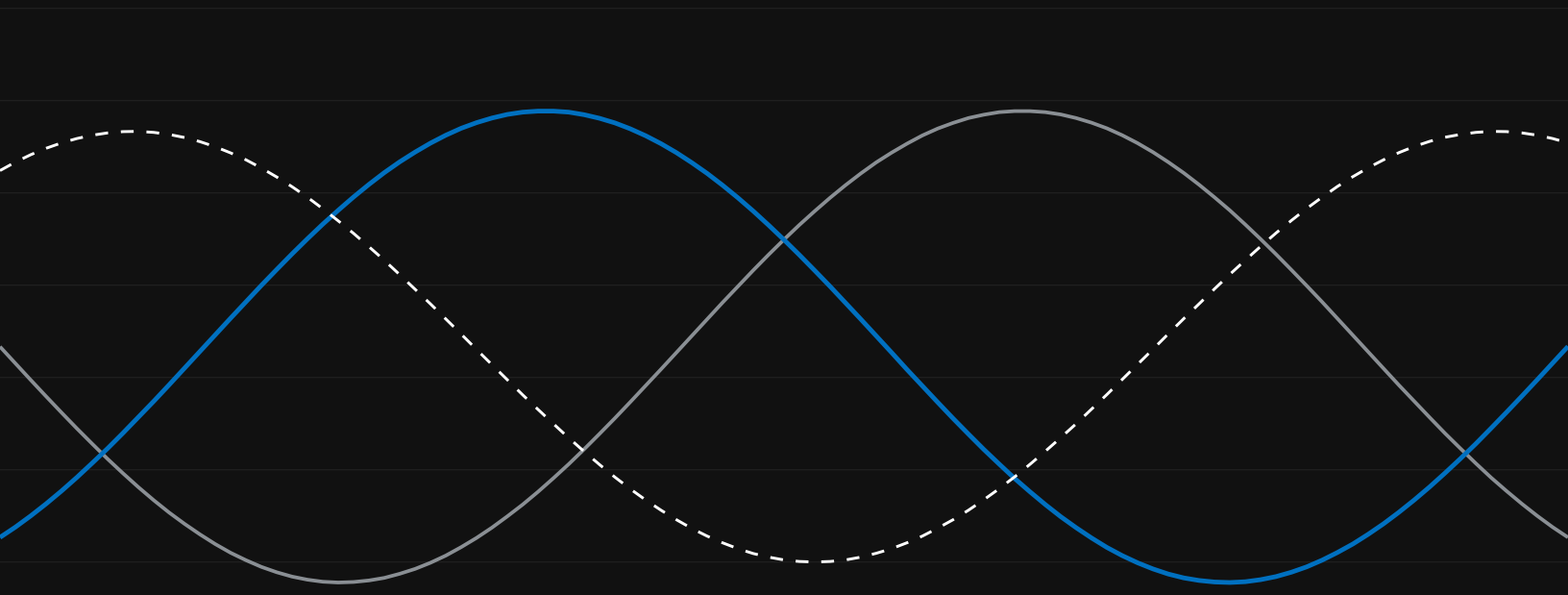
Module 05 · Workbook · Student edition

Adversary Management

The method behind the Day-5 resilience measures, and every measure it produced, each protecting the one element its threat names.



Copyright and legal notices

© 2026 ethicallyHackingspace (eHs)®. All rights reserved.

> **Printing.** To save toner, print from page 2. The cover is a dark full-page plate and carries nothing the pages after it do not.

TLP:AMBER. Limited disclosure. Recipients may share this document only within their own organization and its clients, on a need-to-know basis, and only to the extent necessary to act on the information.

This document is part of the Full Spectrum Space Cybersecurity Professional program. It is provided to enrolled learners and to the credentialing bodies it is submitted to. Sharing beyond what that marking permits, and any resale, is not authorized.

Verbatim sources. Every taxonomy definition quoted in this document is the published METEORSTORM taxonomy text, quoted exactly and never abbreviated, paraphrased or reworded. Where the course explains an element in its own words, the explanation is not presented as the definition. One typographical error in the published file, a doubled period, is corrected.

Trademarks. ethicallyHackingspace (eHs)® is the copyright holder of this publication; D2 Team CORP is its publisher. Other names appearing in this document are the property of their respective owners and are used for identification only.

No warranty. This publication is provided for education. It is not legal, regulatory, or engineering advice for any specific system.

Publisher	D2 Team CORP, a 501(c)(3) nonprofit
Program	Full Spectrum Space Cybersecurity Professional
Document	Module 05 Adversary Management, module workbook, student edition
Edition	Student edition · revised 2026-11-19
Contact	www.d2teamcorp.org

Student edition

The teaching chapters and the complete worked deliverable.

What this document is and how to use it

What it is. The Module 05 workbook for Adversary Management, METEORSTORM Function 05: the method, taught once, and the complete worked result for Kestrel Orbital, the fictional satellite operator this course uses as its example.

How to use it. Read it beside the Module 05 lesson, then keep it as your reference for the method. The contents list every chapter and section with its page.

What goes with it. The Module 05 question set is a separate download; the answers to its questions are printed in it.

How to use this workbook

The Module 05 lesson on the course site runs in the order below. This workbook is the reference for every step. The lettered parts are worked on the lesson page, not in this workbook.

Story film	Master Adversary Management at Kestrel Orbital
Video 1	Four proposals, one budget
Video 2	Counting what recurs
Part A	Which element do the paths keep naming?
Video 3	Reading a measure record
Video 4	The measure that cannot be implemented
Part B and C	Assemble the measure records, then two drafts at the gate
Closing story film	The week at Kestrel Orbital: what it produced
Check	Check your understanding

Use this at work. Blank record sheets, for your own use, are in the METEORSTORM desk pack on the course downloads page.

© 2026 ethicallyHackingspace (eHs)®

Contents

CH 1 **The Day in One Page** 6

CH 2 **What Both Departments Bring to the Table** 7

The Owner field, and why it exists 7

CH 3 **The AN-RES Method, and the Twin** 8

Choosing among the four goals 9

Where the element sits in its life, and what the measure can therefore be 10

The digital twin 12

Why this is a repeatable process 13

CH 4 **The Catalog, Complete** 13

CH 5 **The Week in Hand** 22

The five sets 22

One ordinal, all five functions 23

What recurs, and what to protect next 24

Your role across the week 25

CH 6 **Tag and Share** 25

CH 7 **Use This at Work** 26

Ten things to do at your work center 26

Desk pack sheets for Function 05 28

Where the method is in this workbook 28

What you will be able to do

We will be looking at resilience engineering so you can turn a week of accumulated analysis into changes to the platform.

O1	State why hardening chosen by conviction cannot be defended
O2	Choose the element to protect by counting recurrence across the chain
O3	Write a measure with one TRE, one goal, an owner and a cadence
O4	State the Day 5 rulings on dual control and the next-build gap
O5	Read a measure in MISP and the element it protects

The detail behind those objectives:

KNOWLEDGE

K1	A resilience measure is a forward-looking change of posture, not an observation and not a detection. It states what the organization will do differently.

© 2026 ethicallyHackingspace (eHs)®

K2	The TRE holds exactly one enumerated platform element, and it is the element the AN-THR the measure counters names as its TOE. There is no chain in the field and no primary among several.
K3	A target may name an element in any structural layer, PCE included. What is fixed is one element, at the lowest layer the source resolves.
K4	Every measure serves one of the four cyber-resiliency goals of NIST SP 800-160 Volume 2: Anticipate, Withstand, Recover, Adapt.
K5	Measures are enumerated prospectively, before they are exercised. That is what makes completeness auditable: each path carries a measure or a consciously accepted residual risk.
K6	Ownership is part of the element. A measure recorded as Both must name the split, because a measure owned by everyone is owned by no one.
K7	The lifecycle of the protected element decides what the measure can be: reachable applies to the element directly, through requires a compensating control on the path to it, and fixed makes the measure a requirement for the next build.
K8	The cadence records what the organization holds today, in-force, phased or next-build, and anything not in force must name a compensating control or a recorded residual risk, because coverage you cannot implement is not coverage.

SKILLS

S1	Inherit the TRE from the driving threat rather than choosing a fresh element, and say where the anchor came from.
S2	Write the reach a measure buys into the description, so protection is never mistaken for a second target.
S3	Choose the resiliency goal by what the measure changes about the attack, and defend the choice against the competing reading.
S4	Design a digital-twin run that would validate a measure, including the trade-off measured and the result that would reject it.
S5	Split a two-department measure into the architectural half and the procedural half, and name an owner for each.
S6	Read the accumulated sets for recurrence, and justify what to protect next by counting rather than by severity.
S7	Run the lifecycle test on the protected element before writing the measure, and record which of reachable, through or fixed it is together with the fact about the platform that decides it.
S8	Write a compensating control that names the element it is applied to and says what it does not buy, and a residual risk that names its owner and what closes it.

ABILITIES

A1	Take an uncountered attack path and produce a measure another operator can adopt without re-deriving the reasoning.
A2	Reject a proposed measure that restates a detection, names an aspiration, or carries no goal, and say precisely which rule it breaks.
A3	Hold a resilience decision to evidence in a room where two of the departments would each rather the other carried the cost.
A4	Say plainly that a measure cannot be implemented on the element it protects, and hold the entry open with a compensating control and a residual risk rather than letting the catalog read as covered.

TASKS

T1	Produce resilience measures whose TRE holds one inherited element and whose reach is written as description.
T2	Produce the goal, counters, owner split and source on every measure, so the set can be reviewed for balance and defended later.
T3	Record the residual risk where a path carries no measure, rather than leaving the path silently uncountered.
T4	Record the lifecycle and the cadence on every measure, and where the cadence is not in force, the compensating control and the residual risk that stand in its place.

© 2026 ethicallyHackingspace (eHs)®

Part I **Orientation**

What the module produces, and what each department brings to the table before any of it can be written.

CH 1 The Day in One Page

Four days in, the platform has a decomposition, a threat catalog, an attack-path map, and a detection portfolio with playbooks. Today both operating departments hold the pen together, because resilience needs operating procedures and architectural change at the same time, and neither department can commit the other.

Why resilience comes last. Not because it matters least, but because it needs the accumulated set to be useful. Only after Functions 02, 03, and 04 can you see which platform elements keep recurring: the elements that appear in the most threats, the most paths, and the most detections are where the adversary keeps having to go. Those are the elements worth spending money on. Run Function 05 first and you harden by intuition; run it last and you harden by evidence. On this first pass the count finds one element on two paths, **SVC:CP:Control Plane:09**, the ground command-acceptance service, and every other element on one. The four measures sit on the four anchors Day 2 fixed, and the count is run again as the catalog grows. Chapter 5 shows the count.

What you build. Four **AN-RES** elements: 2 Ground, 1 Link, 1 Space. Every one names one platform element it protects (TRE), the path or threat it counters, its resiliency goal, and the department that owns it. Every one also records where the protected element sits in its life and the cadence the measure actually holds at, because two of these four cannot be implemented on the element they protect today. Chapter 4 prints the whole deliverable.

The chain, closed. One chain is one number carried across the week, and Day 5 is where the chain closes. Day 2 anchored **AN:THR:Threat:00** to **SVC:CP:Control Plane:09**, the ground command-acceptance service. Day 3 walked **AN:ATT:Attack Path:00** to that same element, Day 4 watched it with **AN:DET:Detection Signature:00**, and today **AN:RES:Resilience Measure:00** hardens it. Threat, path, signature and measure all carry ordinal 00 and all name that one element. Every entry in chapter 4 works the same way.

The Owner field. Every measure names the department that carries it. A measure that is an operating procedure belongs to Satellite Operations. A measure that is an architectural change belongs to Satellite Design and Engineering. Most belong to both, and the split is written out, because a measure owned by everyone is owned by no one.

What the week ends with. A working decomposition, an anchored threat set, an attack-path set, a signature and playbook set, and a resilience-measure set, all against the same reference platform and all in the same five-field language. Chapter 5 shows the five sets as one artifact and walks a single ordinal through all of them.

© 2026 ethicallyHackingspace (eHs)®

CH 2 What Both Departments Bring to the Table

> "All three claims are defensible, and no evidence on the table ranks them. Nothing counts which element the week's own work keeps naming."

Days 2 to 4 each had one department holding the pen: the Security Operations Center (SOC) on Day 2, Satellite Design and Engineering on Day 3, the SOC again on Day 4. Day 5 is the only analytic session with two, and the reason is structural rather than ceremonial. A resilience measure almost always has two halves: something must be built, and something must be done differently every day thereafter. Dual-control commanding is a workflow in the commanding software and a discipline on the operations floor. Frequency agility is a waveform capability and a band-switching procedure. Commit only one half and the measure does not hold.

The Owner field, and why it exists

Owner value	What it means	Example from this catalog
Satellite Design and Engineering	The measure is an architectural change: something is built, signed, or re-designed.	Measure 03, measured-boot architecture and signing pipeline
Satellite Operations	The measure is an operating procedure: something is done differently on every pass.	No measure in this set is owned by Satellite Operations alone; the discipline halves sit inside the Both entries
Both, with the split named	Two halves, each committed by its department, written out so neither can assume the other.	Measures 00, 01, and 02

> **The rule.** A measure recorded as Both must name the split. "Both" on its own is a measure nobody owns; "Satellite Design and Engineering builds the segmentation and dual-approval workflow, Satellite Operations holds the maintenance-window and peer-review discipline" is a measure two people can be held to.

© 2026 ethicallyHackingspace (eHs)®

Part II **The method and the catalog**

The process for producing one entry correctly, then the complete catalog it produced, entry by entry.

CH 3 The AN-RES Method, and the Twin

> "Hardening by evidence is the only version that can be defended when the budget is questioned. Recurrence is countable because every entry anchors to exactly one element."

Inputs. The week's attack-path and threat sets against the telecommand path, and a working session with Satellite Operations and Satellite Design and Engineering. Two mandate texts frame the session. NIS2 Article 21(2) lists among its measures "(c) business continuity, such as backup management and disaster recovery, and crisis management" and "(d) supply chain security". Executive Order 14144, Sec. 3(c) as amended by Executive Order 14306, sets requirements for "protection of command and control of the civil space system, including backup or failover systems": the backup or failover systems are named as things to protect. Of the four measures in chapter 4, Measure 03 carries supply-chain provenance verification. None of the four is a backup-management, disaster-recovery or failover measure, and the Recover goal is carried by the Day-4 playbooks rather than by a measure in this set.

Output. One AN-RES element per measure, each anchored via TRE to the one platform element it protects. Its identifier is the five-field ETEN Module 01 taught, LAYER:TAG:LABEL:ORDINAL:Description, with SOURCE added and the TRE standing where a structural element carries its PARENT.

The published definition. The METEORSTORM taxonomy defines AN-RES, Resilience Measure, as: "Validated and operational protective capability ensuring converged space system resistance or recovery from confirmed threats." An AN-RES entry may be enumerated prospectively: the method below writes a measure before it is exercised, so an entry in chapter 4 is written before the measure is validated and operational. The cadence, with the compensating control and the residual risk, is the record of how far the entry is from validated and operational, and a phased or next-build entry is not presented here as already meeting the definition.

> **The constraint.** Every element carries exactly one TRE element, names its resiliency goal and names its owner. A measure with no target, no goal or no owner is decoration, not resilience. The TRE may name an element in **any** structural layer, PCE included: what is fixed is that it holds one element, at the lowest layer the source resolves, and that it is the element the AN-THR this measure counters already names as its TOE. Every element also declares the lifecycle of the element it protects and the cadence the measure holds at, because a measure that cannot be implemented is not a control in force.

© 2026 ethicallyHackingspace (eHs)®

The six steps, fixed order

1. **Enumerate the LAYER.** LAYER = AN, fixed. A resilience measure is a decision about the platform, not a part of it.
2. **Identify the resiliency goal.** One of Anticipate, Withstand, Recover, or Adapt, per NIST SP 800-160 Volume 2. SOURCE takes exactly two values, **observable** or **synthetic**, declared at the gate and stamped on the entry; the report, guidance or engineering source behind the measure is cited in the description, never in SOURCE. Measures are enumerated **prospectively**, before they are exercised, which is what makes completeness auditable: a reviewer walks the attack paths and checks that each has a corresponding measure or a consciously accepted residual risk.
3. **Set the TAG to RES.** A Resilience-Measure element within the Analytic Layer.
4. **Assign an ORDINAL.** Two digits from 00, one per distinct measure. Each measure keeps the ordinal of the chain it closes, so this week's four are 00, 01, 02, 03. An ordinal is issued once and never renumbered.
5. **Enumerate the TRE.** Target of Resilience Enhancement: **one** enumerated platform element the measure protects, and it is the same element the AN-THR this measure counters names as its TOE. AN-RES uses TRE, not TOE or TDM: the element made more resilient, not the element exploited or the element scanned. One element, never a list, and never a "primary" among several. The wider chain the protection reaches is written in the description. Then run the **lifecycle test** on that element, below, because where it sits in its life decides whether the measure can be implemented on it at all.
6. **Write the DESCRIPTION.** The measure, the resiliency goal it serves, the AN-ATT or AN-THR elements it counters, and the source citation: internal engineering, control-framework guidance, a peer-shared pattern, or a post-incident lesson. Record the **cadence** the measure actually holds at, and where that cadence is not in force, the compensating control or the residual risk that stands in its place.

Repeat for the next measure. When every enumerated path carries a measure or a recorded residual risk, the AN-RES enumeration is current.

> **Why one element and not a list.** A field holding two elements cannot say which one the entry is about. Two later readers act on that field: an auditor asks whether the path is countered, and an engineer asks what to change. Give them two elements and they answer different questions from the same record. The reach is real and it belongs in the description, where it can be read as reach rather than mistaken for a second target.

Choosing among the four goals

The four cyber-resiliency goals come from NIST SP 800-160 Volume 2, and every AN-RES serves exactly one of them. NIST SP 800-160 Volume 2 defines the four goals: Anticipate, "maintain a state of informed preparedness for adversity"; Withstand, "continue essential mission or business functions despite adversity"; Recover, "restore mission or business functions during

© 2026 ethicallyHackingspace (eHs)®

and after adversity"; Adapt, "modify mission or business functions and/or supporting capabilities in response to predicted changes in the technical, operational, or threat environments." The test column below is this course's working test for choosing among them, not the publication's wording.

Choose by what the measure changes about the attack, not by how important it feels:

Goal	Test	In this catalog
Anticipate	It removes the opportunity before the adversary acts.	Measures 00 and 03
Withstand	The mission continues while the attack is under way.	Measures 01 and 02
Recover	It restores a known-good state afterwards.	Carried by the Day-4 playbooks rather than by a measure in this set
Adapt	It changes the platform so the same path does not work twice.	Not in this set; the honest reading of a four-measure catalog

The same measure can be argued into two goals, and that argument is worth having, because the goal determines how the measure is later reviewed for effectiveness. An Anticipate measure is reviewed by asking whether the opportunity is still closed; a Withstand measure by asking whether the mission still runs under load. Record the goal you can defend, and record why.

Where the element sits in its life, and what the measure can therefore be

The TRE says what a measure protects. It does not say what you are allowed to change. Those are two different questions, and the second one has a test of its own, because a measure protects an element but cannot always be implemented *on* that element. Measured boot cannot be implemented on boot firmware that is already in orbit. A waveform lives in a radio that is already flying. A ground service can be rebuilt this quarter. Same catalog, three different kinds of measure, and until you say which is which they all read the same on the page.

The lifecycle test. Ask where the protected element sits in its life. The answer decides what the measure can be.

Lifecycle	The protected element	So the measure is
reachable	Changeable now.	Applied to the element directly.
through	Fixed in itself, but reachable through something you do control.	A **compensating control** on the path to it.
fixed	Fixed for its service life.	A requirement for the **next build**. It cannot be implemented on what is flying.

© 2026 ethicallyHackingspace (eHs)®

The cadence. The lifecycle is a fact about the element. The cadence is a statement about the organization: what it actually holds today, which is the thing an auditor, a regulator, and the next operator on shift all want to know.

Cadence	What the organization holds today
in-force	Implemented, or implementable this quarter.
phased	Part is implementable now, part belongs to the next build.
next-build	Cannot be implemented on the flying platform at all.

> **The rule that keeps the catalog honest.** Anything not in force must name a **compensating control** or a recorded **residual risk**. Coverage you cannot implement is not coverage. A compensating control names the element it is applied to. A residual risk names its owner and what closes it. Where the cadence is in force, both fields are empty, and that emptiness is a statement rather than an omission.

What a compensating control is, and what it is not. It is not a weaker version of the measure and it is not a promise to build one. It is a control you can implement today, placed on something you do control, chosen because the adversary has to cross it to reach the element you cannot change. It buys distance, not trust. Saying so plainly is the point: a compensating control written as though it hardened the protected element re-creates exactly the false reading the lifecycle test exists to prevent.

Worked case: measure 03, where the catalog read as covered and nothing was implemented

AN:RES:Resilience Measure:03 specifies supply-chain provenance verification **at integration**, and its TRE is **AST:FW:Firmware:01**, the on-board computer boot firmware. That vehicle is in orbit. Integration happened before launch. The measure cannot be implemented on the element it protects: the lifecycle is **fixed** and the cadence is **next-build**.

The second half is worse. The paired signature AN:DET:Detection Signature:03 cannot fire either, because Function 03 recorded its required source as a **Gap**. So against the one threat that reaches the flight computer, Kestrel holds nothing today: no control on the element, and no visibility of it. Before these fields existed, this entry read on the page exactly like measures 00 and 01, whose cadence is in-force. That is the failure the cadence field exists to prevent. A catalog that reads as covered where nothing is implemented is worse than one that admits the gap, because it stops anyone looking.

The compensating control, recorded on the entry. Measured boot cannot be implemented on **AST:FW:Firmware:01** in orbit, so the flight firmware is protected from the ground instead: dual approval on every image entering the patch deployment pipeline **AST:SW:Software:03**, provenance verification before staging, and a hold on any push outside a window on **SVC:CP:Control Plane:12**. The dual approval and the window hold are the firmware-push gate of AN:RES:Resilience Measure:00, under that measure's owner split and cadence. This does not make the flight firmware trustworthy; it makes it harder to reach. That sentence is part of the record, not a caveat on it: harden what the adversary must cross, and say what you have not fixed.

The residual risk, recorded with its owner. The flying vehicle carries no boot-time attestation and its signature AN:DET:Detection Signature:03 cannot fire. A tampered image that reaches the on-board computer is undetected on orbit. Owner: Satellite Design and Engineering, closed by measured boot on the next build.

© 2026 ethicallyHackingspace (eHs)®

Nothing else about the entry moves: same ordinal, same TRE, same goal, same owner. What changes is that a reader can now tell a measure recorded in-force from a measure waiting on the next build.

Worked case: measure 02, one record with two lifecycles

AN:RES:Resilience Measure:02 bundles two things. The pre-arranged backup band and the automatic switching threshold are configuration and procedure, and Satellite Operations can adopt them now. The frequency-agile spread-spectrum waveform is not: the entry itself assigns it to Satellite Design and Engineering, and it lives in the radio of a spacecraft that is already flying. One record, two lifecycles, which is why the lifecycle reads **through** and the cadence reads **phased**.

The compensating control. The pre-arranged backup band and the automatic switching threshold are implementable now on **SVC:HY:Hybrid:02**, and carry the measure until the agile waveform flies. Satellite Operations owns the procedure.

The residual risk. Until a frequency-agile spread-spectrum waveform flies, the link can be denied faster than a band switch can be authorized. Owner: Satellite Design and Engineering, for the next spacecraft.

> **Why this is one record and not two.** The chain requires exactly one measure per ordinal: threat, path, signature and measure all carry 02 and all name **AST:SI:Signal:00**. Splitting the measure into an operations entry and an engineering entry would put two measures on one ordinal and break the property the whole week rests on. The two lifecycles are expressed where they belong, in the cadence, the compensating control and the residual risk, so a reader sees one measure and can still tell which half is implementable now.

And the two that need neither field. Measures 00 and 01 protect elements that are reachable now, a ground control-plane service and the console operator software, so their lifecycle is **reachable**, their cadence is **in-force**, and they carry no compensating control and no residual risk. Read the four entries together and the catalog says out loud what it holds: two measures in-force, one phased, one next-build. In-force keeps the meaning the cadence table gives it, implemented, or implementable this quarter; the entry does not say which of the two, and under the Day 5 ruling nothing reaches the platform before the digital twin.

The digital twin

A digital twin is a high-fidelity virtual replica of the operational system, pairing flight software, simulated subsystems, and an RF-environment model so a candidate measure runs end to end in simulation. Every AN-RES measure changes how the platform behaves under stress, so the twin is where measures are validated, adversary scenarios rehearsed, and trade-offs quantified before a measure is accepted into the design. The twin is not one of the 44 elements of the Day-1 decomposition; it is the test bench a measure is tried on before it touches the platform. Satellite Operations runs the twin campaigns, and the Security Operations Center confirms that the detections still fire. A twin run is not shared with Space ISAC members.

The ruling, stated in the Module 05 story film, is that nothing touches the flying platform until it has been applied to the digital twin. Here is what a twin run looks like for measure 02, so the ruling becomes a method you can run.

© 2026 ethicallyHackingspace (eHs)®

Twin run · validating AN:RES:Resilience Measure:02, frequency-agile link

Question: does automatic band-switching keep the command link usable under the jamming profile of AN:ATT:Attack Path:02, and what does it cost?
Scenario: replay the chain-02 profile against the twin: sustained noise injection across the primary uplink band, timed to an overhead pass, run twice, once with the measure applied and once without.
Without the measure: noise floor crosses the threshold, the link degrades then loses lock, and the command window is lost for the remainder of the pass. Commanding waits for the next contact.
With the measure: the switch fires at threshold and commanding continues on the backup band for the remainder of the pass, at reduced throughput.
The cost, quantified: the twin shows the second-order effects of the measure on mission capability, duty cycle, downlink margin and power budget while it is active. That is the trade-off curve, and it is why this is an engineering decision rather than an obvious yes.
The abuse case, also run: an adversary who learns the threshold could deliberately trip it to herd the platform onto the weaker band at will. The threshold logic is exercised against exactly that abuse on the twin before it flies.
Rejection criterion: if the measure cannot hold the command link through the simulated attack, or if the duty-cycle cost breaks the mission profile, it is rejected on the evidence rather than on argument.

Every measure in chapter 4 carries the twin question it would be validated by, so this pattern generalizes rather than sitting as a single example.

Why this is a repeatable process

CNSSI 1200 (August 2025), which implements CNSSP No. 12, requires a hardware root of trust for secure boot on space platforms. Compliance is not one-and-done: under FISMA and the NIST Risk Management Framework (SP 800-37 Rev. 2), a subset of security controls must be assessed at least annually. That is why resilience is a repeatable, cross-organizational process rather than a one-time fix, and why the resilience set is explicitly a living artifact: as the architecture, the attack-path set, and the adversary evolve, the set evolves with them. (Sources: CNSSI 1200, August 2025; NIST SP 800-37 Rev. 2.) CNSS policy binds national security systems and FISMA binds federal systems. Kestrel Orbital is neither; both are cited for the discipline they model, a measure reassessed on a cycle, not as duties on Kestrel.

CH 4 The Catalog, Complete

> “Every measure names the one platform element it protects, the threat or attack path it counters, the resiliency goal, and the department that owns it.”

How to read each entry. The first row is the anchor: the one element the TRE names, inherited from the AN-THR this measure counters. Everything under it is the record a department acts on. The lifecycle and cadence rows answer the question chapter 3 taught, whether the measure can be implemented on the element it protects and what the organization

© 2026 ethicallyHackingspace (eHs)®

holds today, and where the cadence is not in force the next two rows carry the compensating control and the residual risk. The reach paragraph after each table lists the further elements the protection touches, printed so the difference between the anchor and the reach is visible; the anchor figure draws the anchor and leaves the reach to that paragraph. The twin question is what the measure would be validated by before it is accepted.

GROUND · 2 AN-RES

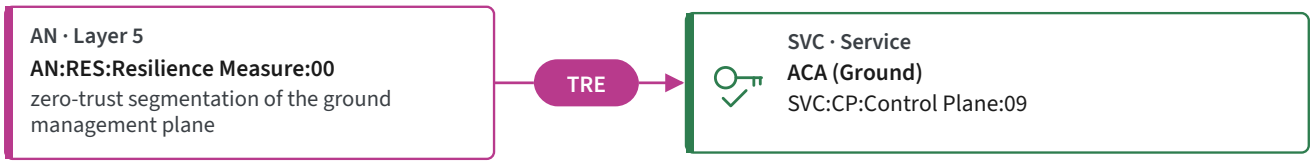
AN:RES:Resilience Measure:00 · Zero-trust segmentation of the ground management plane

Strict zero-trust segmentation of the ground management plane from external networks; require hardware-rooted attestation on any management-plane access; gate firmware pushes behind dual-approval workflow with a maintenance-window enforcement.

Field	Value
TRE (anchor)	**SVC:CP:Control Plane:09**
What that is	The ground command-acceptance service. The one element this measure protects, taken from AN:THR:Threat:00. Day 3 walked to it and Day 4 watches it.
Counters	AN:ATT:Attack Path:00 · AN:THR:Threat:00
Goal	**Anticipate: it removes the high-impact path entirely by raising the barrier to management-plane access**
Owner	Both. Satellite Design and Engineering owns the segmentation and dual-approval rebuild; Satellite Operations owns the maintenance-window discipline.
Lifecycle	**reachable**. The ground command-acceptance service can be changed now, so the measure is applied to the element itself.
Cadence	**in-force**. Implemented, or implementable this quarter.
Compensating control	None, and none needed. The cadence is in force, so nothing is standing in for this measure.
Residual risk	None recorded. The cadence is in force, so the field is empty.
SOURCE	observable
Source citation	NIST SP 800-207 (Zero Trust Architecture)
Twin question	Does an operator still complete a legitimate emergency firmware push inside the dual-approval workflow within the pass window, and what does the added latency cost?

© 2026 ethicallyHackingspace (eHs)®

Figure 1 AN-RES anchors · 1 of 4 entries · after AN:RES:Resilience Measure:00



One measure, one anchor. The measure sits in Layer 5 and names one platform element through its **TRE** field. What the segmentation additionally shields is in the reach paragraph below, not in this figure, because the reach is description and the anchor is the target.

Why this looks like the Module 02 figure. It is the same figure with a different tag. That is the point of the chain: AN:RES:Resilience Measure:00 names the element AN:THR:Threat:00 named, so the element on the right has not moved all week.

Reach behind the anchor. Segmenting the management plane also shields the ground crypto service (**SVC:CP:Control Plane:08**), the patch deployment pipeline (**AST:SW:Software:03**) and the patch binaries (**AST:DA:Data:02**), because the route to all three ran through the management plane. None of those is a second TRE. They are what the anchor buys, and they belong in this paragraph so a reader can tell protection from target.

> **Field note**
>
> Both ground measures need both departments, and a measure owned by everyone is owned by no one. Ruling: Owner is recorded as Both, with the split named. Satellite Design and Engineering builds the segmentation and the dual-control workflow; Satellite Operations holds the maintenance-window and peer-review discipline. First win: every ground measure now names the department that carries each half, so nothing waits on an unnamed owner.

© 2026 ethicallyHackingspace (eHs)®

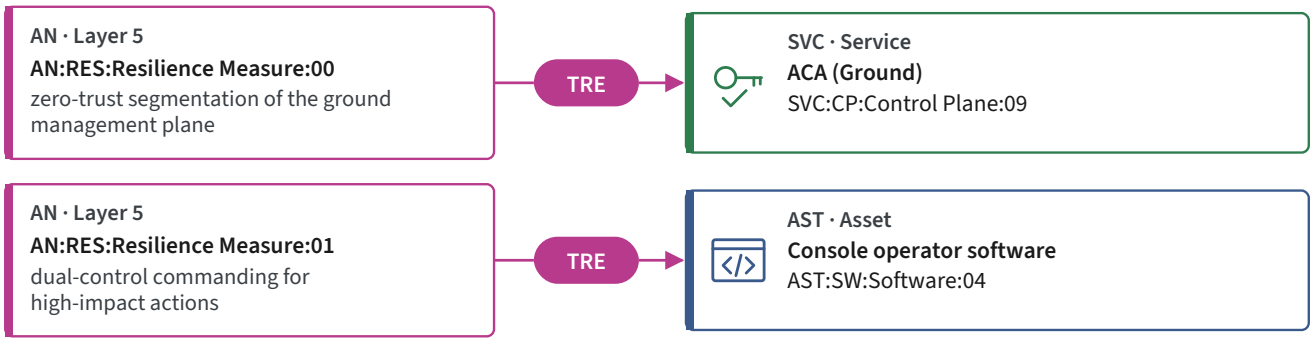
AN:RES:Resilience Measure:01 · Dual-control commanding for high-impact actions

Dual-control commanding for high-impact actions (a second operator must approve before transmission); role and shift baselines and pre-pass briefings make out-of-pattern actions stand out.

Field	Value
TRE (anchor)	**AST:SW:Software:04**
What that is	The console operator software. The one element this measure protects, taken from **AN:THR:Threat:01**. Day 3 walked to it and Day 4 watches it.
Counters	**AN:ATT:Attack Path:01 · AN:THR:Threat:01**
Goal	**Withstand: high-impact commanding continues safely while a credential is compromised, because one credential alone cannot release a high-impact sequence**
Owner	Both. Satellite Design and Engineering owns the dual-control workflow in the commanding software; Satellite Operations owns the operational discipline of peer review.
Lifecycle	**reachable**. The console operator software can be changed now, so the approval gate is built into the element itself.
Cadence	**in-force**. Implemented, or implementable this quarter.
Compensating control	None, and none needed. The cadence is in force.
Residual risk	None recorded. The cadence is in force, so the field is empty.
SOURCE	observable
Source citation	NIST SP 800-53 AC-5 and AC-6 (separation of duties, least privilege); NIST SP 800-160 v2 withstand-goal guidance
Twin question	Under a time-critical anomaly, does dual control delay a legitimate recovery command past the point of safety? If it does, the measure needs a defined break-glass path, itself audited.

© 2026 ethicallyHackingspace (eHs)®

Figure 2 AN-RES anchors · 2 of 4 entries · after AN:RES:Resilience Measure:01



The second measure anchors to an asset, so its card reads AST · Asset, in the asset color. Two measures, two structural layers, and in both cases the anchor was inherited rather than chosen.

What you do not choose. The anchor is not an authoring decision on Day 5. It was fixed on Day 2. If you find yourself picking a different element, either the measure counters a different threat than you think, or the threat was anchored wrong, and that is a Day 2 defect to raise rather than a Day 5 workaround.

Reach behind the anchor. Dual control also constrains the operator console (**AST:HW:Hardware:04**), the Satellite Console service (**SVC:CP:Control Plane:13**) and the ground command-acceptance service (**SVC:CP:Control Plane:09**), since the approval gate sits between the operator and all three. The TRE still names one element: the console software, where the gate is built.

Note the feedback loop. This measure is also what turns Day 4's Signature 01 from Partial to something stronger: the peer-review tag stream that the signature depends on is produced by the dual-control workflow this measure builds. Function 05 is not only defending against the adversary, it is closing the dependencies Function 04 had to declare.

© 2026 ethicallyHackingspace (eHs)®

LINK · 1 AN-RES

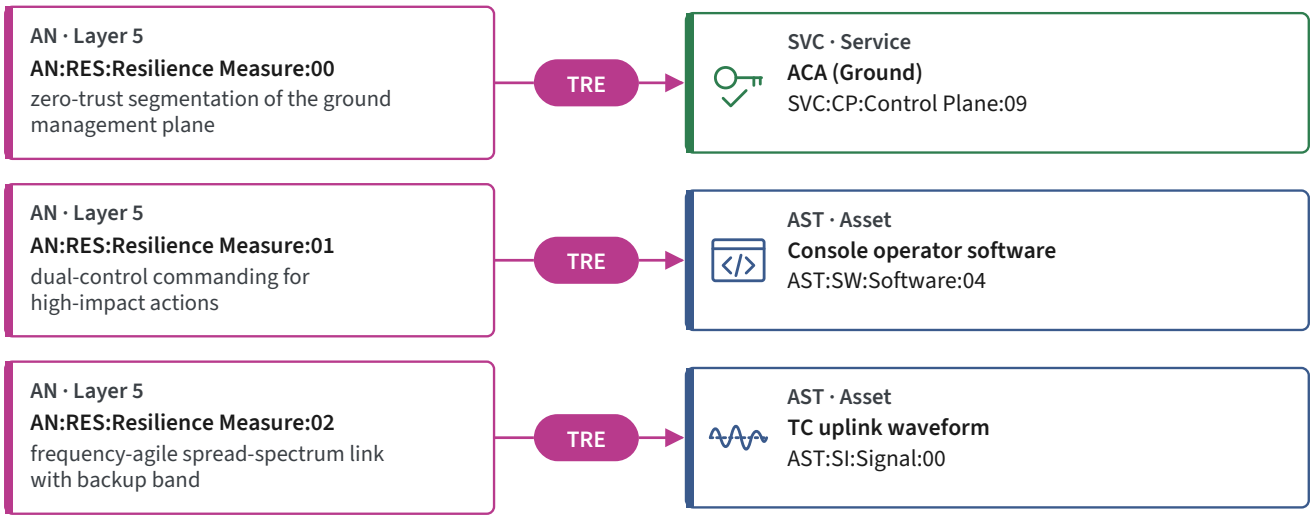
AN:RES:Resilience Measure:02 · Frequency-agile spread-spectrum link with backup band

Frequency-agile / spread-spectrum link operation with pre-arranged backup band; the spacecraft command receiver and the Kiruna ground terminal switch to the pre-arranged backup band automatically when the noise floor exceeds threshold, under a band-switching procedure Satellite Operations owns; Satellite Design & Engineering owns the agility waveform.

Field	Value
TRE (anchor)	**AST:SI:Signal:00**
What that is	The telecommand uplink waveform. The one element this measure protects, taken from AN:THR:Threat:02. Day 3 walked to it and Day 4 watches it.
Counters	AN:ATT:Attack Path:02 · AN:THR:Threat:02
Goal	**Withstand: communications continue under sustained interference**
Owner	Both. Satellite Design and Engineering owns the frequency-agile waveform implementation; Satellite Operations owns the band-switching procedure.
Lifecycle	**through**. The waveforms live in a radio that is already flying, so the measure reaches them through the band plan and the switching procedure the ground does control.
Cadence	**phased**. The backup band is adoptable now; the frequency-agile waveform belongs to the next build.
Compensating control	The pre-arranged backup band and the automatic switching threshold are implementable now on **SVC:HY:Hybrid:02**, and carry the measure until the agile waveform flies. Satellite Operations owns the procedure.
Residual risk	Until a frequency-agile spread-spectrum waveform flies, the link can be denied faster than a band switch can be authorized. Owner: Satellite Design and Engineering, for the next spacecraft.
SOURCE	observable
Source citation	ITU interference-mitigation guidance; SPARTA EX-0016 (Jamming) mitigation patterns
Twin question	The worked run in chapter 3: does the link hold under the chain-02 jamming profile, at what duty-cycle and downlink cost, and can an adversary herd the platform by tripping the threshold?

© 2026 ethicallyHackingspace (eHs)®

Figure 3 AN-RES anchors · 3 of 4 entries · after AN:RES:Resilience Measure:02



The link measure joins. Its anchor is a signal asset, which is a reminder that the target layer follows the source rather than the segment: any structural layer may be named, PCE included, at the lowest layer the source resolves.

The measure is written before it is exercised. Nothing on this platform has yet run the agility waveform under a real jamming campaign. The measure is enumerated anyway, which is what makes coverage auditable: a reviewer walks the four paths and asks whether each carries a measure or an accepted residual risk, not whether each has already been tested.

Reach behind the anchor. Band agility also protects the link access control and authentication service (**SVC:CP:Control Plane:05**), the FEC and ECC service (**SVC:HY:Hybrid:01**) and the tracking and telemetry service (**SVC:HY:Hybrid:02**), all of which degrade with the waveform. The TRE names the waveform because that is the element the threat named.

> **Field note**
>
> Satellite Operations wanted the band switch automatic, at machine speed; Satellite Design and Engineering warned that an adversary who learns the threshold could herd the platform onto the backup band at will. Ruling: the switch stays automatic, and the threshold logic is exercised on the digital twin against exactly that abuse before it flies. First win: the jamming response is rehearsed in simulation rather than argued.

© 2026 ethicallyHackingspace (eHs)®

SPACE · 1 AN-RES

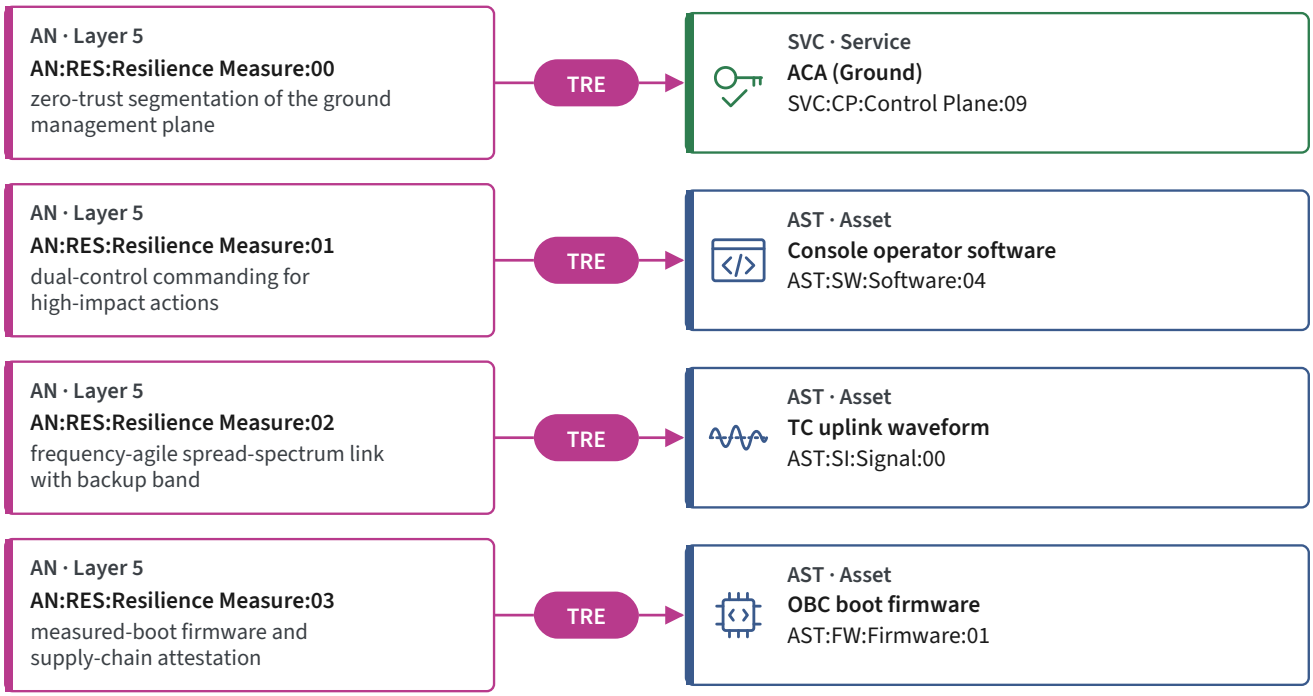
AN:RES:Resilience Measure:03 · Measured-boot firmware and supply-chain attestation

Measured-boot firmware attestation with signed-vendor manifest; supply-chain provenance verification at integration; quarantine of any component whose hash does not match the signed expected value.

Field	Value
TRE (anchor)	**AST:FW:Firmware:01**
What that is	The on-board computer boot firmware. The one element this measure protects, taken from AN:THR:Threat:03. Day 3 walked to it and recorded its required data source, the boot-time firmware measurement and attestation record, in state Gap; Day 4 rated Signature 03's coverage Gap on it.
Counters	AN:ATT:Attack Path:03 · AN:THR:Threat:03
Goal	**Anticipate: on the build that carries it, tampered firmware never reaches an operational role**
Owner	Satellite Design and Engineering, sole owner of the measured-boot architecture, the signing pipeline, and the supply-chain verification process.
Lifecycle	**fixed**. Measured boot cannot be implemented on the on-board computer boot firmware in orbit, and attestation specified at integration cannot be applied to a vehicle that has already launched.
Cadence	**next-build**. Nothing in this measure can be implemented on the flying platform.
Compensating control	Measured boot cannot be implemented on **AST:FW:Firmware:01** in orbit, so the flight firmware is protected from the ground instead: dual approval on every image entering the patch deployment pipeline **AST:SW:Software:03**, provenance verification before staging, and a hold on any push outside a window on **SVC:CP:Control Plane:12**. The dual approval and the window hold are the firmware-push gate of AN:RES:Resilience Measure:00, under that measure's owner split and cadence. This does not make the flight firmware trustworthy; it makes it harder to reach.
Residual risk	The flying vehicle carries no boot-time attestation and its signature AN:DET:Detection Signature:03 cannot fire. A tampered image that reaches the on-board computer is undetected on orbit. Owner: Satellite Design and Engineering, closed by measured boot on the next build.
SOURCE	observable
Source citation	NIST SP 800-193 (Platform Firmware Resilience); SLSA framework supply-chain guidance
Twin question	Does attestation reject a tampered image without also rejecting a legitimate emergency patch, and what is the recovery path if a valid image fails verification on orbit?

© 2026 ethicallyHackingspace (eHs)®

Figure 4 AN-RES anchors · 4 of 4 entries · the complete Day-5 resilience anchor map



Four measures, four anchors, and the same four elements Day 2 produced. This figure and the Module 02, 03 and 04 figures are identical on the right-hand side, which is what a working chain looks like at the end of a week.

What the chain bought. Four elements were named once in the Day 1 decomposition, anchored by the threats on Day 2, and carried through four functions without a single cross-reference table. An auditor holding ordinal 03 holds the threat, the route, the signature and the measure, and can ask the only question that matters: is this exposure countered, or is the residual risk accepted on the record?

Reach behind the anchor. The reach of this measure is the patch update service (**SVC:CP:Control Plane:12**), where Attack Path 03 enters and where the compensating control holds any push outside a window, and the C&DH service (**SVC:HY:Hybrid:00**), where the path pivots. None of those is a second TRE. The TRE names the on-board computer boot firmware because that is the element the threat named.

© 2026 ethicallyHackingspace (eHs)®

> **Field note**
>
> This measure was argued twice before Day 5: Day 3 recorded the required data source on this element, the boot-time firmware measurement and attestation record (**RDS:02** on Attack Path 03), in state Gap with Satellite Design and Engineering as owner, and Day 4 rated Signature 03's coverage Gap for the same reason. Ruling: Satellite Design and Engineering signs as sole owner of the measured-boot architecture, the signing pipeline, and the supply-chain verification. Second ruling, once the cadence was written down: the measure is **next-build**, so the entry carries the ground-side compensating control and the residual risk rather than reading as covered. First win: the next build that flies attestation arrives with Signature 03 already written, and on that vehicle the residual risk closes. On the vehicles flying today it stays recorded.

Part III **Putting it to work**

Who reads what you wrote, and how it is shared as machine-readable intelligence rather than a document a partner has to re-key.

CH 5 The Week in Hand

> "There are only two honest answers per attack path: a measure on its anchor element, or a recorded residual risk with an owner. Removing the third is the audit."

The five sets

Module	Function	Set	Size	Anchor field
01	F01 Concept of Operations	The CONOPS decomposition	44 elements (4 PCE, 4 SEG, 15 SVC, 21 AST)	PARENT
02	F02 Contextualized Threat Modeling	AN-THR threat catalog	4 (Ground 2, Link 1, Space 1)	TOE
03	F03 Converged Detection Engineering	AN-ATT attack paths	4, with 12 required sources (RDS and RSS)	TOE, one element, the same one the threat names
04	F04 Incident Response Preparation	AN-DET signatures plus playbooks	4 + 4	TDM, that same element
05	F05 Adversary Management	AN-RES resilience measures	4	TRE, that same element

Read the last column downward. From Function 02 onward the anchor field changes name and the element does not: TOE, TOE, TDM, TRE, all naming one thing. That is the chain, and it is why an ordinal is enough to hold a whole chain.

© 2026 ethicallyHackingspace (eHs)®

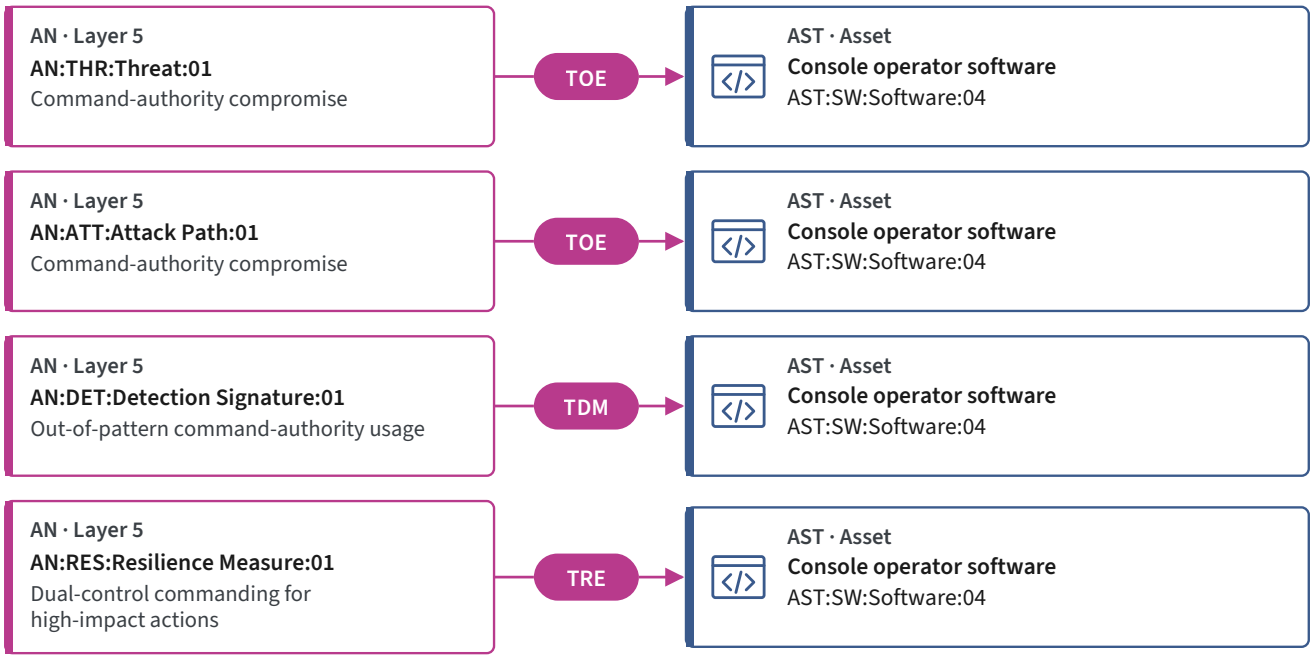
One ordinal, all five functions

The course claims that a single identifier chain runs through every function. Here it is for ordinal 01, in full:

Function	Element	What it added	Owner
F01	**AST:SW:Software:04**	The console operator software exists, is named once, and sits under the Satellite Console service, the Ground segment, and the Terrestrial environment.	SCOR, for all three departments, as the Day 1 CONOPS
F02	AN:THR:Threat:01	An adversary with stolen or coerced command authority would target it. TOE names that one element.	Security Operations
F03	AN:ATT:Attack Path:01	The route through it: console hardware, then the console software itself, then the ground command-acceptance service. What a defensive cyber operator must hold to see it is carried on the path itself, as required data sources; this path needs no signal source. TOE names that same element.	Satellite Design and Engineering with the SOC
F04	AN:DET:Detection Signature:01 + PB-01	A rule that fires on out-of-pattern command authority, and the playbook that contains, recovers, and reports when it does. TDM names that same element.	Security Operations
F05	AN:RES:Resilience Measure:01	Dual control, so a single compromised operator cannot execute the high-impact action at all. TRE names that same element.	Split: Satellite Design and Engineering owns the dual-control workflow in the commanding software; Satellite Operations owns the peer-review discipline

© 2026 ethicallyHackingspace (eHs)®

Figure 5 One ordinal across the functions: every entry names the same platform element



One element, four target fields. The element never changes across that table. What changes is the question being asked about it: F02 asks what an adversary wants with it, F03 asks how they reach it, F04 asks what would be visible, F05 asks what to change. Four questions, four field names, one **AST:SW:Software:04**. If any row named a different element, the chain would be broken and the reader would need a cross-reference table to reassemble it.

What each function added that the previous one could not. F01 gave the element a name every department uses. F02 said an adversary wants it. F03 said how they would reach it and where that reaching is visible. F04 made the visibility fire and gave the response an owner and a clock. F05 removed the opportunity, or narrowed it, so the earlier layers have less work to do. Remove any one link and the chain breaks: a threat with no element is intelligence, a path with no threat is speculation, a signature with no path watches nothing in particular, and a measure with no accumulated evidence is a guess about where to spend.

What recurs, and what to protect next

Read the accumulated set for repetition, and count it rather than recall it. On this first pass each of the four anchors appears exactly once in each catalog: one threat, one attack path, one detection signature and one resilience measure, because one ordinal carries one chain. Recurrence shows one level down, in the elements the attack paths cross and collect from. Counted across the four paths in Module 03, waypoints and required-source elements together, one element appears in two paths: **SVC:CP:Control Plane:09**, the ground command-acceptance service, is the pivot of Path 00 and the objective of Path 01. Every other element appears in exactly one path. That count compares exact identifiers and does not roll an asset up to its parent. Counted by parent, more overlap would show, for example: Path 00 ends at the patch deployment pipeline, **AST:SW:Software:03**, whose parent is the patch update service, **SVC:CP:Control Plane:12**, where Path 03 enters, and Measure 03's compensating control sits on both. The method publishes no rule for counting by parent, so that overlap is recorded

© 2026 ethicallyHackingspace (eHs)®

here and not counted. By identifier, then, the count names one element on this pass, and that is the adversary-management answer: the ground command-acceptance service is where two of the four paths go. It is the anchor of chain 00, which Measure 00 protects, and it is in the reach of Measure 01. No anchor is shared between chains, so each of the four measures still protects its own anchor, and the count is run again every time the catalog grows. The count covers waypoints and required-source elements only. The reach paragraphs and the compensating controls in chapter 4 are description, not targets, and they do cross chains: Measure 01's reach includes **SVC:CP:Control Plane:09**, the anchor of chain 00, and **AST:SW:Software:03** appears both in Measure 00's reach and in Measure 03's compensating control, whose dual approval and window hold are Measure 00's firmware-push gate. Elements that keep appearing are where the adversary keeps having to go, so they are where hardening buys the most, and they are also where a single failure costs the most. The count did not choose the anchors, which were fixed on Day 2, one per chain, and it does not rank the other three. What it gives is one element the evidence points at and the rule for the next pass: the next measure this platform needs is not chosen by which threat is scariest, it is chosen by counting.

Your role across the week

Adversary management is the fifth and final function where a Full Spectrum professional drives change, and you do not have to be the resilience engineer or the operator to lead it. Resilience needs both operating procedures and architectural change, and Satellite Operations and Satellite Design and Engineering can sometimes be provided by separate organizations from each other and from Security Operations. Your job is to build the cross-functional team and get them to commit measures together. Across the week, these five functions have been your deliberate points of insertion: each one is where you reach across organizational lines and transform how those departments defend the platform together.

CH 6 Tag and Share

> **TAG** `meteorstorm:AN="AN-RES"`

The record in MISP. The measure is the event. The event for `AN:RES:Resilience Measure:00` carries two taxonomy tags: `meteorstorm:AN="AN-RES"`, which says the event is a resilience measure, and `meteorstorm:SVC="SVC-CP"`, which names the kind of element it protects, not which Control Plane service. Three text attributes carry the rest, each with a comment:

- `AN:RES:Resilience Measure:00`, with the comment "Counters AN:THR:Threat:00. NIST SP 800-160 v2 goal: Anticipate."
- **GOAL = Anticipate**, with the comment "One of four: Anticipate, Withstand, Recover, Adapt. Exactly one per measure."
- **TRE = SVC:CP:Control Plane:09**, with the comment "Target of resilience enhancement. Equals the TOE it counters."

The one element the measure protects is read in the TRE attribute, never in a tag and never in the ordinal: the ordinal 00 numbers the chain, and the element's own ordinal is 09. A peer operator who receives the event reads the measure, the one element it protects, the threat it counters and its resiliency goal. The owner split, the cadence, the compensating control and the residual risk are fields of the entry in chapter 4; this event does not carry them as attributes.

The twin run stays with Kestrel. A twin run is the validation step of chapter 3. Neither the Space ISAC Exchange memo nor this workbook defines a format for sharing one, so a twin run is not claimed here as something that crosses to a peer.

© 2026 ethicallyHackingspace (eHs)®

CH 7 Use This at Work

This workbook teaches Function 05 on Kestrel Orbital. To run it on your own platform, work from the **METEORSTORM desk pack**, a separate course download. Its sheets are blank framework templates. They are for your own use and are not returned to the course.

Ten things to do at your work center

Function 05 is run last so that you harden by evidence and not by intuition: the elements that appear in the most threats, the most paths and the most detections are where the adversary keeps having to go, and those are the elements worth spending money on. Each of these can be done with what is already on your desk, in the order given. They are for your own use and are not returned to the course. The sheets named are in the METEORSTORM desk pack.

01 **Count recurrence before you choose what to protect.** Read the accumulated set for repetition, and count it rather than recall it. Compare exact identifiers, and do not roll an asset up to its parent.
What you gain: the next measure is chosen by counting, not by which threat is scariest, and the adversary begins to lose the element reused most.
Chapter 1 and Chapter 5, What recurs, and what to protect next · desk pack sheet 15, Function 05: recurrence tally

02 **Apply the constraint to one measure.** Check that it carries exactly one TRE element, names its goal and names its owner. A measure with no target, no goal or no owner is decoration, not resilience.
What you gain: recurrence stays countable, because every entry anchors to exactly one element.
Chapter 3, The constraint · desk pack sheet 13, Function 05 Adversary Management: method card

03 **Choose the goal by what the measure changes about the attack.** Pick one of Anticipate, Withstand, Recover or Adapt, not by how important the measure feels. Record the goal you can defend, and record why.
What you gain: the goal sets how the measure is later reviewed, an Anticipate measure by asking whether the opportunity is still closed, a Withstand measure by asking whether the mission still runs under load.
Chapter 3, Choosing among the four goals · desk pack sheet 13, Function 05 Adversary Management: method card

04 **Name the one element the measure protects.** The TRE holds one enumerated element, never a list and never a "primary" among several, and it is the element the threat this measure counters names as its TOE. Write the wider reach in the description.
What you gain: the auditor who asks whether the path is countered and the engineer who asks what to change read the same answer from the same record.
Chapter 3, The six steps, step 5, and Why one element and not a list · desk pack sheet 14, Function 05: resilience measure record

05 **Run the lifecycle test on the protected element.** Ask where it sits in its life: reachable, through or fixed. The answer decides whether the measure is applied to the element directly, is a compensating control on the path to it, or is a requirement for the next build.
What you gain: a reader can tell a measure that can be implemented now from one waiting on the next build.
Chapter 3, Where the element sits in its life, and what the measure can therefore be · desk pack sheet 13, Function 05 Adversary Management: method card

© 2026 ethicallyHackingspace (eHs)®

06 **Record the cadence the measure actually holds at.** Write in-force, phased or next-build. Anything not in force must name a compensating control or a recorded residual risk; a residual risk names its owner and what closes it.
What you gain: the catalog admits its gaps, where a catalog that reads as covered with nothing implemented stops anyone looking.
Chapter 3, The rule that keeps the catalog honest · desk pack sheet 14, Function 05: resilience measure record

07 **Write each compensating control as what it is.** It is a control you can implement today, placed on something you do control, and it names the element it is applied to. Say plainly what you have not fixed.
What you gain: the adversary has to cross it to reach the element you cannot change, and no reader mistakes that distance for a hardened element.
Chapter 3, What a compensating control is, and what it is not · desk pack sheet 14, Function 05: resilience measure record

08 **Name the owner, and write out the split.** An architectural change belongs to the department that builds it and an operating procedure to the department that runs it. A measure recorded as Both must name which half each department commits.
What you gain: a measure two people can be held to, because a measure owned by everyone is owned by no one.
Chapter 1 and Chapter 2, The Owner field, and why it exists · desk pack sheet 14, Function 05: resilience measure record

09 **Write the twin run for one measure.** State the question, the scenario run twice, once with the measure applied and once without, the cost, the abuse case and the rejection criterion.
What you gain: the measure is accepted or rejected on the evidence rather than on argument, and the way an adversary could turn it against the platform is exercised before it reaches the platform.
Chapter 3, The digital twin · desk pack sheet 16, Function 05: twin run sheet

10 **Walk every attack path.** Check that each one carries a measure or a recorded residual risk with an owner. When every enumerated path carries one or the other, the enumeration is current.
What you gain: completeness you can audit, because no path is left with neither answer.
Chapter 3, The six steps, step 2 and the repeat line · desk pack sheet 13, Function 05 Adversary Management: method card

© 2026 ethicallyHackingspace (eHs)®

Desk pack sheets for Function 05

Sheet	Use it to
Quick reference, two pages	Read the layers, the tags and the identifier syntax without opening a workbook.
Function 05 method card	Apply the constraint to each measure, then run the six steps in order, with the goal test and the lifecycle test.
Function 05 resilience measure record	Write one resilience measure per record, with its one TRE, goal, owner, lifecycle, cadence, and compensating control or residual risk.
Function 05 recurrence tally	Count which elements the attack paths keep naming, by exact identifier.
Function 05 twin run sheet	Write the question, scenario, cost, abuse case and rejection criterion for one measure.
Completion checklist across the chain	Check that every measure not in force names a compensating control or a residual risk.

Where the method is in this workbook

You need	Chapter and heading
The Owner field	Chapter 2, The Owner field, and why it exists.
The constraint that stands as the gate	Chapter 3, The constraint.
The six steps	Chapter 3, The six steps, fixed order.
The goal test	Chapter 3, Choosing among the four goals.
The lifecycle test and the cadence	Chapter 3, Where the element sits in its life, and what the measure can therefore be.
The rules	Chapter 3, The rule that keeps the catalog honest: anything not in force names a compensating control or a recorded residual risk. Chapter 3, Why one element and not a list.
A twin run, worked	Chapter 3, The digital twin.
Four complete worked records	Chapter 4.
The recurrence count	Chapter 5, What recurs, and what to protect next.

© 2026 ethicallyHackingspace (eHs)®