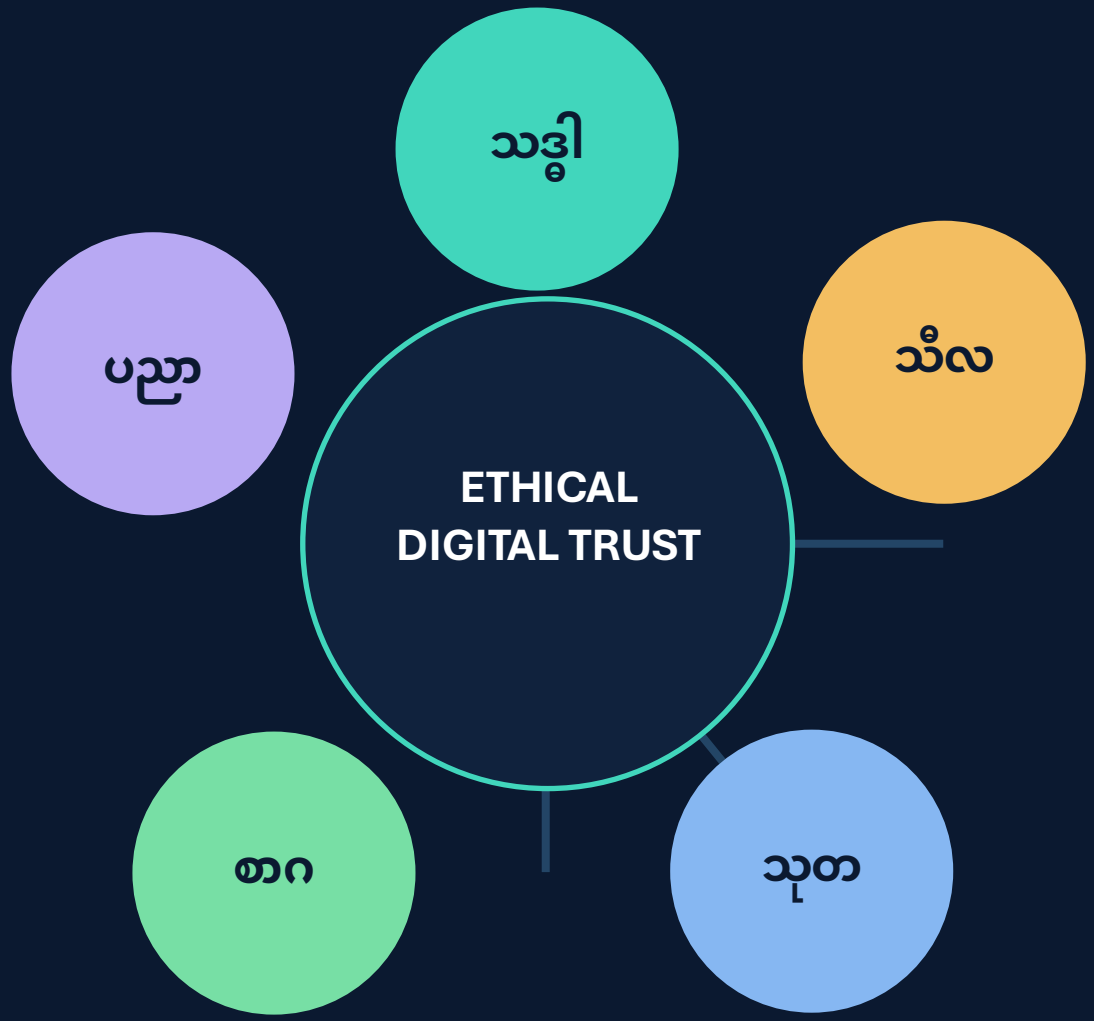
ETHICS · RESILIENCE · DIGITAL TRUST

ဓမ္မနှင့်

ဒစ်ဂျစ်တယ်လုံခြုံရေး

သဒ္ဓါ • သီလ • သုတ • စာဂ • ပညာ

Mangala Sutta · Five Precepts · Seven Noble Treasures
Web Security · Business · AI · Practical Roadmaps



60-MINUTE KEYNOTE + TECHNICAL REFERENCE APPENDIX

CYBERSECURITY

for a Safer IT, Business and Society

DHAMMA × ETHICAL LEADERSHIP × PRACTICAL CONTROLS

သဒ္ဓါ သီလ သုတ စာဂ ပညာ

ETHICAL MINDSET + TECHNICAL CONTROLS = SAFER SYSTEMS

2026 DBIR: three different risk signals

31%

Breaches beginning with exploitation of vulnerabilities

Share of investigated breaches

48%

Breaches involving a third party

Share of investigated breaches

~~ 45% ~

Employees using unapproved AI tools frequently

and social Engineering traps

Employee-use figure, NOT breach share

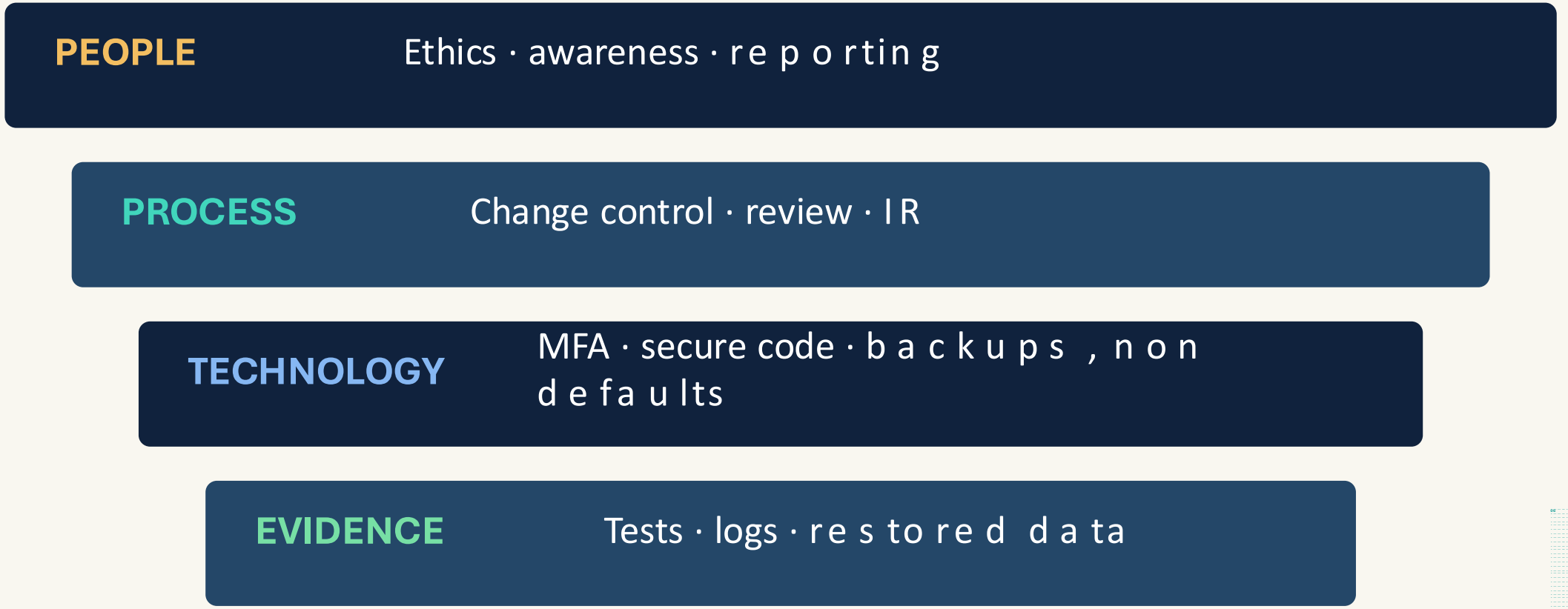
Verizon DBIR 2026 · verizon.com/about/news/breach-industry-wide-dbir-finds

ESSENTIAL IDEAS

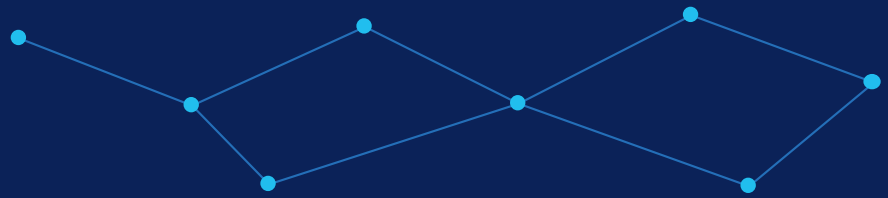
The central distinction: values ≠ te c h n ic a l c o n tro ls

1	D H A M M A	O ffe r s e th ic a l o rie n ta tio n , s k illfu l c o n d u c t, m in d fu ln e s s , d is c e rn m e n t a n d c a re
2	S E C U R IT Y E N G IN E E R IN G	U s e s a u th e n tic a tio n , a u th o riz a tio n , p a tc h in g , e n c ry p tio n , m o n ito rin g a n d re c o v e ry
3	B U S IN E S S G O V E R N A N C E	A s s ig n s o w n e r s , in c e n tive s , ris k d e c is io n s , re s o u rc e s a n d a c c o u n ta b ility
4	E V ID E N C E	S h o w s w h a t w o rk s : te s te d re s to re s , lo g s , re v ie w s , in c id e n t e x e rc is e s

Four mutually supporting foundations



Four Foundations of Digital Trust



PEOPLE

Awareness, capability and ethical conduct

PROCESS

Policies, approvals, exercises and reviews

TECHNOLOGY

Identity, encryption, patches and monitoring

EVIDENCE

Tests, audit trails and verified recoveries

SECURITY IS NOT A PRODUCT • IT IS A DISCIPLINE

PART 01

မင်္ဂလာတရား ၃၈ ပါး

• ငါးပါးသီလ • သဒ္ဓါ၊ သီလ၊ သုတ၊ စာဂ၊ ပညာ

IT • Website Security • Business • A I

Human flourishing as disciplined action—n o t a c h a r m th a t g u a ra n te e s a ll o u tc o m e s .

38 Blessings: A Lifelong Path

Maṅgala Sutta (Sn 2.4 / Khp 5): grouped themes, not a substitute for the full traditional list.

WISE COMPANY

Good influences and good environments

LEARNING & SKILL

Training, knowledge and useful work

ETHICAL RELATIONSHIPS

Honesty, family duties and restraint

HEEDFULNESS & INSIGHT

Mindfulness, patience and wise reflection

GOOD OUTCOMES GROW FROM GOOD CONDITIONS

Dhamma Meaning vs Digital Analogy



ORIGINAL TEACHING

The suttas concern liberation, ethical conduct and wholesome human flourishing.

MODERN APPLICATION

We use selected principles as a reflective lens for workplace decisions and technical safety.

ANALOGY ≠ DOCTRINAL EQUIVALENCE

Maṅgala Sutta: the full path in four movements

1

1–10

Wise community, suitable conditions, learning, discipline and speech

2

11–20

Family, work, generosity, harmlessness, restraint and heedfulness

3

21–29

Respect, humility, gratitude, patience and Dhamma discussion

4

30–38

Renunciation, deeper insight and a mind unmoved by worldly conditions

Khp 5 / Sn 2.4 · suttafriends.org/sutta/khp5/

Blessings that speak directly to modern work

ပညာရှိနှင့် ပေါင်းသင်း = = ? < > . > < ...

Choose reputable mentors, security reviewers and ethical partners.

ဗဟုသုတ + အတတ်ပညာ

Build competence; keep runbooks, labs and peer learning.

ဝိနယ + ကောင်းမွန်သောစကား

Approvals, incident truthfulness and disciplined change.

အပြစ်ကင်းသောအလုပ်

Avoid deceptive business and unauthorized security testing.

အပ္ပမာဒ — မမေ့လျော့မှု

Continuous verification: logs, backups, access and review.

သည်းခံမှု၊ နှိမ့်ချမှု

Calm incidents; hear criticism and improve systems.

Khp 5 / Sn 2.4 · suttafriends.org/sutta/khp5/

PART 02

အရိယာဓန ၇ ပါး

Seven noble treasures: spiritual meanings first; responsible digital applications second.

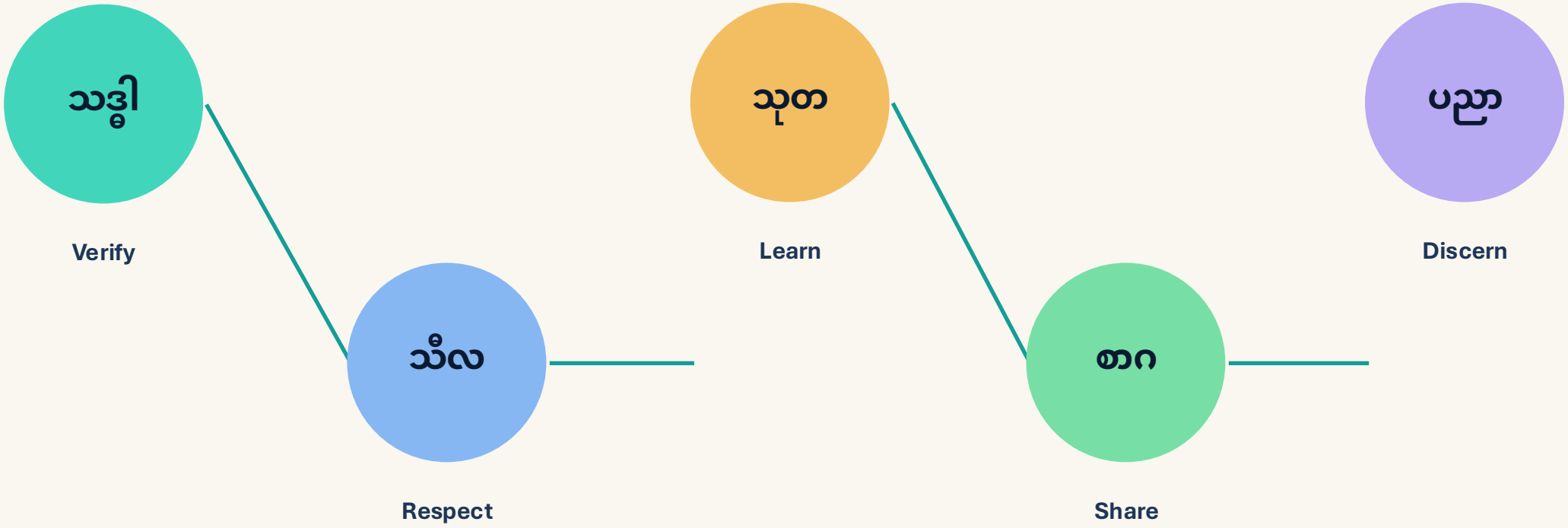
Seven noble treasures — canonical order

1	သဒ္ဓါ · SADDHĀ	Confidence in the Tathāgata's awakening
2	သီလ · SĪLA	Ethical restraint / keeping training rules
3	ဟိရီ · HIRĪ	Moral conscience regarding wrongdoing
4	ဩတ္တပ္ပ · OTTAPPA	Moral concern about wrongdoing and its consequences
5	သုတ · SUTA	Hearing, retaining and understanding good teachings
6	စာဂ · CĀGA	Generosity, freedom from stinginess
7	ပညာ · PAÑÑĀ	Penetrative insight into arising and passing away

AN 7.6 · dhammatalks.org/suttas/AN/AN7_6.html

ILLUSTRATION

Five qualities as a practical leadership lens



AN 7.6 · dhammatalks.org/suttas/AN/AN7_6.html

သဒ္ဓါ · Saddhā: c o n fid e n c e , n o t g u llib ility

D H A M M A S E N S E

C o n fid e n c e in th e B u d d h a ’s a w a k e n in g a n d w h o le s o m e p r a c tic e . It is n o t s im p ly tr u s tin g e v e r y p e r s o n o r e m a il.

M O D E R N A N A L O G Y

C h e c k id e n tity a n d c la im s ; v e r ify p a y m e n tc h a n g e s in d e p e n d e n tly ; p r e fe r e v id e n c e o v e r p r e s s u r e o r s ta tu s .

AN 7.6 · dhammatalks.org/suttas/AN/AN7_6.html

သီလ · Sīla: keep trustworthy boundaries

DHAMMA SENSE

ငါးပါးသီလ

Abstaining from killing, stealing, sexual misconduct, false speech and intoxicants leading to heedlessness.

MODERN ANALOGY

Respect authorization, protect customer data, avoid fraud and harassment, and report incidents truthfully.

AN 7.6 · dhammatalks.org/suttas/AN/AN7_6.html

သုတ · Suta: learning becomes shared capability

DHAMMA SENSE

Hearing, remembering, examining and understanding good teachings repeatedly.

MODERN ANALOGY

Read vendor advisories; run staff training; keep practical runbooks; rehearse recovery and share lessons.

AN 7.6 · dhammatalks.org/suttas/AN/AN7_6.html

චාග · Cāga: generosity with boundaries

DHAMMA SENSE

Being generous and openhanded, free from the stain of stinginess.

MODERN ANALOGY

Mentor colleagues, share secure templates, help affected customers and disclose weaknesses responsibly.

AN 7.6 · dhammatalks.org/suttas/AN/AN7_6.html

ပညာ · Paññā: discernment of consequences

DHAMMA SENSE

Spiritual insight into arising and passing away, directed to the ending of suffering.

MODERN ANALOGY

Ask what can fail; rate plausible impacts; validate AI output; test backup restores; choose proportionate controls.

AN 7.6 · dhammatalks.org/suttas/AN/AN7_6.html

ဟိရီ + ဩတ္တပ္ပ: the inner guardrails

HIRĪ / MORAL CONSCIENCE

Avoid dishonest actions even when nobody is watching. Example: refusing to browse patient or customer files out of curiosity.

OTTAPPA / MORAL CONCERN

Understand potential harm and consequences. Example: refusing unapproved production experiments or unsafe data exports.

AN 7.6 · dhammatalks.org/suttas/AN/AN7_6.html

Five Precepts: Five Digital Commitments

Modern analogies; not literal cyber definitions of the traditional precepts.

NON-HARM	Avoid reckless acts that may harm people or critical services
NO STEALING	No unauthorized accounts, credentials or customer data
RESPECT	Protect consent, dignity and private information
TRUTHFULNESS	No phishing, false claims or hidden incidents
HEEDFULNESS	No impaired or careless privileged operations

ETHICAL RESTRAINT BUILDS A CULTURE OF TRUST

Five precepts → five digital integrity promises

1	၁ မသတ်ဖြတ်	Avoid intentional harm and reckless actions that could injure people
2	၂ မခိုးယူ	Do not access or extract what has not been authorized
3	၃ ကာမမှားမှုမပြု	Protect consent, dignity, sensitive information and workplace safety
4	၄ မုသားမပြော	No phishing, deceptive reporting or material concealment
5	၅ မူးယစ်မှုရှောင်	Avoid impaired operations and heedless privileged changes

AN 7.6 · dhammatalks.org/suttas/AN/AN7_6.html

ငါးပါးသီလ — Digital responsibility

မသတ်ဖြတ်၊ မထိခိုက်စေ	Avoid deliberate destructive activity and negligent safety impact
မပေးသောပစ္စည်း မယူ	No unauthorized access, credential theft or data misuse
ကာမမှားမှု ရှောင်	Respect consent, dignity, privacy; prevent harassment
မုသားမပြော	No phishing, fabricated claims or breach concealment
မူးယစ်မှု ရှောင်	Avoid impaired privileged work; apply operational discipline

Audience exercise: Would you trust this instruction?

A "CEO" email urgently requests a new bank account for tomorrow's invoice.

1

What looks legitimate?

2

What needs verification?

3

Which safer channel?

FACILITATOR TAKEAWAY · Confirm through a known number or established approval path, not the email itself.

PART 03

Cybersecurity fundamentals

Reduce technical risk with layered, testable controls.

Think like a risk owner—not only a tool buyer

6

NIST CSF 2.0 functions organize governance, risk understanding, protection, detection, response and recovery.

Data describes observed breaches in the cited study period. It is NOT a forecast for your organization.

NIST CSF 2.0 · nist.gov/cyberframework

NIST CSF 2.0: six functions in one system



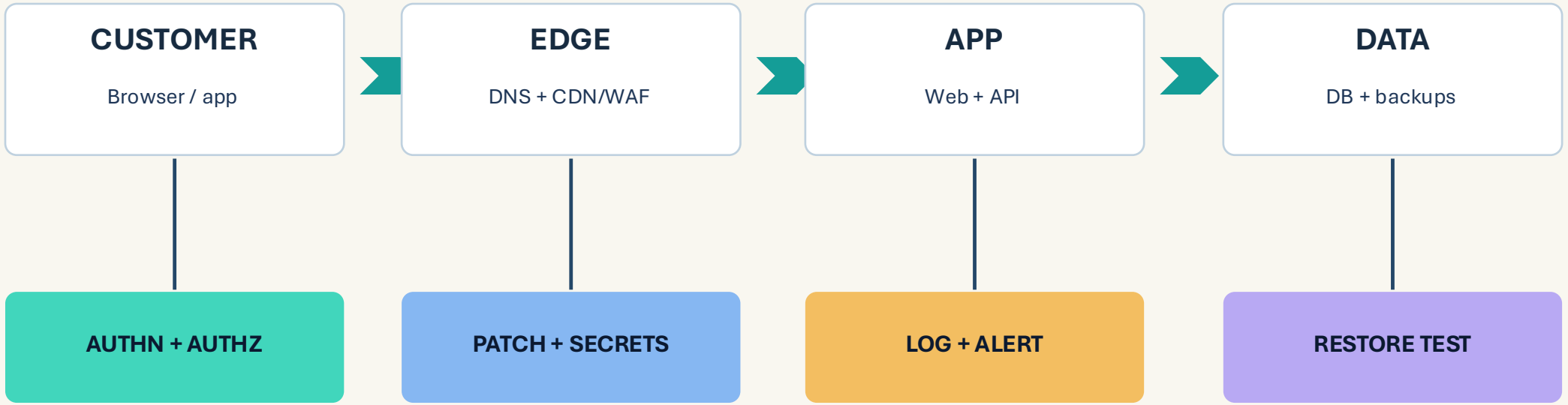
NIST CSF 2.0 · nist.gov/cyberframework

Threat-model the critical path

1	ASSETS	Identity provider, email, DNS, website, customer data, backups
2	THREATS	Credential compromise, exploitation, data exposure, fraud, outage
3	WEAKNESSES	Exposed admin portals, outdated plugins, overprivileged tokens
4	CONSEQUENCES	Privacy impact, financial fraud, downtime, reputational harm
5	CONTROLS, Polocies	MFA, secure code, patching, segmentation, logging, restore tests

CISA CPG · cisa.gov/cybersecurity-performance-goals

A secure website has multiple trust boundaries



Controls must protect EACH trust boundary—not only the login page.

CISA CPG / CIS CONTROL THEMES

High-impact baseline: start here

01 Secure identity

MFA for admins and email; no shared privileged accounts.

02 Control exposure

Inventory and patch internet-facing servers and software.

03 Protect critical data

Minimize, classify, encrypt, back up and control access.

04 Detect actionable events

Alert on unusual admin logins, exports and config changes.

05 Practice recovery

Protected backups and actual restore tests.

06 Assign accountability

Named owner, escalation path, business impact and review.

CISA CPG · cisa.gov/cybersecurity-performance-goals | CIS Controls v8.1 · cisecurity.org/controls/v8-1

OWASP Top 10:2025 in four learning clusters

1 ACCESS

A01 Broken Access Control
A07 Authentication Failures

2 CONFIG + SUPPLY

A02 Misconfiguration
A03 Supply Chain Failures
A04 Cryptographic Failures

3 CODE + DESIGN

A05 Injection
A06 Insecure Design
A08 Integrity Failures

4 OPERATIONS

A09 Logging & Alerting
A10 Exceptional Conditions

A broken-access-control example

A customer changes /orders/1042 to /orders/1043 and sees another person's invoice.

1

Who should be denied?

2

Where enforce checks?

3

What test proves fix?

FACILITATOR TAKEAWAY · Enforce object authorization server-side on EVERY request; test as multiple roles.

Identity: verify, authorize, monitor

1

AUTHENTICATE

Passkeys / phishing-resistant MFA where feasible; protect email and recovery

2

AUTHORIZE

Server-side role checks; least privilege; review joiners / movers / leavers

3

RECOVER

Rotate affected tokens; revoke sessions; secure backup authentication

NIST SP 800-63-4 · csrc.nist.gov/pubs/sp/800/63/4/final

Secure-by-design application checklist

1	DESIGN	Identify data flows, abuse cases, trust boundaries, high-risk features
2	BUILD	Use parameterized SQL; context-aware output encoding; safe file handling
3	DEPENDENCIES	Inventory SBOM/repositories, patch, verify package provenance
4	VERIFY	Peer code review, test authz, scan code and dependencies
5	OPERATE	Secure configuration, secrets rotation, alerting and recovery

OWASP ASVS v5.0 · owasp.org/www-project-application-security-verification-standard/

Backups are not resilience until tested

WE HAVE A BACKUP

"The dashboard is green. We have never restored the application and database together."

WE CAN RECOVER

"Restores are tested with known owners, dependencies, RTO/RPO targets and separate backup credentials."

CISA CPG · cisa.gov/cybersecurity-performance-goals

Incident response is a rehearsed sequence



Document ownership and communications across all five steps

NIST SP 800-61r3 · csrc.nist.gov/pubs/sp/800/61/r3/final

Tabletop: a public backup is discovered

A cloud folder exposes a customer-contact backup. Nobody knows whether it was accessed.

1. First 15 minutes?
2. Preserve which evidence?
3. Who needs a call?
4. How to prevent repeat?

FACILITATOR TAKEAWAY · Restrict access; preserve logs; scope exposure; follow legal/privacy process; fix the root cause.

NIST SP 800-61r3 · csrc.nist.gov/pubs/sp/800/61/r3/final

PART 04

Responsible business and AI

Ethical leadership + operational controls + human accountability.

Customers deserve three assurances

1

RESPECT

Minimal data collection; clear and limited purposes

2

TRUTH

Accurate claims, honest breach communications, no dark patterns

3

RECOVERY

Documented support, tested restoration and incident ownership

AI-generated security advice: approve or refuse?

An AI assistant suggests: “Disable authentication temporarily to solve the website outage.”

1. What is the impact?
2. Which facts are missing?
3. Can we test safely?

FACILITATOR TAKEAWAY · Do not make an unsafe production change without evidence, approval and rollback.

Responsible AI: five practical boundaries

Protect prompts

Redact credentials, customer records and incident secrets.

Verify answers

Check official docs; do not invent citations or commands.

Sandbox code

Review privileges; test script effects before production.

Lock down local APIs

Auth, firewall, logging, model provenance and backup policy.

Human decision owner

Named approver for deployment, customer and legal impact.

Five measurable indicators for leadership

1	MFA COVERAGE	Share of privileged accounts using MFA; check recovery paths
2	EXPOSURE AGE	Days critical external vulnerabilities remain unmitigated
3	RESTORE SUCCESS	Can a critical service be restored and validated?
4	RESPONSE TIME	Time to detect, escalate and contain confirmed incidents
5	LEARNING LOOP	High-impact corrective actions closed and re-tested

CIS Controls v8.1 · cisecurity.org/controls/v8-1

30/60/90 day implementation (sample only)

DAYS 1–30

Name owners; inventory critical assets; secure email/admin MFA; patch exposed systems; protect backups.

DAYS 31–60

Review roles; harden DNS, CERTs and server settings; update dependencies; define alert rules and response contacts.

DAYS 61–90

Test service restore; tabletop a breach; review access controls; measure gaps; fund next risk priorities.

CISA CPG · cisa.gov/cybersecurity-performance-goals | CIS Controls v8.1 · cisecurity.org/controls/v8-1

Closing exercise: one commitment for seven days

Choose the single improvement you can actually deliver by next week.

1. Which system is critical?
2. What is the weakest control?
3. Who owns the fix?
4. What proof will we keep?

FACILITATOR TAKEAWAY · A named owner + a testable outcome is stronger than an inspirational promise.

Main message

သီလ	ယုံကြည်မှုတည်ဆောက်ခြင်း — honesty, respect, accountability
သုတ	သိပ္ပံ၊ နည်းပညာ၊ အတွေ့အကြုံမှ သင်ယူခြင်း
ပညာ	အန္တရာယ်ကို ခွဲခြားသိမြင်၍ သင့်တော်သော control ရွေးချယ်ခြင်း
သတိ	Alert, change, backup နှင့် လူ့အမှားများကို မမေ့မလျော့ စောင့်ကြည့်ခြင်း

Seven takeaways worth remembering

1	သဒ္ဓါ	Confidence grounded in wholesome guidance; verify operational claims
2	သီလ	Stay inside ethical and technical authorization boundaries
3	ဟိရီ / ဩတ္တပ္ပ	Conscience and concern restrain misuse of power
4	သုတ	Keep learning, documenting, practicing and sharing lessons
5	စာဂ	Give help and knowledge without disclosing confidential data
6	ပညာ	Understand causes, trade-offs, evidence and residual risk
7	အပ္ပမာဒ	Build ongoing attention, not a one-time security campaign

AN 7.6 · dhammatalks.org/suttas/AN/AN7_6.html | Khp 5 / Sn 2.4 · suttafriends.org/sutta/khp5/

နိဂုံးချုပ် — ယနေ့မှ စ၍ လက်တွေ့အသုံးချရန်

1	သဒ္ဓါ	အခြေခံတရားကို ယုံကြည်ကျင့်သုံးပြီး အလုပ်ခွင်တွင် သက်သေကိုလည်း စစ်ဆေးပါ။
2	သီလ	အခြားသူ၏ ဒေတာ၊ ကိုယ်ရေးလုံခြုံမှုနှင့် ခွင့်ပြုချက်ကို လေးစားပါ။
3	သုတ	သင်ယူမှု၊ မှတ်တမ်းတင်မှုနှင့် လေ့ကျင့်စမ်းသပ်မှု မရပ်တန့်ပါနှင့်။
4	စာဂ	အန္တရာယ်မဖြစ်စေသော ပညာ၊ အကူအညီနှင့် အတွေ့အကြုံများ မျှဝေပါ။
5	ပညာ	အန္တရာယ်၏ အကြောင်းရင်းကို သိမြင်၍ သင့်တော်သော ကာကွယ်မှုကို ရွေးချယ်ပါ။

AN 7.6 · dhammatalks.org/suttas/AN/AN7_6.html

PART END

Questions & Discussion

သီလဖြင့် ယုံကြည်မှု • သုတဖြင့် လေ့လာမှု • စာဂဖြင့် အကျိုးပြုမှု • ပညာဖြင့် ဆင်ခြင်မှု

PART A

DEEP-DIVE APPENDIX

Optional references, implementation templates, doctrinal detail and extra discussion activities.

Mangala Sutta 1–10: foundations

1	01	Avoiding association with the foolish
2	02	Associating with the wise
3	03	Honoring those worthy of honor
4	04	Living in a suitable place
5	05	Previous meritorious deeds
6	06	Directing oneself rightly
7	07	Extensive learning
8	08	Skilled craft or art
9	09	Well-trained discipline
10	10	Well-spoken speech

Khp 5 / Sn 2.4 · suttafriends.org/sutta/khp5/

Mangala Sutta 11–20: family and conduct

1	11	Caring for mother and father
2	12	Caring for spouse and children
3	13	Peaceful/unconfused livelihood and work
4	14	Generosity
5	15	Righteous conduct
6	16	Helping relatives
7	17	Blameless actions
8	18	Abstaining from evil
9	19	Restraint from intoxicants
10	20	Heedfulness in wholesome states

Khp 5 / Sn 2.4 · suttafriends.org/sutta/khp5/

Mangala Sutta 21–29: discipline and dialogue

1	21	Respect
2	22	Humility
3	23	Contentment
4	24	Gratitude
5	25	Timely hearing of Dhamma
6	26	Patience
7	27	Being easy to advise
8	28	Seeing and meeting renunciants
9	29	Timely discussion of Dhamma

Khp 5 / Sn 2.4 · suttafriends.org/sutta/khp5/

Mangala Sutta 30–38: insight and peace

1	30	Austerity / self-restraint
2	31	The holy life
3	32	Seeing the Noble Truths
4	33	Realization of Nibbāna
5	34	Mind unshaken by worldly conditions
6	35	Sorrowlessness
7	36	Freedom from defilement
8	37	Security and peace of mind
9	38	Unconquered / secure through fulfilling these blessings

Khp 5 / Sn 2.4 · suttafriends.org/sutta/khp5/

မင်္ဂလာတရား ၃၈ ပါးမှ သင်ခန်းစာ

ပညာရှိသူနှင့် ပေါင်းသင်း	Reliable mentors, ethical experts, trusted sources
အတတ်ပညာနှင့် ဗဟုသုတ	Technical competency and continuous professional development
စည်းကမ်းရှိခြင်း	Change control, approvals, checklists, audit trail
ကောင်းမွန်သောစကား	Honest customer communication and incident reporting
အပြမာဒနှင့် သတိ	Monitoring, review, preparedness, careful decisions

Canonical meaning vs contemporary analogy

1

DOCTRINE

The teachings address ethics, insight, suffering and liberation

2

ANALOGY

We apply selected principles to engineering and business judgment

3

BOUNDARY

Cybersecurity controls are not canonically listed in the suttas

Khp 5 / Sn 2.4 · suttafriends.org/sutta/khp5/ | AN 7.6 · dhammatalks.org/suttas/AN/AN7_6.html

မေတ္တာ၊ ကရုဏာ၊ ခန္တီ — security culture

မေတ္တာ · Mettā

Be respectful;
make customer and staff security
guidance supportive.

ကရုဏာ · Karuṇā

Respond to affected people with
concern,
not with blame or indifference.

ခန္တီ · Khantī

Stay patient while investigating;
avoid rash destructive actions.

အပ္ပမာဒ · Appamāda

Heedfulness: notice risks,
check facts and act responsibly.

Khp 5 / Sn 2.4 · suttafriends.org/sutta/khp5/

Greed · aversion · delusion: recognize risky incentives

1	LOBHA (GREED)	Misuse data or manipulate customers for revenue at any cost
2	DOSA (AVERSION)	Blame people and take retaliatory action during an incident
3	MOHA (DELUSION)	Assume security because "we have a firewall" or "AI said so"
4	PRACTICAL RESPONSE	Independent review, transparent metrics, careful controls and humility

Right speech in incident communications

1

TRUTHFUL

Report what is confirmed; avoid invented certainty

2

TIMELY

Inform designated parties without unnecessary delay

3

USEFUL

Provide practical next steps and protect affected people

Khp 5 / Sn 2.4 · suttafriends.org/sutta/khp5/

Zero-trust practical checklist

1	VERIFY EXPLICITLY	Authenticate users/services and check device/resource context
2	LEAST PRIVILEGE	Scope rights by asset and task, review them regularly
3	ASSUME BREACH	Segment systems; protect logs; prepare for credential compromise
4	CONTINUOUS CHECK	Reevaluate sessions and risky behavior according to context
5	BE HONEST	Zero trust is an architectural strategy, not a branded silver bullet

NIST CSF 2.0 · nist.gov/cyberframework

DNS /domain /email protection checklist

1	DOMAIN	Registry/registrar MFA, locked access, controlled recovery contacts
2	DNS	Document zone changes, restrict admin access, monitor changes
3	EMAIL	SPF, DKIM and DMARC planned with testing/monitoring
4	CERTIFICATES	Track TLS expiry and renewal automation
5	DEPENDENCIES	Prepare for DNS provider outage and unauthorized delegation

CISA CPG · cisa.gov/cybersecurity-performance-goals

Linux & web-server hardening checklist

1	PATCH	Maintain supported OS/runtime; remove obsolete plugins and packages
2	SSH	Key-based authentication and restricted administrator access
3	WEB	HTTPS, secure headers/cookies and reasonable upload limits
4	SECRETS	No credentials in code, logs or public backups
5	BACKUPS	Restore test including config, DB and dependency order
6	LOGS	Protected central logs; alert on high-impact administrative actions

CIS Controls v8.1 · cisecurity.org/controls/v8-1

Authentication & authorization test examples

1	LOGIN	Reject invalid credentials; review lockout/rate limit trade-offs
2	SESSION	Secure cookies, session rotation, logout invalidation
3	ROLE	Customer cannot read another customer record
4	ADMIN	Staff-only endpoints deny unauthenticated or unprivileged users
5	RECOVERY	Reset flow verifies identity; tokens single-use and short-lived

OWASP ASVS v5.0 · owasp.org/www-project-application-security-verification-standard/

Software supply-chain security

1	INVENTORY	Versioned list of components and transitive dependencies
2	SOURCE	Approved registries; review maintainer and package provenance
3	BUILD	Protect CI/CD runners, tokens, signing material and artifacts
4	UPDATE	Patch widely exploited vulnerabilities with staging and rollback
5	REVIEW	Perform code/dependency/secret scanning and exception tracking

OWASP Top 10:2025 · top10.owasp.org | OWASP ASVS v5.0 · owasp.org/www-project-application-security-verification-standard/

Logging that produces a response

1	COLLECT	Log significant authentication and administrative events
2	PROTECT	Limit access; synchronize clocks; resist tampering
3	ALERT	Escalate meaningful deviations: privilege change, unusual export
4	REHEARSE	Test that a human actually receives and triages the alert
5	RETENTION	Keep only what is justified by risk, law and business needs

Data minimization: why it reduces risk

1

COLLECT

Ask whether each field is necessary

2

PROTECT

Encrypt, isolate, log sensitive access

3

DELETE

Set retention & disposal policy; validate deletion

Recovery objectives: a worked example

1

RTO

Illustrative: service returns within 4 h

2

RPO

Illustrative: tolerate up to 1 h lost changes

3

TEST

Prove both in a timed restore drill

Illustrative five-by-five risk matrix

ILLUSTRATIVE scoring matrix Use context, evidence, and owner review.

1	2	3	4	5
2	4	6	8	10
3	6	9	12	15
4	8	12	16	20
5	10	15	20	25

Impact ↑

Likelihood →

Risk register template: required fields

1	ASSET + OWNER	What is at risk and who is accountable?
2	THREAT + WEAKNESS	What event is plausible and why?
3	EVIDENCE	What validates the exposure and estimated impact?
4	DECISION	Treat, transfer, avoid or explicitly accept risk
5	DUE DATE	Who implements which control by when?
6	RESIDUAL RISK	What remains after validation and what triggers review?

NIST CSF 2.0 · nist.gov/cyberframework

Tabletop: ransomware on a website

Users report encryption notices on a public service; the backup console may share admin credentials.

1. What must be isolated?
2. How preserve evidence?
3. Can backups survive?
4. How communicate?

FACILITATOR TAKEAWAY · Use an incident lead, separated credentials, tested backups and credible status updates.

NIST SP 800-61r3 · csrc.nist.gov/pubs/sp/800/61/r3/final

Tabletop: phishing through messaging

A staff member gets a Messenger message claiming to be IT support and asking for an OTP.

1. Verify via which channel?
2. Should OTP be shared?
3. What if already shared?

FACILITATOR TAKEAWAY · Never share a one-time code; report quickly; revoke sessions and review activity if compromised.

Security measures by organization size

MICRO/COMMUNITY

MFA, managed hosting, updates, backups, basic incident contacts, staff training.

SMALL BUSINESS

Role review, secure development checks, alerting, supplier oversight, restore drills.

GROWING ORGANIZATION

Formal risk register, advanced monitoring, secure CI/CD, periodic tests, resilience exercises.

CISA CPG · cisa.gov/cybersecurity-performance-goals | CIS Controls v8.1 · cisecurity.org/controls/v8-1

Sample weekly evidence ledger

1	MFA	Privileged-user coverage and new recovery exceptions
2	PATCH	Critical exposures: age, mitigation, owner, due date
3	ACCESS	Account additions/removals and reviews
4	BACKUP	Most recent successful restore and issues
5	ALERTS	Important detection outcomes and missed escalations
6	ACTIONS	Open major corrective tasks; blockers; decisions

CIS Controls v8.1 · cisecurity.org/controls/v8-1

Business continuity: offline-first thinking

1	CONNECTIVITY	Alternative communication plan when internet is unreliable
2	POWER	UPS for critical devices; graceful shutdown and recovery steps
3	PEOPLE	Deputies for key decisions; protect phone recovery accounts
4	VENDORS	Document hosting, DNS, payments and support dependencies
5	CUSTOMERS	Simple status message and fallback contact method

CISA CPG · cisa.gov/cybersecurity-performance-goals

Local LLM security architecture

1	HOST	Patch OS, restrict network interfaces and remote access
2	MODEL	Track provenance/license; scan and approve downloaded weights
3	WEB UI	Access control, logging, backups, trusted updates
4	DATA	Minimize prompt logs and access to confidential files
5	TOOLS	Sandbox generated code; disable unnecessary privileged integrations
6	OUTPUT	Fact-check sources and require change approval

CISA CPG · cisa.gov/cybersecurity-performance-goals

Safer AI prompting: before / after

RISKY INPUT

“Here is our live database dump and root SSH key. Fix everything automatically.”

SAFER INPUT

“Here is a synthetic schema and redacted error. Propose steps; list risks, tests and rollback. Do not execute anything.”

Incident communications: avoid these mistakes

1	FALSE CERTAINTY	Do not claim "no data accessed" when evidence is incomplete
2	PUBLIC SPECULATION	Describe confirmed scope and what is still under review
3	BLAME CULTURE	Protect reporting and preserve accountability
4	DELETION	Do not destroy evidence unintentionally
5	LEGAL OBLIGATIONS	Consult counsel/privacy leads on sector- and jurisdiction-specific duties

NIST SP 800-61r3 · csrc.nist.gov/pubs/sp/800/61/r3/final

Teaching activities: optional 5-minute drills

1	PAYMENT FRAUD	Check bank-detail change via a known channel
2	ACCESS CONTROL	Explain why ID changes must be denied server-side
3	BACKUP	Describe a restore test and identify missing dependencies
4	DATA PRIVACY	Remove unnecessary fields from a registration form
5	AICODE	Identify dangerous assumptions in a generated shell command

CISA CPG · cisa.gov/cybersecurity-performance-goals

Glossary — Dhamma + security

1	SADDHĀ / ŚRADDHĀ	Conviction/confidence (original Buddhist context matters)
2	SĪLA / SUTA / CĀGA	Ethical conduct / learning / generosity
3	PAÑÑĀ / HIRĪ / OTTAPPA	Wisdom / moral conscience / moral caution
4	MFA / IAM / TLS	Multi-factor authentication / identity access / transport encryption
5	RTO / RPO / IR	Recovery time / recovery point / incident response
6	ASVS / CSF / CPG	Application verification / cyber framework / performance goals

Primary references and reading list

M1	Maṅgala Sutta (Khp 5 / Sn 2.4)	https://suttafriends.org/sutta/khp5/
D1	Dhana Sutta / AN 7.6	https://www.dhammatalks.org/suttas/AN/AN7_6.html
S1	NIST CSF 2.0	https://www.nist.gov/cyberframework
S2	OWASP Top 10:2025	https://top10.owasp.org/
S3	OWASP ASVS v5.0	https://owasp.org/www-project-application-security-verification-standard/
S4	NIST SP 800-61 Rev.3	https://csrc.nist.gov/pubs/sp/800/61/r3/final
S5	CISA Cybersecurity Performance Goals	https://www.cisa.gov/cybersecurity-performance-goals
S6	CIS Critical Security Controls v8.1	https://www.cisecurity.org/controls/v8-1
S7	Verizon DBIR 2026	https://www.verizon.com/about/news/breach-industry-wide-dbir-finds

References and scope

Dhamma	AN 7.6 Dhana Sutta — https://www.dhammatalks.org/suttas/AN/AN7_6.html
Mangala	Mangala Sutta (Sn 2.4 / Khp 5), reputable Pali translations
Cybersecurity	NIST CSF 2.0 — https://www.nist.gov/cyberframework
Websecurity	OWASP Top 10 — https://owasp.org/www-project-top-ten/
Baseline	CISA CPG — https://www.cisa.gov/cross-sector-cybersecurity-performance-goals

Important limitations and professional care

1	NO ABSOLUTE GUARANTEE	Dhamma and controls do not make all outcomes perfectly safe
2	NO LITERAL EQUIVALENCE	Modern security comparisons are illustrations, not canonical instructions
3	NO UNAUTHORIZED TESTING	Never scan, exploit or access third-party systems without consent
4	NO COMPLIANCE GUARANTEE	Frameworks and examples do not establish jurisdiction-specific compliance
5	REVIEW BEFORE USE	Verify current advisories, laws, and software-specific guidance

Khp 5 / Sn 2.4 · suttafriends.org/sutta/khp5/ | AN 7.6 · dhammatalks.org/suttas/AN/AN7_6.html | NIST CSF 2.0 · nist.gov/cyberframework | OWASP Top 10:2025 · top10.owasp.org

More ...if..., — Website & IT Security

Security is a system of people, process, technology, and evidence.

Security objectives: CIA + resilience

Confidentiality	Only authorized people access sensitive information
Integrity	Data and configurations remain accurate and untampered
Availability	Services work when legitimately needed
Resilience	Recover safely after error, attack or outage

Threat model: what can go wrong?

Assets	Customer data, DNS, email, website, admin console, backups
Adversaries	Fraudsters, malicious insiders, automated bots
Weaknesses	Stale plugins, shared credentials, exposed storage
Impact	Privacy harm, downtime, financial loss, reputation

OWASP Top 10:2025 — Risk areas

Access and configuration	Broken Access Control; Security Misconfiguration
Supply chain and cryptography	Software Supply Chain Failures; Cryptographic Failures
Application logic	Injection; Insecure Design; Authentication Failures
Integrity and visibility	Software or Data Integrity Failures; Logging & Alerting Failures
Exceptions	Mishandling of Exceptional Conditions

Identity & access

MFA / passkeys	Use phishing-resistant MFA for privileged access where feasible
Least privilege	Separate admin and ordinary accounts; restrict each role
Lifecycle	Joiner, mover, leaver access reviews and rapid revocation
Recovery	Protect password resets, recovery keys and service tokens

Secure website development

Design	Threat model, trust boundaries, authorization decisions
Coding	Parameterized SQL, output encoding, safe uploads
Dependencies	Inventory and patch frameworks, libraries and plugins
Testing	Code review, SAST/DAST, authorized penetration testing

Infrastructure and DNS

TLS / HTTPS	Valid certificates, strong configuration, secure cookies
DNS	Protect registrar, DNS account, zone changes and DNSSEC where suitable
Network	Segment databases and management networks
Hardening	Remove unused services; patch; secure backups and logging

Backups: can you restore?

Copies	Protected copies, including offline or immutable where practical
Separation	Backup admin credentials separate from production
Test	Restore sample data and a whole service in isolation
Objectives	Agree recovery time (RTO) and recovery point (RPO)

NIST CSF 2.0 — Six functions

GOVERN	Policy, risk appetite, ownership, supplier oversight
IDENTIFY	Assets, data, dependencies, risks
PROTECT	Identity, training, patching, encryption, backups
DETECT	Logs, alerts, anomalies
RESPOND / RECOVER	Contain, communicate, restore and improve

Incident response: five steps

1 Detect	Validate alert and scope; capture timestamps
2 Contain	Restrict access; preserve evidence
3 Investigate	Determine affected data, systems and root cause
4 Recover	Rebuild/restore, rotate credentials, verify
5 Learn	Notify as required, document and test corrective actions

Case study — Exposed customer backup

Discovery	Public storage link accidentally exposes a customer database backup
Immediate action	Restrict access and preserve logs; alert incident lead
Assessment	Determine exposure window, content and possible access
Communication	Distinguish known facts and uncertainties; legal/privacy review
Prevention	Access policy, automated checks, backup isolation

Case study — Ransomware on a web server

Signal	Files encrypted; website offline; abnormal admin activity
First response	Isolate affected host, preserve evidence, activate response team
Recovery	Rebuild from trusted source and restore verified backups
Prevention	MFA, patching, network segmentation, immutable backups
Dhamma link	Calm decisions, truthfulness, concern for affected users

Security checklist — D a ily

R e vie w	C ritic a l a le rts , s u s pic io u s a d m in lo g ins a n d n e w e x po s u re s
B a c k up s	C o nfirm b a c k up jo b s ta tu s a n d a le rt fa ilu re s
C h a n g e s	In s pe c t h ig h -ris k c h a n g e s a n d u n e x pe c te d a c c o u n ts
E s c a la tio n	R e c o rd a n d re po rt s u s pic io u s e v e n ts p ro m p tly

Security checklist — W e e k ly

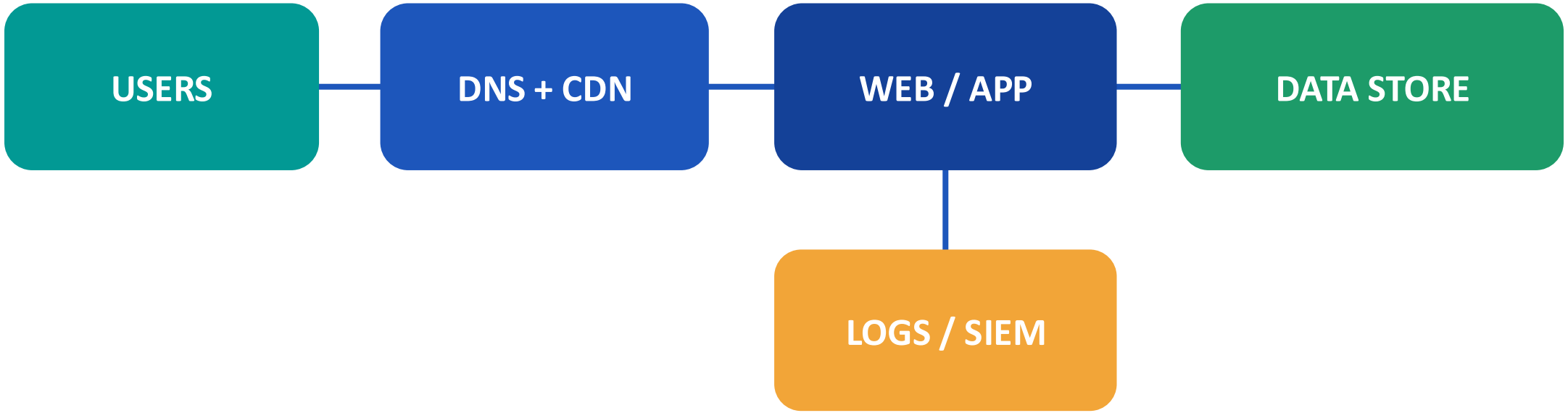
P a tc h	P rio ritiz e e x p lo ite d a n d h ig h -im p a c t v u ln e ra b ilitie s
A c c e s s	R e v ie w p riv ile g e d a c c e s s a n d s e rv ic e a c c o u n ts
E x p o s u re	C h e c k a d m in in te rfa c e s , c e rtific a te s a n d p u b lic s to ra g e
V a lid a tio n	T e s t a s a m p le b a c k u p re s to re o r c o n tro l

Security checklist — M o n th ly

R e vie w	R isk re g is te r, v e n d o rs , d a ta re te n tio n a n d e x c e p tio n s
E x e rc is e	T a b le to p a n in c id e n t o r p h is h in g s c e n a rio
R e s to re	R u n m e a n in g fu l re c o v e ry te s t
Im p ro ve	C lo s e c o rre c tive a c tio n s a n d u p d a te d o c u m e n ta tio n

Secure Website: Trust Boundaries

Editable architecture, simplified for a typical small-business web application.



HTTPS • MFA • Secure coding • Segmentation • Logging • Backups

DEFENSE IN DEPTH • AUTHORIZATION ON EVERY REQUEST

Website Security — Six Essentials



HTTPS / TLS	Protect traffic in transit; configure secure cookies
IDENTITY	MFA and unique admin accounts
UPDATES	Patch OS, CMS, plugins and dependencies
APP SECURITY	Validate input; parameterize SQL; encode output
WAF + RATE LIMITS	Mitigate selected abusive traffic patterns

NO SINGLE CONTROL MAKES A WEBSITE SECURE

Web App: Build Security into Design



AUTHENTICATE

Know who the requester is

AUTHORIZE

Check every sensitive action server-side

HANDLE DATA SAFELY

Parameterize queries; encode output

REVIEW & TEST

Code review, scanning and authorized tests

BROKEN ACCESS CONTROL IS NOT FIXED BY A WAF

OWASP Top 10:2025 — Key Clusters



ACCESS & CONFIG

Access control, security misconfiguration

BUILD & SOFTWARE

Supply chain, integrity and insecure design

DATA & INPUT

Cryptography and injection risks

OPERATIONS

Authentication, logging and error handling

USE TOP 10 FOR AWARENESS; VALIDATE WITH THREAT MODELING

Identity: Stronger than a Password



AUTHENTICATION

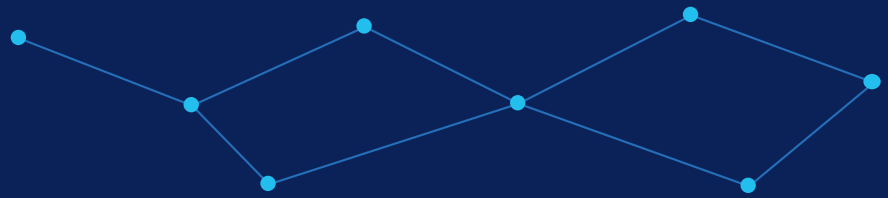
Use phishing-resistant MFA/passkeys for high-value accounts where practical.

AUTHORIZATION

Least privilege, separate admin roles, review access, remove stale accounts.

SECURE EMAIL FIRST: IT OFTEN RESETS EVERYTHING ELSE

IT Infrastructure Security



NETWORK

Firewall rules, segmentation, VPN / ZTNA

ENDPOINT

EDR, patching, disk encryption, device policy

DATA

Encryption, DLP where suitable, backups

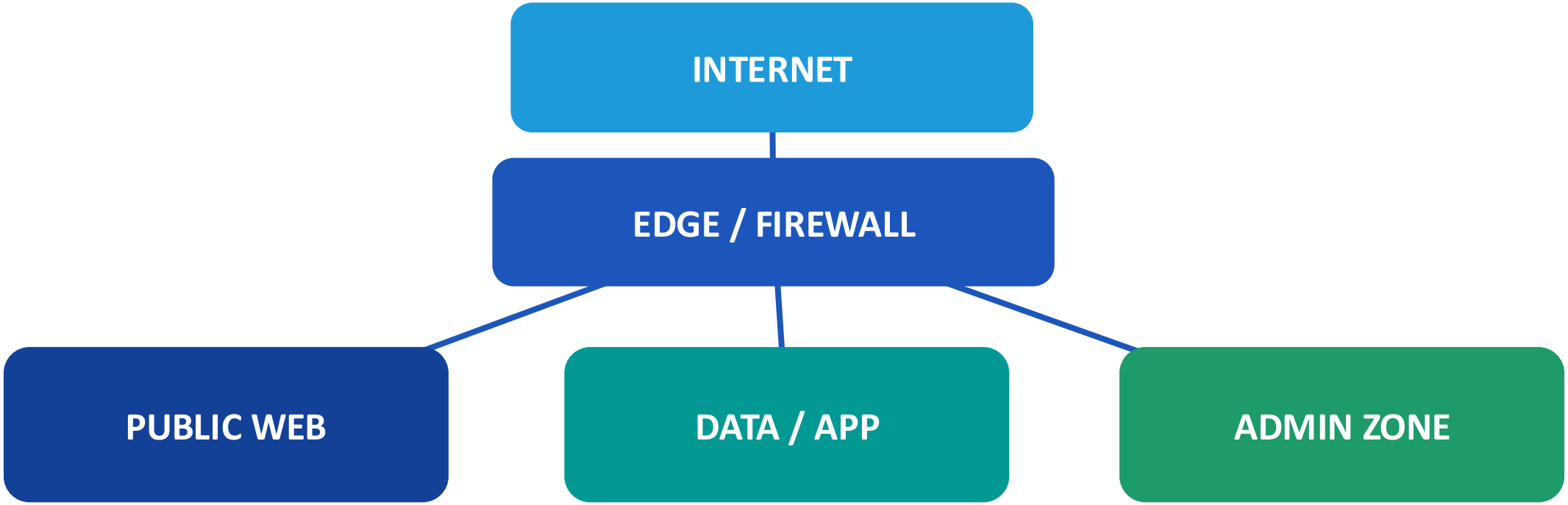
VISIBILITY

Logs, alert ownership, incident runbooks

LAYERED SECURITY + MONITORING + CONTINUOUS IMPROVEMENT

Network Security: Layers, Not Magic

A simplified design-review sketch based on your original IT Security infrastructure slide.



Explicit policies • Limited reachability • Alerted changes

SEGMENT PUBLIC, APPLICATION, DATA AND MANAGEMENT ZONES

WAF, IDS/IPS, VPN, EDR



THE RIGHT TOOL, THE RIGHT JOB

WAF filters some HTTP abuse; IDS/IPS monitors or blocks matched traffic; VPN provides network tunnel access.

WHAT THEY DO NOT SOLVE

None replaces secure coding, least privilege, patching, malware response or tested recovery.

COMPLEMENTARY LAYERS — NOT A UNIVERSAL SHIELD

Protect Endpoints & Servers



PATCH

Update supported systems quickly

HARDEN

Remove unused services; enforce configuration

MONITOR

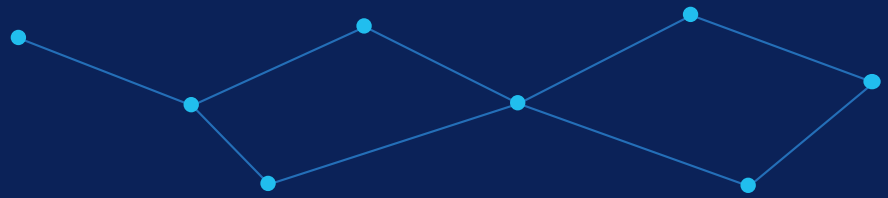
EDR/logs and detection ownership

RECOVER

Rebuild from trusted sources and tested backups

CONTROL THE CONFIGURATION — VERIFY THE RESULT

Backups: Recovery Must Be Tested



01 COPY

Protect copies

02 ISOLATE

Separate credentials

03 RESTORE

Test regularly

04 VERIFY

Check integrity

A SUCCESSFUL BACKUP JOB IS NOT A SUCCESSFUL RECOVERY

Logging → Detection → Action



COLLECT

Auth, changes, access and app errors

CORRELATE

Priority alerts, synchronized time

TRIAGE

Owner, severity and playbook

IMPROVE

Close gaps and tune detection

LOGS ARE ONLY USEFUL WHEN SOMEONE RESPONDS

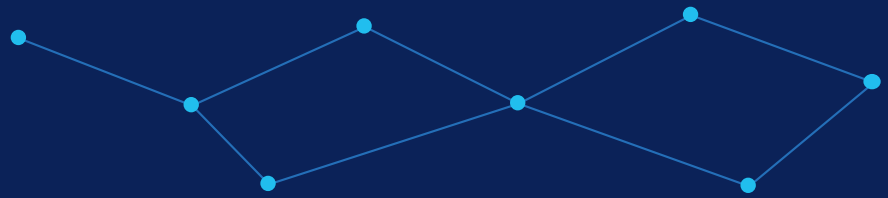
Incident Response: A Calm Sequence



01 DETECT	02 CONTAIN	03 ANALYZE	04 RECOVER	05 LEARN
Confirm facts	Limit impact	Preserve evidence	Restore safely	Fix cause

PRESERVE EVIDENCE • COMMUNICATE TRUTHFULLY

Case Study: Public Backup Exposure

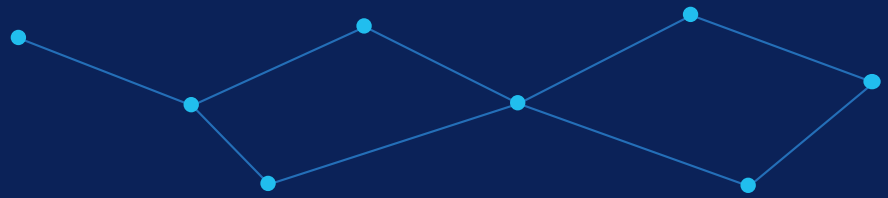


Fictional scenario for a security tabletop.

A PRIVATE BACKUP BECOMES PUBLIC

First: restrict access and preserve logs. Then assess data scope and notification obligations.

and …



CHE … C L E …. ; do not stop learning …, developing, check and secure yourself … and your circle & soeciet ….

even more ….

Keep on study more … gradually and SAFELY ++

Stay SAFE and Good Luck ++