereignty in a Post-Perimeter World

Control Loop Displacement — Loss of human oversight caused by automation tempo and delegated execution.
→ *Cyber Resilience in the Information Age* — Chapter 6 — Rise of Autonomous Threats & Defences

Critical Exposure Points — Junctions where compromise produces disproportionate operational or societal impact.
→ *Cyber Resilience in the Information Age* — Chapter 2 — Strategic Risk Architecture & Operational Control
→ *Cyber Resilience in the Information Age* — Chapter 3 — Strategic Risk Architecture — Foundations of Control Design

D

Datafication — Conversion of actions, preferences, and relationships into structured digital information.
→ *Cyber Resilience in the Information Age* — Chapter 1 — The Rise of the Information Age

Data Integrity and Trust — Stability of information flows preserving confidence in system operation and governance.
→ *Cyber Resilience in the Information Age* — Chapter 2 — Core Principles of Cybersecurity

Data Sovereignty — Governance, jurisdiction, and authority over data use, flow, and inference.
→ *Cyber Resilience in the Information Age* — Chapter 1 — Data, Power & the New Strategic Landscape
→ *Cyber Resilience in the Information Age* — Chapter 6 — Data Sovereignty in a Post-Perimeter World

Decision Surface — Boundary where information becomes action, requiring authority and accountability.
→ *Cyber Resilience in the Information Age* — Chapter 5 — Incident Readiness and Adaptive Containment

Detection Velocity — Time between signal emergence and human-recognised significance.
→ *Cyber Resilience in the Information Age* — Chapter 5 — Incident Readiness and Adaptive Containment

Distributed Risk — Exposure embedded across interconnected nodes rather than isolated systems.
→ *Cyber Resilience in the Information Age* — Chapter 1 — Structural Shifts in Risk Exposure

Distributed Trust Anchors — Validators and attestors confirming legitimacy in decentralised systems.
→ *Cyber Resilience in the Information Age* — Chapter 6 — Open Systems & Decentralised Trust

E

Embedded Decision Architecture — Structural scaffolding through which autonomous systems interpret and act on stimuli.
→ *Cyber Resilience in the Information Age* — Chapter 6 — Rise of Autonomous Threats & Defences

Explainable Architecture — Architectural property where AI contributions remain interpretable by humans.
→ *Cyber Resilience in the Information Age* — Chapter 5 — Platform Architecture for AI-Augmented Resilience

Exposure Mapping — Identifying points where data flow or aggregation introduces systemic risk.
→ *Cyber Resilience in the Information Age* — Chapter 1 — Mapping Exposure in a Connected World

Exponentiality — Compounding acceleration of technological change and cascading systemic effects.
→ *Cyber Resilience in the Information Age* — Chapter 1 — The Rise of the Information Age

F

Failure Propagation — How disruption spreads, amplifies, or is contained across dependencies.
→ *Cyber Resilience in the Information Age* — Chapter 5 — Scenario Analysis and Structural Stress Testing

Federated Identity Models — Cross-organisational identity fabrics introducing shared trust and dependency risk.
→ *Cyber Resilience in the Information Age* — Chapter 4 — Identity & Trust as Anchors of Resilience

G

Governability Under Speed — Preserving interpretability, override, and constraint below human tempo.
→ *Cyber Resilience in the Information Age* — Chapter 6 — Acceleration Vectors & Strategic Asymmetries

Governance by Design — Embedding oversight, reversibility, and constraint into system architecture.
→ *Cyber Resilience in the Information Age* — Chapter 5 — Platform Architecture for AI-Augmented Resilience

Governance-Embedded Systems — Architectures integrating oversight and proportional override into operations.
→ *Cyber Resilience in the Information Age* — Chapter 6 — Strategic Imperatives for the Next Information Age

H

I

Identity as the New Perimeter — Identity verification as the primary anchor for trust and access.
→ *Cyber Resilience in the Information Age* — Chapter 2 — From Perimeters to Ecosystems

Information Centralisation — Concentration of data control creating efficiency and dependency simultaneously.
→ *Cyber Resilience in the Information Age* — Chapter 1 — Data, Power & the New Strategic Landscape

J

Judgement Separation — Clear boundary between articulated reasoning and accountable decision-making.
→ *Cyber Resilience in the Information Age* — Chapter 5 — Risk Mapping and Structural Prioritisation

K

L

Layered Accountability — Separation of signal, reasoning, and governance layers to preserve authority visibility.
→ *Cyber Resilience in the Information Age* — Chapter 5 — Platform Architecture for AI-Augmented Resilience

Layered Control Architecture — Defence logic embedded across prevention, detection, response, and recovery layers.
→ *Cyber Resilience in the Information Age* — Chapter 2 — Strategic Risk Architecture & Operational Control
→ *Cyber Resilience in the Information Age* — Chapter 3 — Strategic Risk Architecture — Foundations of Control Design

M

Metric Triangulation — Correlating multiple artefacts or lenses to validate interpretive confidence.
→ *Cyber Resilience in the Information Age* — Chapter 5 — Structural Metrics and Balanced Perspectives

N

O

Operational Agility — *Ability of control frameworks to evolve without introducing fragility.*
→ *Cyber Resilience in the Information Age — Chapter 2 — Strategic Risk Architecture & Operational Control*
→ *Cyber Resilience in the Information Age — Chapter 3 — Strategic Risk Architecture — Foundations of Control Design*

P

Propagation Velocity — Speed at which disruption spreads across dependencies and trust boundaries.
→ *Cyber Resilience in the Information Age* — Chapter 6 — Acceleration Vectors & Strategic Asymmetries

Proportional Intelligence Deployment — Using AI as a bounded utility aligned to decision criticality and risk.
→ *Cyber Resilience in the Information Age* — Chapter 6 — Strategic Imperatives for the Next Information Age

Q

R

Resilience by Design — Designing systems where resilience is a primary architectural outcome.
→ *Cyber Resilience in the Information Age* — Chapter 6 — Strategic Imperatives for the Next Information Age

Residual Visibility — Making explicit what remains unmanaged or conditionally managed.
→ *Cyber Resilience in the Information Age* — Chapter 5 — Risk Mapping and Structural Prioritisation

Risk Alignment — Structural fit between exposure, appetite, and resource allocation.
→ *Cyber Resilience in the Information Age* — Chapter 2 — Core Principles of Cybersecurity
→ *Cyber Resilience in the Information Age* — Chapter 6 — Strategic Imperatives for the Next Information Age

S

Scenario-Integrated Playbooks — Response frameworks embedded within architecture rather than checklists.
→ *Cyber Resilience in the Information Age* — Chapter 4 — Embedded Recovery & Systemic Containment

Structural Resilience — Security, recovery, and continuity engineered directly into design.
→ *Cyber Resilience in the Information Age* — Chapter 2 — Core Principles of Cybersecurity

Structural Traceability — Ability to follow how a concept is interpreted from intent through constraint.
→ *Cyber Resilience in the Information Age* — Chapter 5 — Risk Mapping and Structural Prioritisation

T

Tempo Gap — Structural mismatch between rapid experimentation and slower validated integration.
→ *Cyber Resilience in the Information Age* — Chapter 6 — Acceleration Vectors & Strategic Asymmetries

Trust Boundary Extension — Structured expansion of control into federated environments.
→ *Cyber Resilience in the Information Age* — Chapter 6 — Data Sovereignty in a Post-Perimeter World

U

V

Visibility-Resilience Link — Relationship between exposure awareness and adaptive security capacity.
→ *Cyber Resilience in the Information Age* — Chapter 1 — Mapping Exposure in a Connected World

W

X

Y

Z

Zero-Trust Foundations — Continuous verification of identity, intent, and system integrity without implicit trust.
→ *Cyber Resilience in the Information Age* — Chapter 4 — Identity & Trust as Anchors of Resilience

Technical Controls Index (CRT-C / CRT-F / CRT-N Families)

This section presents a consolidated view of the technical control families underpinning the Cyber Resilience Toolkit (CRT).

It reflects the structural logic used across the CRT-C (Controls), CRT-F (Foundations), and CRT-N (NIST-aligned) catalogue series.

Entries are arranged alphabetically (A—Z). Each term includes a concise definition and, where relevant, cross-references to the guide and chapter in which the concept is discussed.

This index is a reference layer, not a configuration manual. It supports reasoning about control coverage, inheritance, dependency structure, and systemic resilience across the CRT environment.

Note — Illustrative Touchpoints

Touchpoints indicate where a control family or structural concept is commonly surfaced within the CRT environment.

They do not imply workflow, execution order, dependency, or required module usage.

CRT-G-01 — Data Security and Privacy

Safeguards information assets across storage, processing, and transmission environments. Focus areas include classification, encryption, integrity assurance, retention, and confidentiality.

CRT Controls:

CRT-C-0001, CRT-C-0002, CRT-C-0003, CRT-C-0004, CRT-C-0005, CRT-C-0006

Control Families / Series:

Data Security

CRT Modules (illustrative touchpoints):

🧮 **Data Classification Registry** (classification, handling rules, scopeable datasets for tasks)

🔐 **Identity & Access Lens** (access constraints, privilege boundaries that protect data)

🎛️ **Programme Builder Export** (governance / architecture / metrics / simulation artefacts referencing data controls)

CRT-G-02 — Access and Identity

Defines mechanisms governing authentication, authorisation, credential lifecycle, and privilege enforcement across users, services, and machine identities.

CRT Controls:

CRT-C-0007, CRT-C-0008, CRT-C-0009, CRT-C-0010, CRT-C-0011, CRT-C-0012

Control Families / Series:

Identity and Access

CRT Modules (illustrative touchpoints):

🔐 **Identity & Access Lens**

🎛️ **Programme Builder Export** (policy/standard drafts, risk briefs, control coverage summaries tied to access controls)

CRT-G-03 — Infrastructure and Connectivity

Ensures the resilience, reliability, and segmentation integrity of core infrastructure, network pathways, and connectivity layers.

CRT Controls:

CRT-C-0013, CRT-C-0014, CRT-C-0015, CRT-C-0016, CRT-C-0017, CRT-C-0018

Control Families / Series:

Infrastructure and Connectivity

CRT Modules (illustrative touchpoints):

📡 **Telemetry Signal Console** (signal presence, retention, parsing readiness, mapped controls)

🧩 **Attack Surface Mapper** (exposure type, trust boundary, entry points, mapped controls)

🔄 **System Integrator Hub** (schema coherence, catalogue exploration, relationship probing)

🎛️ **Programme Builder Export** (architecture views, zoning/trust-boundary views, service-chain summaries)

CRT-G-04 — Application and Integration Risk Management

Focuses on application-layer security, API trust boundaries, integration pathways, and service-to-service change governance.

CRT Controls:

CRT-C-0019, CRT-C-0020, CRT-C-0021, CRT-C-0022, CRT-C-0023, CRT-C-0024

Control Families / Series:

Application and Integration

CRT Modules (illustrative touchpoints):

🔄 **System Integrator Hub** (integration surfaces, relationship mapping, coherence checks)

🧩 **Attack Surface** Mapper (service-chain / entry point framing)

📡 **Telemetry Signal Console** (application telemetry sources, API events, detection surfaces)

🎛️ **Programme Builder Export** (architecture artefacts: data-flow/service-chain, control coverage)

CRT-G-05 — Third-Party and Vendor

Evaluates dependencies, supplier assurance, contractual resilience, and propagation risk across vendor and platform ecosystems.

CRT Controls:

CRT-C-0025, CRT-C-0026, CRT-C-0027, CRT-C-0028, CRT-C-0029, CRT-C-0030

Control Families / Series:

Supply-Chain Risk

CRT Modules (illustrative touchpoints):

🛰️ **Supply Chain Exposure Scanner**

🎛️ **Programme Builder Export** (third-party questionnaire, vendor risk summary, risk brief snapshots)

CRT-G-06 — Behavioural and Human

Reinforces resilience through awareness, simulation, cultural feedback loops, and behavioural mechanisms influencing system exposure.

CRT Controls:

CRT-C-0031, CRT-C-0032, CRT-C-0033, CRT-C-0034, CRT-C-0035, CRT-C-0036

Control Families / Series:

Human Factors

CRT Modules (illustrative touchpoints):

🎛️ **Programme Builder Export** (awareness script/training outline, audit checklist, exception register, continuous control narrative)

📂 **Structural Controls & Frameworks** (Org Governance Profile + governance setup context that shapes behavioural governance artefacts)

CRT-G-07 — Regulatory and Framework Alignment

Defines compliance pathways, jurisdictional overlays, oversight requirements, and governance-aligned policy structures.

CRT Controls:

CRT-C-0037, CRT-C-0038, CRT-C-0039, CRT-C-0040, CRT-C-0041, CRT-C-0042

Control Families / Series:

Governance and Compliance

CRT Modules (illustrative touchpoints):

📁 **Structural Controls & Frameworks**

Org Governance Profile (Org & Scope)

Governance Setup (Framework Onboarding)

Operational Extensions (Org-Specific)

Mapping Explorer

🎛️ **Programme Builder Export** (policy document, standard, audit checklist, risk brief/ register snapshot)

CRT-G-08 — Emerging Technologies and Systemic Risks

Addresses systemic risk arising from emerging technologies, automation, AI-driven dependency structures, and concentration risk across digital ecosystems.

CRT Controls:

CRT-C-0043, CRT-C-0044, CRT-C-0045, CRT-C-0046, CRT-C-0063, CRT-C-0064, CRT-C-0047, CRT-C-0048

Control Families / Series:

Emerging Technologies

CRT Modules (illustrative touchpoints):

🎛️ **Programme Builder Export** (AI risk controls as governance/architecture/metrics artefacts)

🔄 **System Integrator** Hub (integration risk, dependency coherence, emergent coupling)

📚 **Reference Data & Trusted Sources** (framework anchors, taxonomies, external reference constraints)

CRT-G-09 — Crisis, Monitoring, and Response

Coordinates detection, triage, containment, and system recovery, supported by telemetry and structural signal aggregation.

CRT Controls:

CRT-C-0049, CRT-C-0050, CRT-C-0051, CRT-C-0052, CRT-C-0053, CRT-C-0054, CRT-C-0061

Control Families / Series:

Incident Response, Monitoring and Telemetry

CRT Modules (illustrative touchpoints):

📡 **Telemetry Signal Console** (monitoring surfaces, detection lag context)

🎛️ **Programme Builder Export** (Incident response playbook, Scenario analysis summary, “What if” structural simulation brief, Resilience metrics brief / coverage-gap overview)

CRT-G-10 — Physical and Environmental Security

Protects physical facilities, environmental controls, and operational conditions underpinning digital infrastructure.

CRT Controls:

CRT-C-0055, CRT-C-0056, CRT-C-0057, CRT-C-0058, CRT-C-0059, CRT-C-0060, CRT-C-0062

Control Families / Series:

Physical Security

CRT Modules (illustrative touchpoints):

🧩 **Attack Surface Mapper** (facilities, environment exposure types, entry points where modelled)

🎛️ **Programme Builder Export** (governance / architecture artefacts where physical constraints matter)

End of Reference — Version Note

This reference concludes the current edition of the Cyber Resilience Toolkit (CRT) — Unified Index & Glossary Reference.

It represents a static snapshot of the systems terminology and integration logic as of publication date.

For live updates, additional definitions, and expanded data mappings, visit:
blakewiltshire.com

Future revisions may align with new releases of the Cyber Resilience in the Information Age volume, system enhancements within the Cyber Resilience Toolkit, or architectural updates to the underlying data registries and YAML index schema.

This marks the end of the current reference volume.

All subsequent updates, change logs, and extended glossaries are maintained within the CRT ecosystem.

This reference will evolve in step with CRT catalogue updates and companion datasets released through the online registry.

Prepared and published by Blake Media Ltd., United Kingdom — 2026 Edition