Carbon Black.

Understanding the FFIEC Cybersecurity Assessment Tool

Table of Contents

How to Use the CAT 3

Background 4

Introduction 5

Inherent Risk Profile 6

Cybersecurity Maturity Level 9

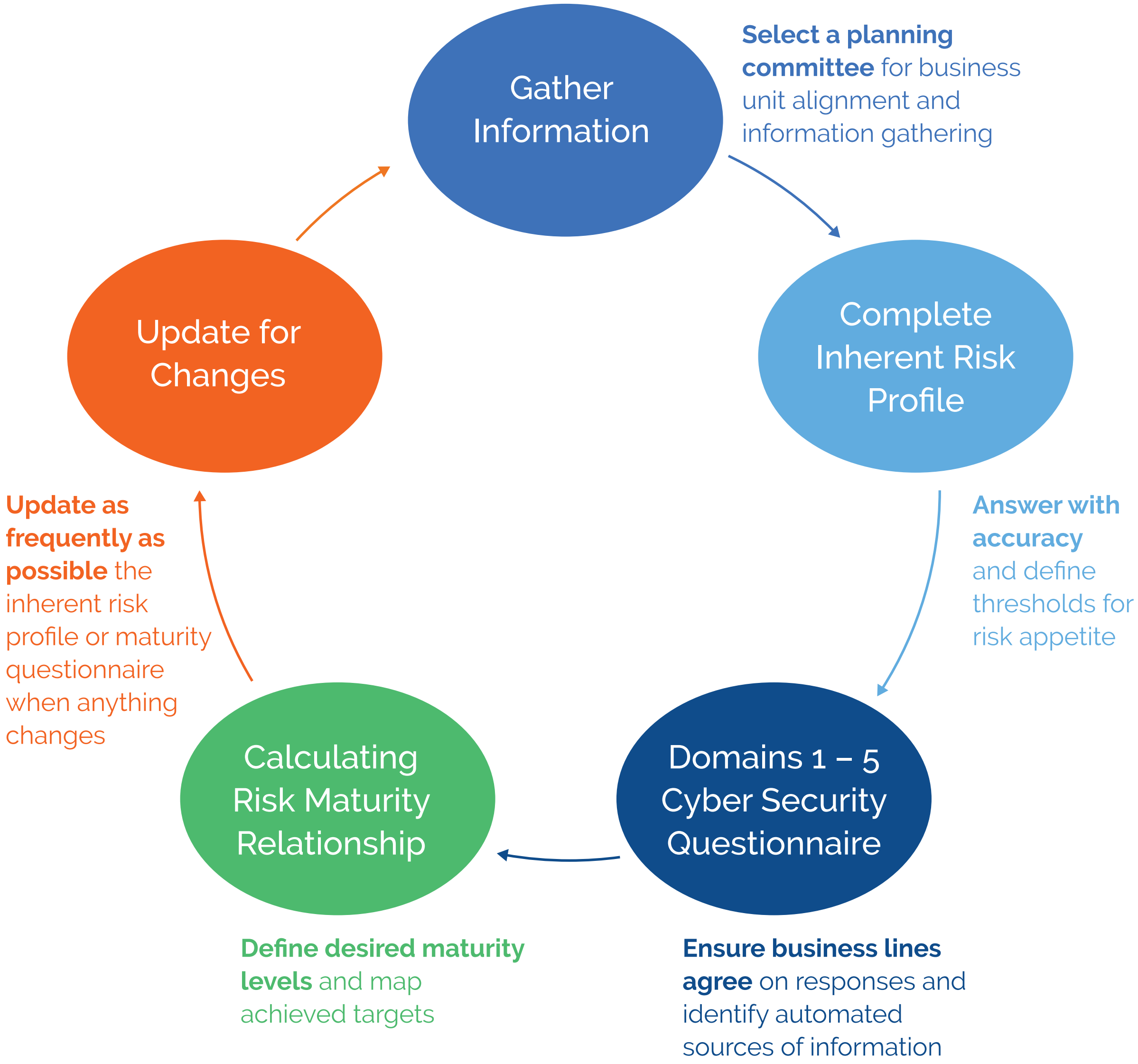
- Domain 1: Cyber Risk Management and Oversight 10
- Domain 2: Threat Intelligence and Collaboration 11
- Domain 3: Cybersecurity Controls 12
- Domain 4: External Dependency Management 13
- Domain 5: Cyber Incident Management and Resilience 14

Risk/Maturity Relationship 16

Case Study: ABC National Bank 16

- Inherent Risk Profile 17
- Cyber Security Maturity Level 19
  - Domain 1 19
  - Domain 2 21
  - Domain 3 23
  - Domain 4 25
  - Domain 5 26
- Overall Risk Maturity 27

How to Use the CAT



Gather Information

Select a planning committee for business unit alignment and information gathering

Complete Inherent Risk Profile

Answer with accuracy and define thresholds for risk appetite

Domains 1 – 5 Cyber Security Questionnaire

Ensure business lines agree on responses and identify automated sources of information

Calculating Risk Maturity Relationship

Define desired maturity levels and map achieved targets

Update for Changes

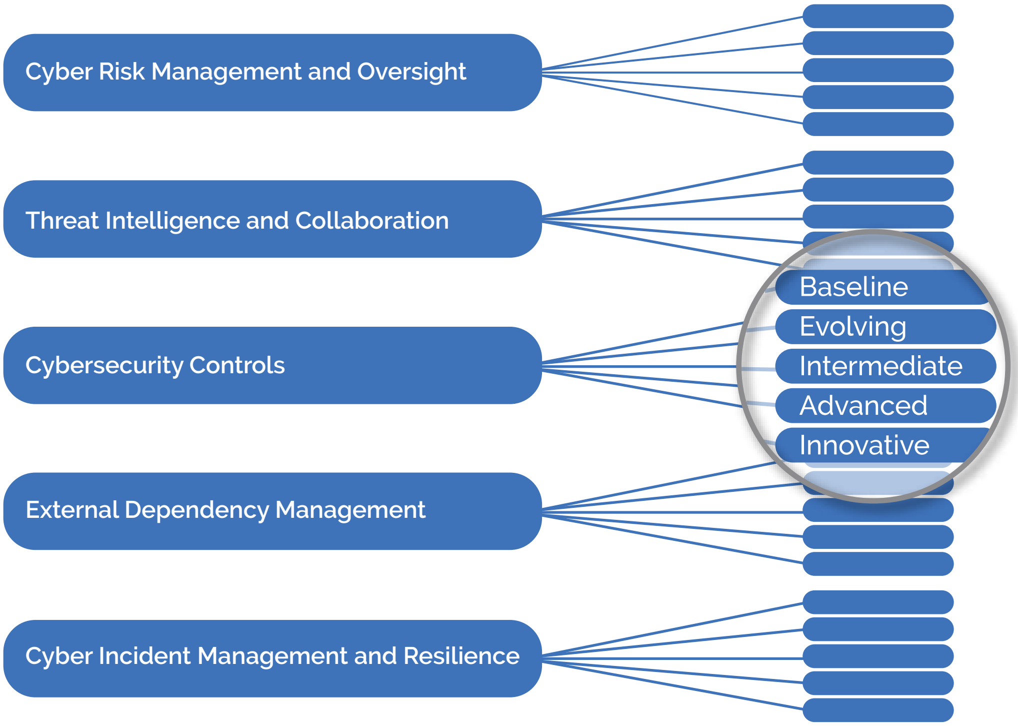
Update as frequently as possible the inherent risk profile or maturity questionnaire when anything changes

Background

In July, 2015 the Federal Financial Institutions Examination Council (FFIEC), in conjunction with the National Institute Standards of Technology (NIST), developed the Cybersecurity Assessment Tool (CAT) to help financial institutions identify their risks and determine their cyber-security preparedness. Banks can use the assessment tool's inherent risk profile to categorize their risk from areas of most concern to least. Once their inherent risks are identified they can rank their cyber-security maturity level from having the bare baseline of security essentials to being proactive and innovative.

The assessment tool consists of two main sections:

- **Inherent risk profile**: Identifies the amount of risk posed to a bank by the types, volume, and complexity of the bank's technologies and connections, delivery channels, products and services, organizational characteristics, and external threats — notwithstanding the bank's risk-mitigating controls.
- **Cybersecurity maturity**: Evaluated in five domains: Cyber Risk Management and Oversight; Threat Intelligence and Collaboration; Cybersecurity Controls; External Dependency Management; and Cyber Incident Management and Resilience. Each domain has five levels of maturity: Baseline, Evolving, Intermediate, Advanced and Innovative. A bank's appropriate cyber-security maturity levels depend on its inherent risk profile.


Cyber Risk Management and Oversight
Threat Intelligence and Collaboration
Cybersecurity Controls
External Dependency Management
Cyber Incident Management and Resilience
Baseline
Evolving
Intermediate
Advanced
Innovative

Introduction

There are multiple benefits to financial institutions performing this exercise, including:

- Identifying factors contributing to and determining the institution's overall cyber risk. This will allow you to understand your institution's exposure and risk appetite.
- Assessing the institution's cybersecurity preparedness. This will help determine how ready you are to defend against an attack.
- Evaluating whether the institutions cybersecurity preparedness is aligned with its risks. In other words, are you prepared for threats you have identified?
- Determining risk management practices and controls that could be taken to achieve the institutions desired state of cyber preparedness. This helps ensure that management has established procedures in case of an incident.
- Informing risk management strategies. Do organizations know or understand management's risk appetite and does training reflect that?

Assessing internal risks and using the FFIEC tool to understand the maturity of your security program will allow Cybersecurity and Risk Officers to focus on the areas of need. In simple terms, "You don't know what you don't know," so evaluating your internal risks will allow you to proactively see where your organization is vulnerable and identify remediation steps to close those identified gaps. The FFIEC assessment tool helps to highlight the areas of security risk and identify potential solutions that can help financial institutions move up the maturity matrix toward "Innovative" status.

Another notable opportunity lies in integrating the CAT's inherent questionnaire into existing risk calculations your organization is currently performing. By upgrading your existing risk management programs with these new sets of questions and responses you can create automated risk rankings that will improve the accuracy and mitigation response time for known vulnerabilities. There is also a benefit in having management's awareness for attestations to known vulnerabilities for audit evidence and preparedness. This is also incorporated into Sarbanes and Oxley (SOX) 2002 section 404 reporting.

Inherent Risk Profile

The inherent risk profile includes a list of questions about specific risk categories and it is critical that the responses be based on current information. The individual or team completing the profile should not guess at the answers; the inability to accurately complete the assessment is itself a vulnerability. For example, not knowing the number of personal devices allowed to connect to the corporate network at any point in time would be a concern. Another aspect that can be difficult to pin down is the number of third parties — including organizations (e.g. vendors and subcontractors) and individuals within those organizations — with access to internal systems (e.g., virtual private network, modem, intranet, direct connection). This assessment will provide valuable insights into existing inherent risks, provided that the responses are accurate and timely.

To complete the Inherent Risk Profile, respondents use the guidance comments to identify the appropriate Risk Level (Least-Minimal-Moderate-Significant-Most) for each of the sections below.

Technologies and Connection Types: Some of the topics covered in this category include the number of Internet service provider (ISP) and third-party connections; whether systems are hosted internally or outsourced; the number of unsecured connections; the use of wireless access; volume of network devices; end-of-life systems; extent of cloud services; and use of personal devices.

Key Considerations:

» There are risks associated with third party providers for connections and storage services. An institution must also have a third party risk assessment procedure in place to be able to accurately depict their inherent risk.

» The more devices connected to the network increases inherent risk, the ability to have an approval and monitoring system around all devices will enhance the institutions maturity.

» Known vulnerabilities for end of life systems include: being incompliant for not having a patch management system; leaving gaps and with unhardened systems; and costly maintenance.

Delivery Channels: Inherent risk increases as the variety and number of delivery channels increases. This category addresses whether products and services are available through online and mobile delivery channels and the extent of automated teller machine (ATM) operations.

Key Considerations:

- More e-commerce and online payment applications are available than ever before.
- The increasing number of platforms for consumer purchases and banking transactions opens more vectors for advanced attacks on both personal and financial information, such as personal identification name and address, as well as bank account and credit card information.
- ATMs pose an external threat to banks that are not able to monitor them for malware injections or other malicious attached device attacks. It's imperative to have an alert system for any intrusions into ATM fixed function application and unapproved devices.

Online/Mobile Products and Technology Services: This category includes various payment services, such as debit and credit cards, person-to-person payments, originating automated clearing house (ACH), retail wire transfers, wholesale payments, merchant remote deposit capture, treasury services and clients and trust services, global remittances, correspondent banking, and merchant acquiring activities. This category also includes consideration of whether the institution provides technology services to other organizations.

Key Considerations:

- Financial intuitions should weigh inherent risk from accepting payments in house versus outsourcing them.
- Financial institutions should consider PCI compliance as well as the financial services regulations.
- Credit card data should be isolated from the corporate network and monitored in real time for anomalous behavior and threats.

Organizational Characteristics: This category considers organizational characteristics, such as mergers and acquisitions, number of direct employees and cybersecurity contractors, changes in security staffing, the number of users with privileged access, changes in information technology (IT) environment, locations of business presence, and locations of operations and data centers.

Key Considerations:

- People account for a large portion of inadvertently creating risk in a company by the lack of security training.
- Privileged account access should be limited and tight supervision should be placed on administrators.
- Financial institutions should consider operations and changes to the business environment when measuring inherent cyber security risk.

External Threats: The volume and type of attacks (attempted or successful) affect an institution's inherent risk exposure. This category considers the volume and sophistication of the attacks targeting the institution.

Key Considerations:

- Consider similar institutions that have had breaches or security incidents.
- Threat factors that were used against those competitors will provide a stepping-stone for known vulnerabilities common to the industry. Other competitors that had security incidents, they can use those to see what common threats are out there or similar things they should be looking for.

At the end of the questionnaire you will total the columns labels selected for each category question.

Cybersecurity Maturity Level

After the inherent risks are scored the next step is to determine your financial institution's overall maturity level — ranked from "Baseline" to "Innovative" — in each of the 5 domains (see Table 1 for guidance).

TABLE 1: MATURITY LEVELS DEFINED

Maturity Levels Defined	
Baseline	Baseline maturity is characterized by minimum expectations required by law and regulations or recommended in supervisory guidance. This level includes compliance-driven objectives. Management has reviewed and evaluated guidance.
Evolving	Evolving maturity is characterized by additional formality of documented procedures and policies that are not already required. Risk-driven objectives are in place. Accountability for cybersecurity is formally assigned and broadened beyond protection of customer information to incorporate information assets and systems.
Intermediate	Intermediate maturity is characterized by detailed, formal processes. Controls are validated and consistent. Risk-management practices and analysis are integrated into business strategies.
Advanced	dvanced maturity is characterized by cybersecurity practices and analytics that are integrated across lines of business. Majority of risk-management processes are automated and include continuous process improvement. Accountability for risk decisions by frontline businesses is formally assigned.
Innovative	Innovative maturity is characterized by driving innovation in people, processes, and technology for the institution and the industry to manage cyber risks. This may entail developing new controls, new tools, or creating new information-sharing groups. Real-time, predictive analytics are tied to automated responses.

DOMAIN 1:
CYBER RISK MANAGEMENT AND OVERSIGHT

Assessment Factors include: Governance; Risk Management; Resources; Training and Culture

- **Governance**: Covers strategies for maintaining policy and oversight in cybersecurity initiatives. Governance of critical business assets for financial services should include inventory assessment for applicable assets and maintenance of policies for protecting them against advanced threats. Baseline status indicates that management is having discussions about risks related to critical infrastructure while an institution with an Innovative maturity level has a committee to verify management's actions for mitigating risks around said critical infrastructure. Policies should be updated and enforcement should be verified, as well as establishing formal IT asset management inventory with real time accuracy and classification management. These aspects are necessary in order to be considered Innovative in governance maturity.
- **Risk Management**: Financial institutions should have assigned officers for risk management and responsibility for critical business assets. The risk management function identifies and analyzes commonalities in cyber events that occur both at the institution and across other sectors to enable more predictive risk management. There should be a process is in place to analyze the financial impact that a cyber incident at the institution may have across the financial sector.

  Organizations should establish a risk management program that performs real time risk assessments and audit functionality. To be considered Innovative, an institution's risk assessments should be updated in real time as changes to the inherent risk profile occur, new applicable standards are released or updated, and new exposures are anticipated. Innovative institutions use information from risk assessments to predict threats and drive real-time responses, as well as advanced or automated analytics.

  Institutions should have internal audit teams to identify gaps in existing security measures. Automated audit reporting for external audits is essential for preparedness and accuracy.
- **Resources**: Includes staffing, tools, and budgeting processes to ensure the institution's staff or external resources have knowledge and experience commensurate with the institution's risk profile. Cybersecurity staffing should include proper training and industry news seminars for up to date trends and threat monitoring.
- **Training and Culture**: Includes the employee training and customer awareness programs contributing to an organizational culture that emphasizes the mitigation of cybersecurity threats. Having a security awareness program and testing its effectiveness will enhance overall security culture.

DOMAIN 2:
THREAT INTELLIGENCE AND COLLABORATION

- **Threat intelligence**: Covers the identification, tracking, and ability to predict cyber threats. An Innovative institution has a threat analysis system that automatically correlates threat data to specific risks and then takes risk-based automated actions while alerting management. The institution is investing in the development of new threat intelligence and collaboration mechanisms (e.g., technologies, business processes) that will transform how information is gathered and shared. There are a number of open source threat intelligence feeds that can provide quicker and the most up-to-date threat intelligence.
- **Monitoring and Analyzing**: Considers how an institution monitors threats and what analysis is performed to identify and remediate vulnerabilities tied to the targeted threats. Integrating with other threat intelligence sources and systems is the best holistic approach for monitoring and alerting for advanced threats. Automatic alerting that is meaningful and compelling can narrow your scope from traditional log mining techniques that typically produce many false positives. While a Baseline level institution logs security events and uses those logs for post-event investigations, an Innovative one has multiple intelligence inputs and tools that enable it to predict attacks and trends.
- **Information Sharing**: Encompasses establishing relationships with peers and information-sharing forums and how threat information is communicated to those groups as well as internal stakeholders. Sharing cyber threat intelligence with business units in real time including the potential financial and operational impact of inaction is key towards becoming more Innovative. A system should automatically inform management of the level of business risk specific to the institution and the progress of recommended steps taken to mitigate the risks.

DOMAIN 3: CYBERSECURITY CONTROLS

» **Preventative**: The controls for preventative security measures include infrastructure management, access and asset management, device/endpoint security, and secure coding practices. Innovative institutions are maintaining risk scores for all of their infrastructure assets and updates in real time based on threats, vulnerabilities, or operational changes. An institution should have a process for managing customer, employee, and third-party authentication and access. There should also be a mix of encryption and authentication for sensitive transactions and information. Endpoint protection is critical as that's where data resides and is the most prized possession from a malicious attack. To protect the golden jewels there should be a centralized end-point management tool that provides fully integrated patch, configuration, and vulnerability management, while also being able to detect malware upon arrival to prevent a security incident and/or attack. Secure coding practices are essential for limiting vulnerabilities found in new software and, automated tools in the development environment should actively scan software code so that security weaknesses can be resolved immediately during the design phase.

» **Detective**: Activities performed for detective controls include: threat and vulnerability detection, anomalous behavior activity detection, and event detection. Having a central console that consolidates and provides alerts in real time about both insider and outsider threats would help an organization qualify as Innovative for detective threat and vulnerability measures. There should be automatic alerts when anomalous behavior or security events occur. The reporting features from the detective solution should provide traceability of the entire timeline of any security event and respond with corrective actions in real time.

» **Corrective**: Patch management and remediation are considered corrective controls. To achieve Innovative status there should be a formal process in place to acquire, test, and rapidly deploy software patches based on criticality, and systems should be configured to retrieve patches automatically. Remediation steps are key to get all systems back to acceptable levels for operations and resolved from a security incident. The institution should will be able to remediate systems damaged by zero-day attacks to maintain current recovery time objectives. Remediation is only effective if it happens quickly — otherwise, the intended damage is done. Remediation steps after vulnerability scans, pen tests, risk assessments, and security incidents, should all be in real-time to achieve Innovative maturity.

DOMAIN 4: EXTERNAL DEPENDENCY MANAGEMENT

- **Connections**: Includes the identification, monitoring, and management of external connections and data flows to third parties. To be considered Innovative, an institution should maintain a monitoring tool that records involvement with third parties via inbound/outbound connections, web portals, or other means of data transfer, this tool should also have real time alerts for incidents such as unauthorized access attempts and anomalous behavior.
- **Relationship Management**: Includes due diligence, contracts, and ongoing monitoring to help ensure controls complement the institution's cybersecurity program. Third party risk assessment teams and management should conduct the proper due diligence when selecting third parties that have some kind of elevated data access privilege. Diagraming how they receive, store, process, transmit, and ultimately delete the information to which they have access is an essential step of third party risk management. Contract language should be structured to secure critical assets and require performance baselines from vendors and contractors.

DOMAIN 5:
CYBER INCIDENT MANAGEMENT AND RESILIENCE

- **Incident Resilience Planning & Strategy**: Incorporates resilience planning and testing into existing business continuity and disaster recovery plans to minimize service disruptions and the destruction or corruption of data. Baseline level organizations have identified roles and responsibilities, and have a communications plan in the event of an incident, whereas at Innovative institutions, the incident response plan is designed to ensure recovery from disruption of services, assurance of data integrity, and recovery of lost or corrupted data following a cybersecurity incident. The incident response process also includes detailed actions and rule-based triggers for automated response. Depending on the nature of an institution's business, defined recovery time objectives and baseline for recovery should be stated in the planning documentation.
- **Detection, Response, & Mitigation**: Refers to the steps management takes to identify, prioritize, respond to, and mitigate the effects of internal and external threats and vulnerabilities. In an Innovative environment the organization is able to detect and block zero-day attempts and inform management and the incident response team in real time. Incident response teams should be able to trace a security incident through the entire process tree to see how it occurred and create future remediation action plans around the vulnerability that was exploited.
- **Escalation & Reporting**: Ensures key stakeholders are informed about the impact of cyber incidents, and that regulators, law enforcement, and customers are notified as required. A mechanism should be in place to ensure real time notification of incidents to management and essential employees through multiple communication channels, with tracking and verification of receipt. Having a real time alert and reporting solution will allow for management to escalate critical events in a timely manner and possibly avoid lengthy public news articles and press from occurring if mitigated appropriately.

Carbon Black provides responses to the inherent risk profile for areas such as asset inventory and (internal/external) connections, as well as other categories. The case study provided later in this guide demonstrates this, as well as how you can achieve an Innovative maturity stance using real time threat detection and response.

One of the key areas where Carbon Black can improve your cyber security is by helping you develop a real time asset inventory, thus shedding light on existing components and systems that may have gone unnoticed by traditional solutions. Further, the risk ranking scores provided by Carbon Black Threat Intel facilitates the ability to create watch lists in Carbon Black Enterprise Response, allowing real-time monitoring and alerting based on indicators of compromise and other factors. Innovative maturity is built with automated, repeatable real time vulnerability assessment, as well as monitoring and alerting.

The days of periodic assessments are far behind us; the more that cyber security professionals have access to instant threat analytics and remediation solutions, the more proactive they can be about incident response. Robust endpoint protection is essential for safeguarding critical data and stopping advanced attacks that typical perimeter solutions miss.

The FFIEC CAT spotlights the need for financial institutions to build cyber security risk programs into their existing frameworks for risk management. Carbon Black can assist management with initially determining their upfront risk by nature of their business transactions and operations, and then show how they can enhance their security levels to becoming more innovative.

Risk/Maturity Relationship

Now that you have walked through the inherent risk profile and rated your institution on the five domains for cyber security maturity, you can assess your overall risk-maturity relationship. Determine the areas your organization fits into table two below.

From there, your next step may involve identifying those solutions that lower your inherent risk while improving your cyber security maturity (e.g. contracting with a third party for processing secure credit card transactions, while maintaining a secure third party vendor selection process).

TABLE 2: RISK/MATURITY RELATIONSHIP

Risk/Maturity Relationship		*Inherent Risk Levels*				
		Least	Minimal	Moderate	Significant	Most
Cyber Security Maturity Level for Each Domain	**Innovative**				🟦	🟦
	Advanced			🟦	🟦	🟦
	Intermediate		🟦	🟦	🟦	
	Evolving	🟦	🟦	🟦		
	Baseline	▒	▒	■	■	■

Case Study: ABC National Bank

ABC Bank is a National Bank with approximately 13000 employees, 1000 banking locations and a corporate office headquarters in the central U.S. region. Established in the late 1960's, the bank has grown and acquired other smaller regional banks in North America. ABC operates through four segments: branch banking (deposit accounts and loans for consumers and small businesses); commercial banking (lending, leasing, and syndicated and trade finance for corporate clients); consumer lending (residential mortgages, home equity loans, and credit cards); and investment advisors (private banking, brokerage, and asset management).

INHERENT RISK PROFILE

The inherent risk profile has been answered to match the industry average responses for the size and product offerings of this type of banking institution. For the detailed profile answers for the inherent and cyber security maturity assessment model please use this excel link as an appendix:

Business Case:

- Have some end-of-life (EOL) systems still in use, including Windows XP and Windows Server 2003, the bank has not yet made an upgrade plan.
- ATMs, wire transfers, ACH and mobile banking applications
- The bank has already experienced security incidents phishing emails sent to customers, and hacking attempts via ATMs infected with malware
- IT Security Director has left the Bank

TABLE 3: INHERENT RISK SCORE

Inherent Risk Score 507.69

Category	Weights	Data Points	<=200 Least	201-400 Minimal	401-600 Moderate	601-800 Sigificant	801-1000 Most
Technologies and connection Types	1	14	0	8	4	2	0
Delivery Channels	1	3	0	0	1	2	0
Organizational Characteristics	1	7	1	0	6	0	0
Online/Mobile Products and Technological Services	1	14	3	3	8	0	0
External Threats	1	1	0	0	1	0	0
Totals	5	39	4	11	20	4	0
			10.26%	**28.21%**	**51.28%**	**10.26%**	**0.00%**

Click the table for the full analysis of the Inherent Risk Score calculation

ABC National Bank's inherent risk profile reveals that they have moderate cyber security risk based on the nature of operations and business transactions they perform. E-banking and mobile banking applications increases inherent risk for obvious reasons but banks have to become innovative in securing these technologies as customer demand for them continues to rise. Conducting regular external penetration tests and application risk assessments are key steps in assessing residual risk once existing security solutions are considered.

Many national banks have EOL systems still in place due to the large amount of infrastructure they have to maintain. Upgrades are costly and often cannot be budgeted for the foreseeable future, leaving financial institutions with few options to secure these legacy systems. They can purchase support packages, which only provide critical patches and leave systems vulnerable. Also, regulations such as PCI DSS require an up to date patch management system, which is not possible with an extended support package, so the institution faces a compliance audit failure. Further, the support packages are very costly, especially if used for an extended period.

Financial institutions that need to keep EOL systems in place should incorporate a compensating control to mitigate the vulnerabilities. Such a solution should protect against all types of malware while only allowing set processes to run. Organizations should also isolate EOL systems from the main infrastructure while hardening them as much as possible.

> The Carbon Black Security Platform tracks, in real time, asset inventory, third party connections, transaction data, as well as covering many other needs identified in the Inherent Risk Profile. The solution helps identify inherent risks for this cyber security assessment while enhancing the organizations overall maturity level.

CYBER SECURITY MATURITY LEVEL
DOMAIN 1: CYBER RISK MANAGEMENT AND OVERSIGHT

TABLE 4: DOMAIN 1 SUMMARY

Domain 1 Totals	Baseline	Evolving	Intermediate	Advanced	Innovative	Total	# Y	#N
Governance	16	11	15	15	5	62	33	29
Risk Management	8	11	10	9	7	45	18	27
Resources	2	4	1	2	1	10	6	4
Training and Culture	5	8	7	2	2	24	10	14
Grand Total						**141**	**67**	**74**

Click the table for the full spreadsheet view of the Domain 1 analysis

DOMAIN 1 SUMMARY

ABC's Domain 1 cyber security maturity results are as follows:

- Governance: **Intermediate**
- Risk Management: **Evolving**
- Resources: **Evolving**
- Training: **Evolving**
- Culture: **Evolving**

How Carbon Black Can Help Improve Domain 1 Cyber Security Maturity

Governance: IT Asset Management is an area for improvement, as ABC National Bank does not have a formal change management system deployed in its environment.

> ABC could use Carbon Black Enterprise Protection's change management policies, which include tracking all change approvals and recording unauthorized attempts. With CB Protection, ABC can also track baseline configurations and drift analysis over time.

Risk Management and Risk Assessment: ABC is not able to assess threat intelligence or automate risk rankings in real time. They answered No to "Advanced or automated analytics offer predictive information and real-time risk metrics", and "The institution uses information from risk assessments to predict threats and drive real-time responses."

> Both CB Protection and CB Response offer real-time threat detection and response via Carbon Black Threat Intel, which aggregates real-time threat data across the most advanced attacks. This provides instant insight to risk rankings of files, software versions, and publishers. ABC Bank does not have a real time audit function, which would be needed for compliance and internal control attestations. CB Protection's offers a console view with up to date policy enforcement and reporting.

DOMAIN 2: THREAT INTELLIGENCE AND COLLABORATION

TABLE 5: DOMAIN 2 SUMMARY

Domain 2 Totals	Baseline	Evolving	Intermediate	Advanced	Innovative	Total	# Y	# N
Threat Intelligence	3	1	3	3	2	12	6	6
Monitoring and Analyzing	2	4	4	5	3	18	10	8
Information Sharing	3	2	4	3	3	15	9	6
Grand Total						**45**	**25**	**20**

Click the table for the full spreadsheet view of the Domain 2 analysis

DOMAIN 2 SUMMARY

ABC's Domain 2 Maturity Results:

- Threat Intelligence: **Intermediate**
- Monitoring and Analyzing: **Intermediate**
- Information Sharing: **Intermediate**

How Carbon Black Can Help Improve Domain 2 Cyber Security Maturity

Domain 2 is concentrated on threat intelligence, the ability to monitor and analyze systems and threats in real time, and the ability to share knowledge of threats to the appropriate parties. To become more innovative, ABC Bank needs a threat analysis system that automatically correlates threat data to specific risks and then takes risk-based automated actions while alerting management.

> Carbon Black Threat Intel is a comprehensive, aggregated advanced threat intelligence solution that combines leading software reputation, threat indicator and attack classification services to provide some of the industry's most powerful, correlated and accurate threat insight.

To achieve a more mature status, ABC would also need to use multiple sources of intelligence, correlated log analysis, alerts, internal traffic flows, and geopolitical events to predict potential future attacks and attack trends. Organizations need to combine threat intelligence from a variety of proprietary and third-party sources.

> CB Threat Intel combines unique threat intelligence and industry-leading third-party intelligence sources to empower security professionals to optimize and improve their prevention, detection, response and recovery capabilities.

ABC should also consider how it shares threat information within the organization. They should procure a mechanism for sharing cyber threat intelligence with business units in real time, including the potential financial and operational impact of inaction.

> The threat intelligence produced by Carbon Black's Threat Research Team is based on analysis from millions of endpoints, providing unique insight into threat behaviors. This results in two cloud-delivered services: threat indicators for emerging attacks and reputation intelligence for known-good, known-bad and unproven software and domains. These two services are further complemented by the Attack Classification Service for attack context and attack attribution.
>
> The combination of this aggregated intelligence—seamlessly integrated with both CB Protection and CB Response—enables security operations and incident response professionals to define trust policies for multiple forms of advanced threat prevention, build custom detection events tailored to specific business requirements, accelerate investigations during a response, and proactively hunt for threats.

DOMAIN 3: CYBERSECURITY CONTROLS

TABLE 6: DOMAIN 3 SUMMARY

Domain 3 Totals	Baseline	Evolving	Intermediate	Advanced	Innovative	Total	# Y	#N
Preventative Controls	33	21	21	10	11	96	70	26
Detective Controls	14	11	11	12	6	54	25	29
Corrective Controls	4	7	7	3	4	24	16	8
Grand Total						**174**	**111**	**63**

Click the table for the full spreadsheet view of the Domain 3 analysis

DOMAIN 3 SUMMARY

ABC's Domain 3 cyber security maturity results are as follows:

- » Preventative Controls: **Intermediate**
- » Detective Controls: **Intermediate**
- » Corrective: **Intermediate**

How Carbon Black Can Help Improve Domain 3 Cyber Security Maturity

A notable opportunity for ABC to improve its cyber security maturity would be to utilize a centralized end-point management tool that provides fully integrated patch, configuration, and vulnerability management, while also being able to detect malware upon arrival to prevent an exploit such as an advanced zero day attack.

> CB Protection provides real-time visibility, detection, response, and proactive, customizable signature-less prevention from advanced persistent threats and zero day attacks.

ABC is currently unable to provide risk scores all of its infrastructure assets and updates in real time based on threats, vulnerabilities, or operational changes.

> At the heart of Cb Protection is a unique, policy-driven approach to application control. It combines real-time visibility and a file discovery agent, with IT-driven controls aided by trust ratings from Cb Threat Intel, to help organizations simplify and automate the set-up and administration of a secure whitelisting platform. This results in a customizable application control solution that combines the highest level of advanced threat protection with minimal end-user impact and administrative overhead.

Becoming more innovative in domain three means having detective controls that alert in real time when triggered events occur, while properly communicating with other controls to remediate and respond using those preventative controls.

> CB Protection offers three levels of preventative protection:
>
> **Default-Deny**: allows only software you trust to run and treats everything else as suspicious.
>
> **Detonate-and-Deny**: Cb Protection automatically sends files from endpoints to network detonation services to be detonated and evaluated for suspicious behavior.
>
> **Detect-and-Deny**: Leverages advanced threat indicators to identify patterns of compromise and enables a security administrator to identify and ban malicious files where appropriate with little to no end-user impact.
>
> Cb Response allows security professionals to understand the root cause of an attack and immediately take steps to remediate and respond. The responder can isolate a particular endpoint from the rest of the environment to prevent further damage, but maintain the connection to the Cb Response console to enable a detailed investigation into the incident.

DOMAIN 4: EXTERNAL DEPENDENCY MANAGEMENT

TABLE 7: DOMAIN 4 SUMMARY

Domain 4 Totals	Baseline	Evolving	Intermediate	Advanced	Innovative	Total	# Y	#N
Connections	4	4	4	2	2	16	11	5
Relationship Management	12	9	5	5	4	35	28	7
Grand Total						**51**	**39**	**12**

Click the table for the full spreadsheet view of the Domain 4 analysis

DOMAIN 4 SUMMARY

ABC's Domain 4 cyber security maturity results are as follows:

- Connections: **Intermediate**
- Relationship Management: **Intermediate**

How Carbon Black Can Help Improve Domain 4 Cyber Security Maturity

Domain 4 is focused on third-party security and the risk associated with sensitive data sharing and access control. ABC would improve its maturity level by having real time updates for monitoring third-party activity around critical assets and access to internal connections.

> ABC National Bank could utilize Cb Protection's alert mechanism when connections are made to unauthorized third parties. This is necessary for financial institutions who rely on many third party providers for sensitive financial transactions and data storage.

Another important factor in Domain 4 is the ability for to be segment or sever connections instantaneously to prevent contagion from cyber attacks.

> Using Cb Response, responders can contain active intrusions instantly with one click by remotely isolating one or multiple endpoints from communicating with the network.
> By still maintaining an active connection with the Carbon Black server — even while isolated — IR teams can perform more conclusive and surgical investigations on or off the network.

DOMAIN 5: CYBER INCIDENT MANAGEMENT AND RESILIENCE

TABLE 8: DOMAIN 5 SUMMARY

Domain 5 Totals	Baseline	Evolving	Intermediate	Advanced	Innovative	Total	# Y	#N
Incident Resilience Planning and Strategy	9	8	9	8	6	40	29	11
Detection, Response, and Mitigation	4	9	9	5	3	30	15	15
Escalation and Reporting	4	3	3	2	1	13	9	4
Grand Total						**43**	**24**	**19**

Click the table for the full spreadsheet view of the Domain 5 analysis

DOMAIN 5 SUMMARY

ABC's Domain 5 cyber security maturity results are as follows:

- Incident Resilience Planning and Strategy: **Advanced**
- Detection, Response, and Mitigation: **Intermediate**
- Escalation and Reporting: **Intermediate**

How Carbon Black Can Help Improve Domain 5 Cyber Security Maturity

Like many institutions ABC Bank is very good at planning and strategy but needs improvement with getting the proper mechanisms in place to execute on those plans.

> With Cb Response's live response for endpoint threat inspection, termination & remediation, ABC's responders could understand the current state of an endpoint, perform remote live investigations, intervene with ongoing attacks, and instantly remediate endpoint threats. This enables incident responders to "see" and "touch" endpoints to take immediate action during an investigation — even while the endpoint remains isolated from the rest of the network.

To become more innovative, ABC should also have a mechanism in place to provide instantaneous notification of incidents to management and essential employees through multiple communication channels, with tracking and verification of receipt.

> Cb Response provides detailed alert notifications via its dashboard and via email, as well as detailed reporting.

OVERALL RISK MATURITY

As a final exercise, we compared ABC National Bank's cyber maturity assessment with and without the Carbon Black Security Platform on their endpoints enterprise wide. The analysis was done using two different target maturity levels — Intermediate and Innovative. The CAT allows you to set your desired target based on your appetite for risk.

First, we scored ABC using an "Intermediate" target level. Based on the current mix of technologies, ABC achieves an 82.11% Intermediate maturity (see Table 9).

TABLE 9: ABC'S INTERMEDIATE MATURITY SCORE — STATUS QUO

Maturity Achieved Against Defined Targets

82.11% Intermediate (status quo)

Domain	Desired Target	% Achieved	Maturity	Achieved	Statements	Least	Minimal	Moderate	Significant	Most
Cyber Risk Management and Oversight	Intermediate	64.89%	*Innovative*	1	15				6.67%	6.67%
			Advanced	5	32			15.63%	15.63%	15.63%
			Intermediate	7	29		24.14%	24.14%	24.14%	
			Evolving	23	34	67.65%	67.65%	67.65%		
			Baseline	31	31	100.00%	100.00%			
Threat Intelligence and Collaboration	Intermediate	88.46%	*Innovative*	0	8				0.00%	0.00%
			Advanced	2	11			18.18%	18.18%	18.18%
			Intermediate	8	11		72.73%	72.73%	72.73%	
			Evolving	7	7	100.00%	100.00%	100.00%		
			Baseline	8	8	100.00%	100.00%			
Cyber Security Controls	Intermediate	80.62%	*Innovative*	2	20				10.00%	10.00%
			Advanced	5	25			20.20%	20.20%	20.20%
			Intermediate	23	39		58.97%	58.97%	58.97%	
			Evolving	30	39	76.92%	76.92%	76.92%		
			Baseline	51	51	100.00%	100.00%			
External Dependency Management	Intermediate	86.84%	*Innovative*	0	6				0.00%	0.00%
			Advanced	3	7			42.86%	42.86%	42.86%
			Intermediate	6	9		66.67%	66.67%	66.67%	
			Evolving	13	13	100.00%	100.00%	100.00%		
			Baseline	16	16	100.00%	100.00%			
Cyber Incident Management and Resilience	Intermediate	84.48%	*Innovative*	1	10				10.00%	10.00%
			Advanced	3	15			20.20%	20.20%	20.20%
			Intermediate	15	21		71.43%	71.43%	71.43%	
			Evolving	17	20	85.00%	85.00%	85.00%		
			Baseline	17	17	100.00%	100.00%			

Next, we added the Carbon Black Security Platform into the security infrastructure and again targeted "Intermediate." That analysis, shown in Table 10, found ABC moving from 82% to 93% Intermediate.

TABLE 10: ABC'S INTERMEDIATE MATURITY SCORE — WITH CARBON BLACK

Maturity Achieved Against Defined Targets

92.98% Intermediate (incorporating Carbon Black)

Domain	Desired Target	% Achieved	Maturity	Achieved	Statements	Least	Minimal	Moderate	Significant	Most
Cyber Risk Management and Oversight	Intermediate	73.40%	*Innovative*	7	15				46.67%	46.67%
			Advanced	11	32			34.38%	34.38%	34.38%
			Intermediate	9	29		31.03%	31.03%	31.03%	
			Evolving	29	34	85.29%	85.29%	85.29%		
			Baseline	31	31	100.00%	100.00%			
Threat Intelligence and Collaboration	Intermediate	100.00%	*Innovative*	4	8				50.00%	50.00%
			Advanced	5	11			45.45%	45.45%	45.45%
			Intermediate	11	11		100.00%	100.00%	100.00%	
			Evolving	7	7	100.00%	100.00%	100.00%		
			Baseline	8	8	100.00%	100.00%			
Cyber Security Controls	Intermediate	91.47%	*Innovative*	8	20				40.00%	40.00%
			Advanced	16	25			64.00%	64.00%	64.00%
			Intermediate	32	39		82.05%	82.05%	82.05%	
			Evolving	35	39	89.74%	89.74%	89.74%		
			Baseline	51	51	100.00%	100.00%			
External Dependency Management	Intermediate	100.00%	*Innovative*	0	6				0.00%	0.00%
			Advanced	3	7			42.86%	42.86%	42.86%
			Intermediate	9	9		100.00%	100.00%	100.00%	
			Evolving	13	13	100.00%	100.00%	100.00%		
			Baseline	16	16	100.00%	100.00%			
Cyber Incident Management and Resilience	Intermediate	100.00%	*Innovative*	6	10				60.00%	60.00%
			Advanced	8	15			53.33%	53.33%	53.33%
			Intermediate	21	21		100.00%	100.00%	100.00%	
			Evolving	20	20	100.00%	100.00%	100.00%		
			Baseline	17	17	100.00%	100.00%			

Extending the analysis further, we ran the numbers using the highest — "Innovative" — target level. Based on the status quo, ABC scores at 61% Innovative (Table 11).

TABLE 11: ABC'S INNOVATIVE MATURITY SCORE — STATUS QUO

Maturity Achieved Against Defined Targets

61.05% Innovative (status quo)

Domain	Desired Target	% Achieved	Maturity	Achieved	Statements	Least	Minimal	Moderate	Significant	Most
Cyber Risk Management and Oversight	Innovative	47.52%	*Innovative*	1	15				6.67%	6.67%
			Advanced	5	32			15.63%	15.63%	15.63%
			Intermediate	7	29		24.14%	24.14%	24.14%	
			Evolving	23	34	67.65%	67.65%	67.65%		
			Baseline	31	31	100.00%	100.00%			
Threat Intelligence and Collaboration	Innovative	55.56%	*Innovative*	0	8				0.00%	0.00%
			Advanced	2	11			18.18%	18.18%	18.18%
			Intermediate	8	11		72.73%	72.73%	72.73%	
			Evolving	7	7	100.00%	100.00%	100.00%		
			Baseline	8	8	100.00%	100.00%			
Cyber Security Controls	Innovative	63.79%	*Innovative*	2	20				10.00%	10.00%
			Advanced	5	25			20.00%	20.00%	20.00%
			Intermediate	23	39		58.97%	58.97%	58.97%	
			Evolving	30	39	76.92%	76.92%	76.92%		
			Baseline	51	51	100.00%	100.00%			
External Dependency Management	Innovative	74.51%	*Innovative*	0	6				0.00%	0.00%
			Advanced	3	7			42.86%	42.86%	42.86%
			Intermediate	9	9		66.67%	66.67%	66.67%	
			Evolving	13	13	100.00%	100.00%	100.00%		
			Baseline	16	16	100.00%	100.00%			
Cyber Incident Management and Resilience	Innovative	63.86%	*Innovative*	1	10				10.00%	10.00%
			Advanced	3	15			20.00%	20.00%	20.00%
			Intermediate	15	21		71.43%	71.43%	71.43%	
			Evolving	17	20	85.00%	85.00%	85.00%		
			Baseline	17	17	100.00%	100.00%			

With the Carbon Black Security Platform in place, ABC's cyber security maturity score moved from 61% to 78% Innovative. Notably, the number of Innovative "controls" in place went from 4 to 25.

TABLE 12: ABC'S INNOVATIVE MATURITY SCORE — WITH CARBON BLACK

Maturity Achieved Against Defined Targets

77.65% Innovative (incorporating Carbon Black)

Domain	Desired Target	% Achieved	Maturity	Achieved	Statements	Least	Minimal	Moderate	Significant	Most
Cyber Risk Management and Oversight	Innovative	61.70%	*Innovative*	7	15				46.67%	46.67%
			Advanced	11	32			34.38%	34.38%	34.38%
			Intermediate	9	29		31.03%	31.03%	31.03%	
			Evolving	29	34	85.29%	85.29%	85.29%		
			Baseline	31	31	100.00%	100.00%			
Threat Intelligence and Collaboration	Innovative	77.78%	*Innovative*	4	8				50.00%	50.00%
			Advanced	5	11			45.45%	45.45%	45.45%
			Intermediate	11	11		100.00%	100.00%	100.00%	
			Evolving	7	7	100.00%	100.00%	100.00%		
			Baseline	8	8	100.00%	100.00%			
Cyber Security Controls	Innovative	81.61%	*Innovative*	8	20				40.00%	40.00%
			Advanced	16	25			64.00%	64.00%	64.00%
			Intermediate	32	39		82.05%	82.05%	82.05%	
			Evolving	35	39	89.74%	89.74%	89.74%		
			Baseline	51	51	100.00%	100.00%			
External Dependency Management	Innovative	80.39%	*Innovative*	0	6				0.00%	0.00%
			Advanced	3	7			42.86%	42.86%	42.86%
			Intermediate	9	9		100.00%	100.00%	100.00%	
			Evolving	13	13	100.00%	100.00%	100.00%		
			Baseline	16	16	100.00%	100.00%			
Cyber Incident Management and Resilience	Innovative	86.75%	*Innovative*	6	10				60.00%	60.00%
			Advanced	8	15			53.33%	53.33%	53.33%
			Intermediate	21	21		100.00%	100.00%	100.00%	
			Evolving	20	20	100.00%	100.00%	100.00%		
			Baseline	17	17	100.00%	100.00%			

For Domain 1 the overall maturity did not increase significantly because of the internal process and procedure nature of the domain. This domain is focused on the governance, security awareness, and people that the financial services company decides to employ.

Carbon Black's threat intelligence capabilities helped ABC improve in Domain 2, but the bank would rely on internal communications and procedures using that threat intelligence to make additional improvements.

In Domain 3 we see significant improvement in ABC's maturity posture because of the detective, protective and corrective controls provided by the Carbon Black Security Platform.

To make progress in Domain 4, the bank must rely on its internal due diligence process.

Finally, ABC saw significant improvement in Domain 5 using the Carbon Black Security Platform because of its effectiveness as an incident response and management tool.

Key Considerations:

- An Innovative cyber security stance can only be maintained by using real time detection and response.
- This is a point in time exercise so it's important to constantly update the CAT whenever there is a change to either the inherent risk profile or the five cyber maturity domains.
- Using real time metrics and reporting will allow you to quickly diagram where you are in your cyber security stance.
- Threat analytics is only as good as how you use them. Procuring solutions with aggregated threat data that can be deciphered and utilized for the most up to date watch lists will enhance your knowledge and response time.
- Use this tool as a baseline and discovery process, not an end all-be all risk measurement. Using it with your existing risk assessment processes will help your institution streamline risk management processes for assessments and audit.

Learn more about how Carbon Black can help you in your cyber security maturity please visit www.carbonblack.com.

Carbon Black.