

SECURE BUILDING COUNCIL

October 2026 · Overview edition

The SHIELD Framework.

The security certification for buildings. How SHIELD works, what it measures, and how to get certified.

3

Chapters

36

Spaces and subject areas

141

Requirements

3

Certification levels

Inside this document

Why SHIELD	03
How the framework works	04
Reading a requirement	05
Chapter 1 · Protective Design	06
Chapter 2 · Systems & Technology	07
Chapter 3 · Operations & Governance	08
Sample requirements	09
Certifying a building	10
The SHIELD platform	11
Becoming a SHIELD Accredited Professional	12
Next steps	13

About this overview

This overview explains the structure of the SHIELD framework and lists every requirement a building is assessed on. Sample requirements from each chapter are written out in full, so you can see how criteria and evidence work at each level.

SHIELD is developed by the Secure Building Council, a 501©(3) nonprofit, with volunteer practitioners from across the building and security industries. Requirements are reviewed by the SBC Technical Committee and may be updated between editions.

SHIELD gives your building a recognized security level, so you can prove your security is reasonable before anyone has to ask.

LEED proves a building is sustainable. SHIELD proves it protects the people and the business inside.

SHIELD focuses on physical building security: the site, the building, its systems and the way it is run. It is technology neutral and outcome based. It scores what a measure achieves, not which product delivers it.

WHAT SHIELD HELPS PROTECT

People

Protect occupants, staff and visitors, and meet your duty of care.

Property and goods

Reduce theft, including package and cargo theft at docks, mail rooms and back-of-house areas.

Operations

Run security more efficiently, from deliveries and visitor flow to incident response.

Liability

Show, with documented evidence, that your security decisions were reasonable.

BUILT FOR

Building owners and operators, developers, property managers, architects, engineers, security consultants and integrators, and everyone else who makes a security decision about a building.

Three chapters. Three levels. Clear evidence.

Every building is assessed on the same requirements, grouped by the spaces and programs you already manage. Each requirement is written at three levels, and the combined result sets the building's SHIELD level.

CHAPTER 1

Protective Design

How the site, building envelope and interior spaces are designed to deter, delay and protect.

33 requirements · 16 areas

CHAPTER 2

Systems & Technology

The security systems each space needs, from video and access control to screening and communications.

66 requirements · 11 areas

CHAPTER 3

Operations & Governance

The policies, people and procedures that keep security working every day.

42 requirements · 9 areas

CERTIFICATION LEVELS



BASELINE SHIELD I

Essential measures that meet duty-of-care standards and protect occupants.



ENHANCED SHIELD II

Advanced protocols and monitoring that adapt as threats evolve.



COMPREHENSIVE SHIELD III

Integrated, holistic protection across every building system.



Backed by evidence. Each requirement lists the documents and photos a SHIELD Accredited Professional reviews, such as specifications, policies, logs and site plans, so you know what to prepare before the assessment.

How each requirement is written

Every requirement follows the same structure. This example comes from Chapter 1, Protective Design.

PROPERTY LINE & SITE PERIMETER

Perimeter Barrier System

SHIELD I

Defined property boundary with natural or installed barriers at primary access points.

SHIELD II

Full perimeter delineation with intent-deterrent barriers; CPTED landscape design applied.

SHIELD III

Hardened perimeter with intrusion-resistant barriers; CPTED-certified design; standoff distances documented.

Evidence a SAP will review: Site plan with barrier annotations; barrier specifications; CPTED review documentation.

1

Area

The space or program the requirement belongs to.

2

Requirement

The security outcome being assessed.

3

Levels

What SHIELD I, II and III look like for this requirement. Higher levels build on lower ones.

4

Evidence

What a SHIELD Accredited Professional reviews to verify the level.

A requirement can be marked not applicable when the space does not exist in the building, for example a building with no below-grade levels or no loading dock.

Protective Design

33

requirements · 16 areas

How the site, building envelope and interior spaces are designed to deter, delay and protect people and assets. Requirements follow the building from the property line inward.

REQUIREMENTS BY AREA

Property Line & Site Perimeter 3

Perimeter Barrier System · Vehicle Standoff / Setback · CPTED Sightline Maintenance

Plazas, Parks & Landscape 2

Hostile Vehicle Mitigation · Crowd Flow & Congregation Design

Building Perimeter & Facades 5

Façade Hardening · Ground-Floor Glazing · Upper-Floor Glazing · HVAC Air Intake Protection · Below-Grade Entry Protection

Parking Lots & Garages 2

Vehicle Approach Control · Pedestrian Flow & Lighting

Retail Spaces 2

Storefront Hardening · Back-of-House Separation

Loading Docks, Shipping & Receiving 3

Standoff & Vehicle Approach · Dock Hardening · Inspection / Quarantine Area

Lobbies & Reception Areas 3

Reception Desk Hardening · Visitor Vestibule / Mantrap Design · Egress Planning & Capacity

Conference & Convening 1

Access Path & Egress

Cafes, Cafeteria & Kitchens 1

BOH / Kitchen Separation

Electrical & Mechanical Equipment Rooms 2

Room Hardening · Fire & Smoke Compartmentation

Network MPOE/Demark Rooms 1

Room Hardening & Pathway Protection

IDF & MDF Rooms 1

Room Hardening & Environmental Protection

Stairs & Vertical Conveyances 2

Stairwell Design (Egress + Security) · Elevator Vestibule Design

Tenant Spaces 2

Inter-Tenant Separation · Tenant Emergency Egress

Balconies & Terraces 1

Edge & Fall Protection

Roofs 2

Roof Edge & Fall Protection · Roof Mechanical Equipment Hardening

Systems & Technology

The security systems each space needs: video surveillance, access control, intrusion detection, screening, communications and the security operations center that ties them together.

REQUIREMENTS BY AREA

Property Line, Site Perimeter, & Façade 4

Video Surveillance · Vehicular Interdiction Measures · Intercom System · Public Address System

Lobby & Reception Area(s) 9

Video Surveillance · Access Control · Visitor Management · Intrusion Detection · Intercom System · Telecom · Public Address System · Turnstiles · Two-way Radio System

Plaza(s) & Park(s) 5

Video Surveillance · Public Address System · Emergency Call Station or Intercom System · Emergency Notification System · Vehicular Interdiction Measures

Security Operation Center(s) 11

Video Surveillance · Video Surveillance System · Access Control · Public Address System · Elevator Monitoring System · Elevator Communication System · Intrusion Detection System Monitoring · Key Management System · Barrier Control System · Remote Release Controls · Two-way Radio System

Loading Dock(s) 8

X-Ray Technology · Two-way Radio System · Video Surveillance · Access Control · Magnetometers · Public Address System · Telecom · Intercom System

Mail Room / Messenger Center(s) 8

X-Ray Technology · Two-way Radio System · Video Surveillance · Access Control · Magnetometers · Public Address System · Telecom · Intercom System

Parking Lot(s) & Garage(s) 6

Video Surveillance · Access Control · Public Address System · Emergency Call Station or Intercom System · Vehicular Interdiction Measures · Telecom

Retail Space(s) 5

Telecom · Access Control · Public Address System · Intercom System · Video Surveillance

Conference & Amenity Space(s) 4

Telecom · Access Control · Public Address System · Video Surveillance

Café(s), Cafeteria(s), & Kitchen(s) 4

Telecom · Access Control · Public Address System · Video Surveillance

Electrical & Mechanical Equipment Rooms 2

Telecom · Access Control

Operations & Governance

42

requirements · 9 areas

The policies, people and procedures that keep security working every day, from credentials and visitors to incidents, training and personnel.

REQUIREMENTS BY AREA

Physical Identity, Credentials & Access Management

5

Credential & Key Issuance · Credential Revocation · Least Privilege Principles · Audits and Periodic Reviews · Role-Based Access Control (RBAC)

Visitor & Vendor Management

5

Identity Verification · Authorization & Access Control · Escort Policies · Vendor Risk Controls · Records & Audit Logs

Alarm Monitoring & Management

3

Alarm Response Playbooks / SOPs · Alarm Auditing Practices (Valid vs. False) · Centralized vs. Decentralized Monitoring

Incident Management & Reporting

5

Incident Response Plans · Escalation Matrices · Incident Documentation Standards · Post-Incident Reviews / After-Action Reporting · Collaboration with First Responders

Security Forensics & Investigations

6

Chain of Custody Procedures · Digital Forensics for Physical Security · Investigation Documentation Standards · Investigator Qualifications and Training · Collaboration with Law Enforcement · Privacy and Legal Compliance

Emergency Management & Notification

1

Emergency Management & Notification

Disaster Recovery & Business Continuity

1

Facility Recovery & Continuity Program

Staff & User Education & Training

5

Security Policy Creation, Review, and Updating · Training Frequency Standards · Role-Based Training · Tabletop & Physical Training · Security Awareness (non-security users)

Personnel Management

11

Background Verification · Screening Measures · Evaluation · Access Control and Revocation · Return of Assets · Exit Interviews · Code of Conduct · Employment Terms and Conditions · Dispute Resolution · Disciplinary Action · Incident Management

One requirement from each chapter.

Three levels of performance and the evidence used to verify them.

CHAPTER 1 · PROTECTIVE DESIGN

BUILDING PERIMETER & FACADES

Ground-Floor Glazing

SHIELD I

Standard glazing meeting building code.

SHIELD II

Laminated glass or security film tested per ASTM F1233; ground-floor windows hardened.

SHIELD III

Ballistic-rated (UL 752) or blast-resistant glazing per ASTM F1642 where threat warrants.

Evidence a SAP will review: Glazing specifications; test certifications; threat-assessment justification.

CHAPTER 2 · SYSTEMS & TECHNOLOGY

LOBBY & RECEPTION AREA (S)

Visitor Management

SHIELD I

Visitors are logged with paper sign-in sheets or via an excel (or similar) spreadsheet.

SHIELD II

Visitors are logged electronically through a visitor management system.

SHIELD III

Visitors are logged electronically through a visitor management system and an ID exchange or verification takes place.

Evidence a SAP will review: Visitor policy; VMS vendor; sample logs.

CHAPTER 3 · OPERATIONS & GOVERNANCE

PERSONNEL MANAGEMENT

Screening Measures

SHIELD I

Entity employs at least 1 of: Criminal Record · Education Verification · Investigative Measures (Polygraph/Psych) · References · Drug Testing · Financial Background · Credential Auth · Credit Reports.

SHIELD II

Entity employs at least 2 of the above screening measures.

SHIELD III

Entity employs 3 or more of the above screening measures.

Evidence a SAP will review: Screening policy; vendor reports by category; sample evidence.

From registration to plaque.

Who does what at each step: the owner registers and chooses a SAP, the SAP assesses the building, and SBC awards the level.

1

Register OWNER

Register the building with its type, size, location and target level.

2

Choose a SAP OWNER

Pick an independent SHIELD Accredited Professional from the directory, or ask SBC to connect you with one.

3

Assessment SAP

The SAP assesses the building against every requirement and collects evidence, on the SHIELD assessment platform or with the manual assessment form.

4

Review SBC

The submission goes through an automated first review, then SBC makes the final decision.

5

Certified SBC

The building receives its SHIELD level, certificate, plaque and a listing in the SHIELD registry.

3 years

Certification is valid for 3 years from the date it is awarded.

Any building

New construction, major renovations and buildings in operation.

Independent

Assessments are carried out by SAPs, not by SBC.

Assessors confirm in writing that everything they submit is accurate, and SBC may audit any assessment.

See the gaps. Plan the fixes. Find solutions.

The SHIELD platform turns an assessment into a clear plan: where the building falls short, what to do about it, what it may cost, and who can help.

The screenshot displays the SHIELD platform interface, which is divided into three main sections:

- Assessment report:** This section shows a list of "Top 5 Gaps" with their respective status and descriptions.

Gap ID	Gap Name	Description	Status
PHY-06	Vehicle standoff and barriers	Hostile-vehicle mitigation protects the highest-consequence gathering points of the property.	NO
PHY-03	Loading dock and service entry controls	Back-of-house entries are frequently exploited because they receive less scrutiny than lobbies.	PARTIAL
TEC-04	Security system cyber hygiene	Physical security devices are a common beachhead for network intrusions.	PARTIAL
OPS-03	Emergency drills and exercises	Drilled buildings evacuate faster and suffer fewer casualties in real events.	PARTIAL
GOV-03	Background screening program	Insider risk is consistently among the costliest and least-detected threat classes.	PARTIAL
- Remediation plan:** This section provides a detailed plan for addressing the gaps. It includes a "Remediation Plan" header, a description of the plan, and a table of actions.

Action	Effort	Cost Est.
Commission a vehicle standoff and hostile vehicle mitigation assessment and implement priority barrier or traffic-control measures for the frontage.	high	\$\$\$
- Solutions Marketplace:** This section allows users to connect with approved vendors to remediate security gaps. It features a search bar, filters for "All Pillars", "All Categories", and "All Tiers", and a list of vendor solutions.

Vendor	Category	Product	Description
Citadel Command Software	CYBER	Unified security command platform for Class A portfolios.	PLATINUM
ClearView Surveillance	VIDEO	Cloud video surveillance with 90-day retention and AI-assisted review.	PLATINUM
Sentinel Access Systems	ACCESS CONTROL	Enterprise access control from lobby turnstiles to credential lifecycle management.	PLATINUM

- 1 See your gaps**
Every requirement the building does not yet meet, in one view.
- 2 Plan and budget**
Prioritized actions with effort and cost estimates to help you choose what to fix first.
- 3 Compare solutions**
Browse providers by category and request quotes. Listings are not endorsements by SBC.

Shown with sample data. Field assessments are completed on the SHIELD assessment platform, powered by ADRM, or with the manual assessment form. Assessment data stays private to the building owner and its assessor.

Become a SHIELD Accredited Professional.

SAPs are the independent professionals who assess buildings against SHIELD. Consultants, architects, engineers and integrators can all apply.

1

Apply YOU

Create your account and share your experience in security, design, engineering or operations.

2

Screening SBC

Every applicant goes through background screening before taking the exam.

3

Prepare YOU

Study the SHIELD Framework on your own, or take optional SHIELD Academy courses.

4

Pass the exam YOU

The SAP exam is taken online and lasts 2 hours. With an active SAP, you can take the SAP-A exam.

5

Assess buildings SAP

Use the SHIELD assessment platform free of charge and appear in the SAP directory.

SAP

SHIELD Accredited Professional

Assess buildings against the SHIELD Framework and lead certification projects.

Renews every 2 to 3 years · 15 CE hours per 2 years

SAP-A

SHIELD Accredited Professional, Advanced

For complex, high-risk and SHIELD III projects. Requires an active SAP.

Renews every 2 to 3 years · 30 CE hours per 2 years

Next steps

Know where your building stands.

Start your certification, become an accredited professional, or keep learning with the people who wrote SHIELD.

1

Certify a building

Register your building and get matched with a SAP.

2

Become a SAP

Apply, pass the exam and start assessing buildings.

3

Learn

Get the Newsletter on Security Design, watch webinars, or explore SHIELD Academy.

SECURE BUILDING COUNCIL

securebuildingcouncil.com ·
info@securebuildingcouncil.com

© 2026 Secure Building Council, a 501(c)(3) nonprofit. SHIELD is a trademark of the Secure Building Council. This overview reflects the framework as of October 2026 and may be updated.