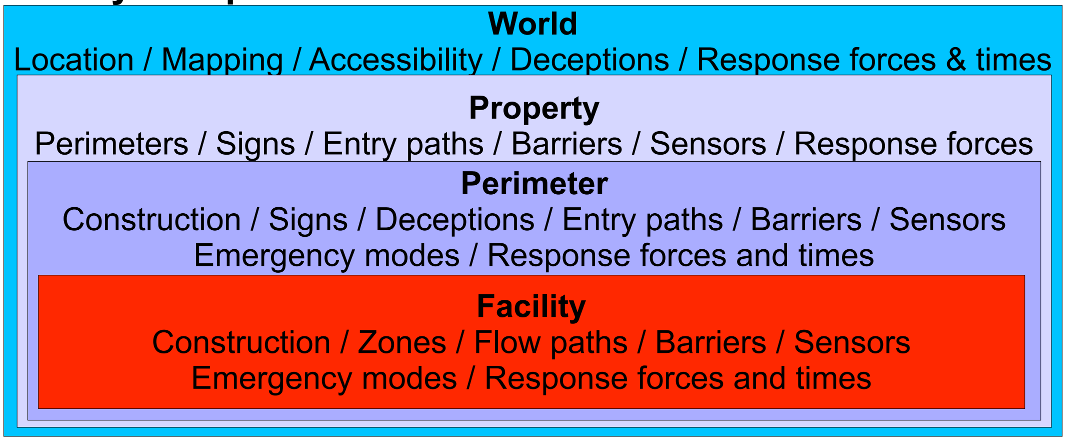
8.4 Perimeters

Rate each issue from 0-10.

Issue	*Rate*
Perimeters are implemented in both physical and logical senses.	
Logical perimeters are co-located with physical perimeters for the added surety associated with their co-location.	
The physical barrier prevents cross-connection between sides.	
Encryption is placed at the physical barrier to enhance separation.	
Perimeters are judged by the set of barriers present against illegitimate passage, the quality of implementation of those barriers, and the ease of passage for legitimate purposes.	
TOTAL (total and divide by 5)	

8.4.1 Physical perimeter architecture



World

Location / Mapping / Accessibility / Deceptions / Response forces & times

Property

Perimeters / Signs / Entry paths / Barriers / Sensors / Response forces

Perimeter

Construction / Signs / Deceptions / Entry paths / Barriers / Sensors
Emergency modes / Response forces and times

Facility

Construction / Zones / Flow paths / Barriers / Sensors
Emergency modes / Response forces and times

Rate each issue from 0-10.

Issue	*Rate*
Physical controls are integrated into informational controls.	
For deterrence there are signs, terrain, location, and deceptions.	
For prevention, perimeters use a wide range of barricades including but not limited to steps, fences, cement separators, moats, mounds, walls, and mine fields as appropriate.	
Perimeter detection uses a wide range of sensor technologies including visual, infrared, ultrasonic, sonic, chemical, pressure, motion, and even animal mechanisms as appropriate to the specifics of the circumstance.	
Reaction involves the movement of forces or use of fires of various sorts.	
Adaptation is undertaken by structural redesigns, movement of facilities, increased or enhanced perimeters, and so forth.	
TOTAL (total and divide by 6)	

8.4.1.1 World

Rate each issue from 0-10.

Issue	*Rate*
Concealment of location by not advertising it or putting signs on doors or putting an address in the corporate directory are used to limit the number of people who know where a facility is for those who do not have legitimate access.	
Locations in remote areas are used as extensive distance barriers to approach without detection only in cases where the added cost is justified.	
Preventing the mapping of an area is not depended on for security purposes.	
Deceptions ranging from false locations in directories to addresses that don't seem to be there to concealment of a facility within another business are used to limit the knowledge of attackers of a target only when justified by the situation.	
Response forces and times associated with their responses are used analysis of location. For example, being located near emergency services provides increased security through decreased response times.	
TOTAL (total and divide by 5)	

8.4.1.2 Property

Rate each issue from 0-10.

Issue	*Rate*
Property location and characteristics such as grades, soil makeup, weather, and surrounding topology are considered for the protective function they play or the deficits they represent in the selection of the property on which a facility is placed and the protection used to augment the property.	
Properties in flood zones, at the end of airport runways, on known fault lines, next to active volcanoes, in tsunami areas, below large bodies of water, near hazardous chemical plants or explosives factories, and in other paths of natural or unnatural disasters are subject to the outrageous fortunes associated with those locations and are avoided when feasible.	
Such properties, when used despite their deficits, are provided with adequate additional protective measures in order to achieve the same level of protection that would commonly be afforded by a different location.	
Perimeters surrounding properties and property lines with natural barriers, barriers within properties such as rivers, lakes, arroyos, cliffs, and similar natural and unnatural barriers are characterized in the analysis of attack graphs into and out of properties.	

Issue	*Rate*
Perimeters and other similar features are considered in the selection and design of protective mechanisms both for their beneficial value and for their impacts on reactions of defensive forcees.	
Accessibility from the air, ground, water, and underground are all characterized and considered in analysis of attack and defense processes.	
TOTAL (total and divide by 5)	

8.4.1.3 Perimeter

Rate each issue from 0-10.

Issue	*Rate*
Perimeters surrounding properties and within properties provide distance and distance has advantages that are exploited for defense.	
Distance is used to reduce electromagnetic, sonic, and other emanation levels.	
Distance is used to increase power levels required for exfiltration of data and it make it more obvious when someone tries to go from one side of the perimeter to the other.	
Distance is used to make it harder to tunnel under or fly above without being detected.	
Distance makes running wires take longer and cost more, and this is taken into account in trading off the benefits of distance with their costs.	
Barriers are used to provide added reduction in emanations of various sorts, blocking visual, sonic, electromagnetic, and other inspection from reaching easy to enter proximate locations.	
Barriers are used to prevent penetration by different sorts of mechanisms ranging from a simple fence that prevents walk-ins to a barrier capable of deflecting a high explosive blast.	
Barriers are selected and designed to defeat the capabilities and intents of the identified threats they are supposed to mitigate.	
Barriers also provide cover for attackers who may be able to hide behind or between barriers to defeat detection, and this is taken into consideration in the design of barriers and related defense mechanisms.	
For the vast majority of cases, barriers have to be permeable to be useful because some amount of legitimate use has to pass into and out of the protected area and this permeability is explicitly considered in their placement, design, and operation.	
Entry paths are provided to allow barriers to be bypassed in controlled ways and under proper identification and authentication processes that grant authorization to pass while still meeting the need to provide adequate protection against identified threats.	

Issue	*Rate*
Mantraps and similar technologies are employed to trap individuals who try to pass a barrier without authorization to do so only when the liability issues associated with this sort of restraint are considered and approval is given by executive management and the legal department.	
For volume entry and exit facilities, entry paths are made fairly direct, proximate to parking or entrances, and able to handle the volumes required while still meeting the security requirements of those barriers.	
Construction of barriers and emergency modes for bypassing barriers are critical to understanding behaviors under unusual circumstances as opposed to normal operational modes and these modes are taken into consideration as part of the construction of those barriers.	
Signs required to provide legal notice as to trespass, proper entry, authorized access and use, and safety and health hazards associated with the property are placed, verified, and maintained properly.	
Sensors around and within properties are used to allow smaller numbers of people to more rapidly detect and triage attempted entries and passage.	
A wide range of sensor technologies are used, ranging from unified heat, sound, light, motion, shape, humidity, temperature, and dew point sensor arrays to simple trip wires and touch sensitive devices that sound alarms, as appropriate to the need.	
Response forces are used in order for these methods to be effective with the time required for response at different force levels acting as a critical factor in the effectiveness against specific threats.	
TOTAL (total and divide by 18)	

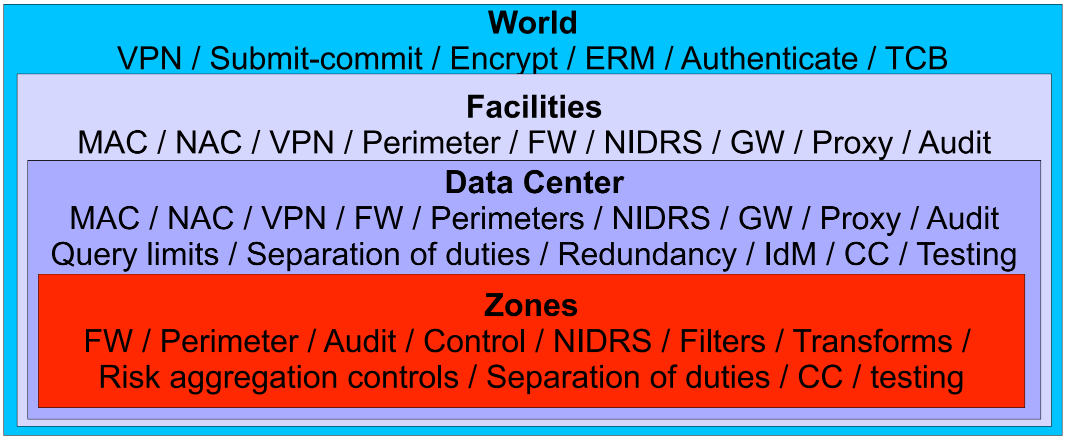
8.4.1.4 Facility

Rate each issue from 0-10.

Issue	*Rate*
Facilities topologies that dictate how things and people go from place to place, internal barriers, sensors, zones, and similar protective mechanisms that are analogous to those on properties, but typically with better controls, are analyzed and considered in the design of facility security.	
Building sound, temperature, and humidity controls, motor generators, doors of different quality with locks of different quality, hinges on one side or the other, and other similar characteristics are reviewed and analyzed as part of facility design to limit event sequences to those that can be adequately handled by response forces.	

Issue	***Rate***
Construction materials and processes dictate the classes of threat capable of bypassing barriers such as walls and doors as a function of time with and without detection and those materials are selected in order to provide desired delays suited to the overall facility defense plan.	
Passage under floors, over ceilings, through air ducts, by picking or tricking locks, electrically or mechanically fooling sensors or tripping opening mechanisms, removing or cutting hinges from doors, and other methods that grant human, other creature, or machine access are considered in the design and implementation of facility protection against identified threats.	
Tailgating, introduction of noxious gases to invoke emergency modes, fires, floods, and any number of other reflexive control attacks that can be induced or occur by accident are considered in facility design.	
Response forces and times are designed to limit the potential consequences associated with attacks from identified threats.	
TOTAL (total and divide by 6)	

8.4.2 Logical perimeter architecture



World

VPN / Submit-commit / Encrypt / ERM / Authenticate / TCB

Facilities

MAC / NAC / VPN / Perimeter / FW / NIDRS / GW / Proxy / Audit

Data Center

MAC / NAC / VPN / FW / Perimeters / NIDRS / GW / Proxy / Audit
Query limits / Separation of duties / Redundancy / IdM / CC / Testing

Zones

FW / Perimeter / Audit / Control / NIDRS / Filters / Transforms /
Risk aggregation controls / Separation of duties / CC / testing

Rate each issue from 0-10.

Issue	***Rate***
Logical perimeters act in much the same way as physical perimeters, providing a series of barriers that slow or stop attackers and are analyzed using similar techniques and with similar rigor.	
Logical perimeters include transforms and separation mechanisms at the outer perimeters, access controls, transforms, enclaves, and filters at facilities perimeters, and a range of other technologies closer into the higher valued content.	
TOTAL (total and divide by 2)	

8.4.2.1 World

Rate each issue from 0-10.

Issue	*Rate*
From the outside world, perimeter mechanisms are oriented toward things that permit the perimeters to be permeated with relative safety.	
Virtual private networks (VPNs) are used to provide encrypted tunnels between non-adjacent areas.	
Authentication technologies allow identity to be authenticated to the degree appropriate for the use.	
Submit-commit mechanisms are used for high valued transactions to provide physically secured devices to the user (to the desired level of surety) so that any mechanism desired can be used to submit a request but an adequately secured method is used to commit to that use.	
Enterprise rights management is used to pack protective mechanisms with content for low surety levels for use at a distance. They are not trusted for medium or high surety needs and risk aggregation is considered in the risks associated with their use.	
Trusted computing bases (TCBs) are used to provide higher assurance at remote locations when appropriate to the situation and surety level.	
TOTAL (total and divide by 6)	

8.4.2.2 Facility

Rate each issue from 0-10.

Issue	*Rate*
Facility-level protection includes mandatory access controls at the network level.	
Facility-level protection includes low-level communications card or processor identification and authentication mechanisms for devices attaching to internal networks and systems.	
Facility-level protection includes VPN termination or internal VPN capabilities,	
Facility-level protection includes physically secured logical network separation perimeters such as virtual local area networks (VLANs)	
Facility-level protection includes firewalls.	
Facility-level protection includes network intrusion and anomaly detection and response systems to detect event sequences with potentially serious negative consequences before they produce consequences exceeding management-defined thresholds.	
Facility-level protection includes gateway systems or proxy servers for situations in which protocol-level attacks are to be prevented.	

Issue	*Rate*
Facility-level protection includes audit mechanisms capable of adequately recording facility-level events to meet all legal, regulatory, and operational needs.	
TOTAL (total and divide by 8)	

8.4.2.3 Data center

Rate each issue from 0-10.

Issue	*Rate*
Data centers have additional protections both at the physical level in terms of internal areas within facilities, and at the network and logical level in terms of similar protections to those for the facility, but with tighter settings and more restrictions.	
Additional protective measures include query limits that limit the syntax and semantics of database queries.	
Additional protective measures include separation of duties protections to assure that risk aggregation is limited from a logical perspective within the data centers.	
Additional protective measures include redundancy for increased assurance levels against denial of services or single points of failure.	
Additional protective measures include identity management systems and interfaces to increase the surety of and specificity of access control decisions.	
Additional protective measures include change control mechanisms to increase the surety of software and configurations for systems with higher valued content for utilities or aggregations of lower valued content that form medium or high risks.	
Additional protective measures include more extensive testing processes.	
TOTAL (total and divide by 7)	

8.4.2.4 Zones

Rate each issue from 0-10.

Issue	*Rate*
Zones are used to further separate portions of networks at a logical level both from a standpoint of classification and need to know, as implied by the access control architecture, and from a standpoint of disaggregation of risks, separation of control from data, and other protective requirements associated with functional unit design and risk management requirements.	

Issue	***Rate***
Zones are implemented with firewalls and other perimeter mechanisms, audit mechanisms, control mechanisms, and separation of audit from control from content.	
Network anomaly and intrusion detection and response systems may be used along with filtering technologies such as virus detection and transform technologies such as those identified for content control to augment solutions in some areas but are not relied on as primary protection mechanisms for medium or high risk levels.	
Separation of duties are implemented so that different individuals have responsibilities in different zones, and this is considered in evaluating risk aggregation controls.	
Change control and testing processes are varied depending on the specific needs of the zones as defined with increased rigor in zones with increased risk.	
TOTAL (total and divide by 5)	

8.4.3 Perimeter summary

Rate each issue from 0-10.

Issue	***Rate***
Perimeter mechanisms are designed to operate at a boundary and not within that boundary.	
Perimeter architecture assumes that it can only limit what will pass the perimeter in what direction at what rate and how long the barrier will withstand what sorts of forces.	
Perimeters are designed to either sever attack graphs or increase the time to traverse links of the attack graph depending on the capabilities being used in order to defeat it.	
Perimeters provide as little friction to normal operation as possible.	
For high volume perimeters like airport entrances or network perimeters, design facilitates low delay times under high load.	
TOTAL (total and divide by 5)	

8.4.4 Roll-up

Enter the summary ratings from each area.

Issue	***Rate***
Perimeters	
Physical perimeter architecture	
World	
Property	
Perimeter	
Facility	
Logical perimeter architecture	
World	
Facility	
Data center	
Zones	
Perimeter summary	
TOTAL (total and divide by 12)	

Startup	***Diligence***	***Typical***	***Excellent***	***Best***
1	5	3	7	9.5