

GOVERNANCE

[Corporate Governance](#)

[Business Ethics](#)

[Public Policy and Government
Relations](#)

[Enterprise Risk Management](#)

[Consumer Privacy and Information
Security](#)

[Third-Party Management](#)

Corporate Governance

One of our most valuable assets at Fifth Third is our reputation for integrity. We are judged by our conduct, and we must act in a manner that merits public trust and confidence.

We believe that a strong corporate governance program is the foundation for a sustainable and well-governed company. Accordingly, we continuously evaluate our structures, processes and controls to ensure they support and promote accountability, effectiveness, transparency and ethical behavior.

BOARD OF DIRECTORS

Our Board of Directors provides oversight of, and guidance to, our executive management team in the development of corporate strategy, risk management, corporate culture and other important aspects of our business, including ESG topics. In order to provide such oversight and guidance, we believe it is important that the Board include a substantial majority of independent directors, strong independent committee chairs and a diverse range of backgrounds and experiences calibrated to the evolving needs of our business and stakeholders. Our directors' average tenure is 6.3 years.

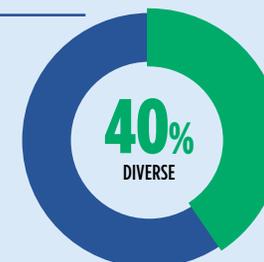
All of our directors are independent under the standards developed by Nasdaq and included in our **Corporate Governance Guidelines**, except for our CEO and one director who was formerly employed by Fifth Third and served as CEO of MB Financial, Inc. We have a lead independent director who is elected annually by the independent directors and facilitates independent Board oversight of management.

At our 2021 annual meeting, our shareholders elected 15 directors, including five female directors, two Black directors and one Latino director.

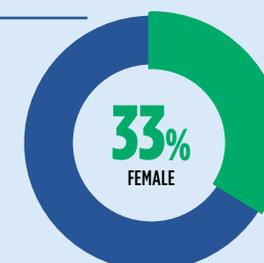
Forty percent of our Board is diverse in terms of ethnicity or gender, including our lead independent director and Audit Committee chair who are each women, and our Technology Committee chair who is Latino.

Board of Directors' Diversity

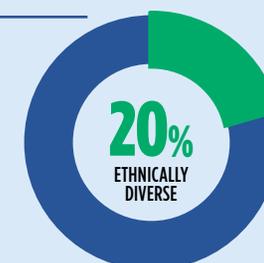
DIRECTORS' DIVERSITY



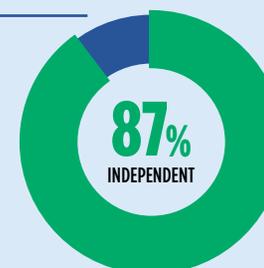
DIRECTORS' GENDER



DIRECTORS' ETHNICITY



DIRECTORS' INDEPENDENCE



Board Performance Evaluation Process



Our **2021 Proxy Statement** includes information about the Board and its committees and their respective responsibilities. It also includes a Board Skills and Attributes Matrix that sets forth the diverse skills and attributes that each director contributes to the Board's oversight of the Company. Eleven of our directors have experience in ESG matters, including all the members of the Nominating and Corporate Governance Committee.

Though evaluations occur continuously, our directors undergo a thorough annual evaluation process to help ensure that Board and committee oversight remain strong and that the mix of skills and backgrounds on the Board remains appropriate. The evaluation process includes one-on-one discussions between the lead independent director and each other independent director, full Board and committee written evaluations, and follow-up action items.

It is important that our Board represents diverse backgrounds and experiences in business, government, education, and technology.

These frank evaluations are an important part of sustainable governance and allow us to identify opportunities to enhance our effectiveness.

The NCG Committee, which oversees these Board evaluations, also is responsible for identifying and assessing potential director candidates using established criteria and our Corporate Governance Guidelines.

Each director must possess the highest personal and professional ethics and integrity and should be devoted to representing the interests of Fifth Third and our stakeholders. Directors must be willing to devote sufficient time to their duties and responsibilities. Directors also must undergo annual ethics training.

It is important that our Board represents diverse backgrounds and experiences in business, government, education, technology and in various areas relevant to our businesses. The NCG Committee carefully considers these and other factors—including judgment, diversity and skills—in determining a mix that best serves the needs of the Board and Fifth Third. **Proactive consideration of diverse candidates is an important part of the NCG Committee recruitment process** and is prioritized under our Corporate Governance Guidelines.

ESG COMMITTEE

In 2020, the NCG Committee established the Environmental, Social and Governance Committee with a charter to provide oversight and review of policies, programs, practices, strategies and approach to ESG topics that reflect Fifth Third’s Core Values.

The ESG Committee monitors emerging risks and trends through communication with stakeholders and recommendations from independent organizations such as SASB, TCFD, GRI, World Economic Forum and the United Nations. Further, **the ESG Committee monitors ESG performance with key data providers, and has oversight of climate strategy, sustainable financing and operational sustainability topics.**

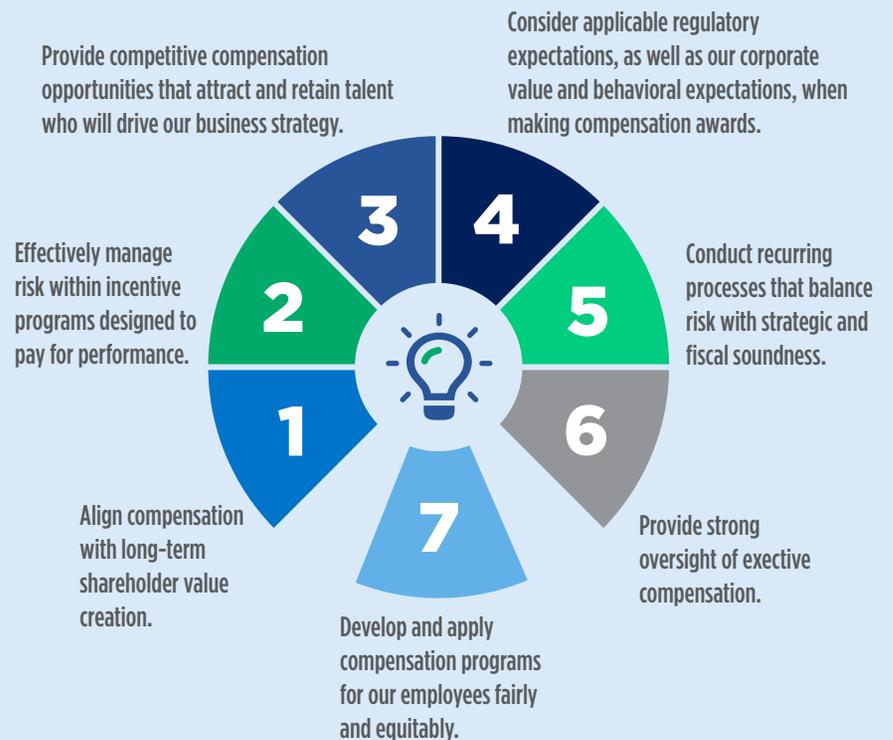
The committee is chaired by the director of ESG reporting & analytics and includes the chief financial officer, chief human resources officer, chief risk officer, chief inclusion and diversity officer, chief compliance officer and director of investor relations, as well as representatives from each line of business, legal, and the community development and social responsibility group. ESG updates are regularly given to the NCG Committee as well as the Board of Directors.

MANAGEMENT

Our management structure is intended to facilitate leadership that is effective and consistent with our corporate standards, and that promotes a strong corporate culture. **We manage our organization on a line-of-business basis, while also maintaining strong corporate functions and appropriate governance.** Our Company’s most senior management body is Enterprise, which is responsible for developing and implementing corporate strategy and managing executive-level operations. ESG updates are provided to Enterprise throughout the year. ■

Compensation Philosophy

Fifth Third endeavors to attract and retain the best talent and to motivate them to fulfill our Vision. We plan to accomplish this by establishing compensation programs that reward our people for delivering the right products to the right customers, in ways that consider our shareholders’ long-term interests and align with Fifth Third’s values, while also staying within our risk tolerance.



Business Ethics

Doing the right thing is central to achieving our Vision to be the One Bank people most value and trust.

Our Vision is a commitment that inspires our employees to create a great customer experience, an engaging workforce and vibrant communities. It forms the bedrock of Fifth Third's reputation as a respected corporate citizen. It is a commitment that begins with each Fifth Third employee.

ETHICS PROGRAM

Fifth Third's Ethics program is overseen by the chief ethics officer, who provides regular reporting on key aspects of the Ethics program to the Audit Committee and the Risk and Compliance Committee of the Board of Directors.

Reports provided include EthicsLine activity and resolutions, conflicts of interest disclosures, and culture and conduct risk dashboards.

The reports also include ethics training and communications updates and progress, Ethics program assessments and the Code of Business Conduct and Ethics.

The chief ethics officer may also escalate ethics matters directly to the Board. The Ethics program is audited and examined as part of the Fifth Third Audit schedule and the schedule of its examiners.

EMPLOYEE CODE OF CONDUCT

Our **Code of Business Conduct and Ethics** is anchored in our Fifth Third Compass, including our Core Values: Work as One Bank, Take Accountability, Be Respectful and Inclusive, and Act with Integrity. It outlines our responsibility to serve with honesty and integrity, and in compliance with both the letter and the spirit of the law.



OUR CODE OF BUSINESS CONDUCT AND ETHICS IS ANCHORED IN OUR FIFTH THIRD COMPASS, INCLUDING OUR CORE VALUES: WORK AS ONE BANK, TAKE ACCOUNTABILITY, BE RESPECTFUL AND INCLUSIVE, AND ACT WITH INTEGRITY.

Ethics Office Foundational Program Elements

 <p>Annual Code Acknowledgment</p>	 <p>Annual Conflicts of Interest Disclosure Questionnaire</p>
 <p>Conflicts Council</p>	 <p>Anonymous, Confidential EthicsLine</p>
 <p>Education & Awareness</p>	 <p>Senior Management/ Board Reporting & Escalation</p>



Our Code of Business Conduct and Ethics forms the foundation of our Ethics Program and helped Fifth Third to be recognized as one of 2021's World's Most Ethical Companies®.

The Code of Business Conduct and Ethics is an important, Board-approved document that serves as a guide to help employees understand how to apply our Core Values to the decisions required of them. **Every employee and contractor is required to review the Code, comply with it and refer to it regularly—and to sign an annual acknowledgment.** In 2020, over 99% of employees and contractors made this acknowledgment, a requirement that is regularly tested and verified.

Additionally, all employees and contractors are required to complete ethics training on an annual basis. In 2020, 99.7% of all required compliance training modules were completed by employees,

including ethics training. Further, ethics training is incorporated into other employee training modules required of employees and contractors depending on specific roles and positions within the Bank. It is important to note that the Board of Directors also undergoes ethics training.

The Code is the foundation of our ethics program at Fifth Third. The foundation helped Fifth Third to be recognized again as one of the 2021 World's Most Ethical Companies®. This honor came from the highly respected Ethisphere Institute, a global leader in defining and advancing the standards of ethical business practices. It puts us in elite company, as **only 135 organizations from around the globe—including only five banks—made the grade.** Ethisphere scores companies in five categories: ethics and compliance, culture of ethics, corporate citizenship and responsibility, governance, and leadership and reputation. Ethisphere also recognized the Bank as one of the World's Most Ethical Companies® in 2019.

ANTI-COMPETITIVE ACTIVITIES

The **Code of Business Conduct and Ethics** outlines Fifth Third's position on anti-competitive activities. Anti-trust laws, also referred to as "competition laws," are rules developed by the U.S. government to protect consumers from predatory business practices. Their goal is to ensure that fair competition exists in the marketplace.

We ensure that business activities that involved any of our competitors are conducted with great care to ensure compliance with all laws and regulations.

Prohibited activities include:

- **Any agreements between competitors** relating to prices, allocations of territories or customers or limitations of products.
- **Use of competitors' confidential or proprietary information.**
- **Engaging in any other anti-competitive behavior,** including disparaging or making false statements in relation to competitors, misappropriating competitors' trade secrets, or encouraging competitors' customers to break contracts.

We are responsible for adherence to the anti-bribery and anti-corruption regulations of the countries in which we operate. This includes the Foreign Corrupt Practices Act, Canada's Corruption of Foreign Public Officials Act, and the U.K. Bribery Act, as well as other applicable laws and regulations. The regulations prohibit bribery of a foreign or domestic government official for the purpose of influencing that official. These regulations apply to conduct both inside and outside of U.S. territory. These regulations also apply to third parties conducting business with Fifth Third such as suppliers and consultants. While Fifth Third has a low risk of anti-bribery and anti-corruption violations, Fifth Third has practices in place for activities that pose a higher risk of violations, such as payments to vendors outside of the United States as well as foreign travel.

ETHICS HOTLINE

Every Fifth Third employee has a responsibility not only to adhere to the Code of Business Conduct and Ethics, but also to raise issues if and when they become aware of misconduct or other violations of our Code. Employees are encouraged to raise questions and concerns directly with their manager or someone in their division's reporting line with whom they feel comfortable talking.

In addition, employees have access to their Human Resources business partner, the Employee Relations Resource Group, Business Security Operations Center, or the Ethics Office, including the 24-hour EthicsLine. Reports can be made to the EthicsLine at any time and employees can choose to remain anonymous. All reports are investigated and taken seriously, and we protect confidentiality to the fullest extent possible. If the investigation determines an employee violation has occurred, prompt corrective action is taken, up to and including termination. Regular reporting of EthicsLine calls is provided to senior management as well as the Audit Committee of the Board.

WHISTLEBLOWER PROTECTIONS

Fifth Third's **Non-Retaliation Policy** for employees who report violations strictly prohibits intimidation of, or retaliation against, individuals who make good faith reports of known or suspected violations of the **Code of Business Conduct and Ethics**, any Fifth Third policy or procedure, or any law or regulation. To ensure

that Fifth Third's non-retaliation practices are robust, the Bank conducts a regular assessment to ensure the policy works as intended and to provide an additional layer of review.

DISCRIMINATION AND HARASSMENT

Discrimination, harassment or intimidation are not tolerated for any reason. This includes discrimination on the basis of an individual's race, color, national origin or ancestry, citizenship status, creed, religion, sexual orientation, transgender status, marital status, civil partnership, pregnancy, parental status or caregiving responsibilities, genetic information, physical or intellectual disability or protected condition, military or veteran status, an individual having been a victim of domestic violence, sexual assault or abuse, or any other status protected under applicable laws. Fifth Third does not require employees to sign mandatory arbitration agreements as a condition of employment or continued employment.*

HUMAN RIGHTS

Striving to be the One Bank that people most value and trust requires operating at the highest ethical standards and upholding the dignity of the individual through every interaction with all we serve,

including customers, employees, communities and shareholders. We support fundamental principles of human rights across all our business activities. Fifth Third's respect for the protection and preservation of human rights is guided by principles set forth in the **United Nations Universal Declaration of Human Rights**.

Our full human rights statement can be found on ir.53.com/esg.



*Fifth Third Securities representatives licensed through the Financial Industry Regulatory Authority have registered representative agreements that require arbitration of claims.

Public Policy and Government Relations

Fifth Third is subject to government regulation and risks generated by new, complex and evolving legislative and regulatory requirements that impact nearly every aspect of our operations.

As a result, customers, employees and shareholders have a measurable stake in the outcome of certain public policy discussions. To mitigate this risk and work toward favorable outcomes, we participate in the public policy process. **Our government affairs program is designed to give us a coordinated voice in public policy through a partnership between the Government Affairs team and Company leaders.**

Fifth Third's advocacy efforts are executed at the local, state and federal level by registered lobbyists. Disclosure of federal lobbying activity occurs via the U.S. Congress, and disclosure of non-federal lobbying activity is provided to appropriate local and state agencies as required by law.

Fifth Third's Political Action Committee supports candidates at the federal, state and local level.

Funds in the PAC consist of voluntary personal contributions from eligible officers of the Company and its subsidiaries. No Company funds are contributed to the PAC. Disclosure of PAC activity can be viewed at [fec.gov](https://www.fec.gov) and our website. Disclosure of PAC activity at the local and state levels is provided to state election authorities in compliance with applicable law.

Fifth Third's political contributions are governed by the **Government Affairs Policy**. The Nominating and Corporate Governance Committee of the Board reviews political contributions semi-annually and approves the policy annually. Fifth Third also maintains a Political Activity Policy that ensures the compliance of the Bank and its employees with laws and regulations governing political contributions. ■



To mitigate legislative and regulatory risks and work toward favorable outcomes, we participate in the public policy process through our government affairs program.

Enterprise Risk Management

Fifth Third Bank has been in business since 1858 and has been successful over this span of years by effectively balancing risk and return.

We take risks every day delivering products and services to customers and executing our business processes and activities. Therefore, **we are responsible for managing these risks effectively to deliver through the cycle value and performance** for our shareholders, customers, employees, and communities.

ALIGNMENT WITH OUR CORE VALUES AND CULTURE

Our Core Values and culture provide a foundation for supporting sound risk management practices by setting expectations for appropriate conduct and accountability across the organization.

Our approach to sound risk management is grounded on each employee living our Core Values and acting in an ethical and responsible manner as we serve the financial needs of our customers and communities.

Our culture is embodied in the Fifth Third Compass, which informs our actions and decisions, from how we navigate our daily work and recognize each other's efforts, to the way we behave with customers, each other and our communities. The Compass also guides our strategic direction and actions as we keep the customer at the center and work toward achieving our Vision to be the one bank people most value and trust.

By focusing on the future and uniting us as one team, the Compass represents who we are, what we believe and how we define success—all of which are key drivers of our risk management strategy.



“Fifth Third’s strong performance is enabled by sound risk management practices that deliver on our commitments to customers, employees, communities and shareholders.”



—BOB SHAFFER, EXECUTIVE VICE PRESIDENT AND CHIEF RISK OFFICER

Fifth Third's Risk Management Framework outlines our approach to managing risk in support of our Vision. Key elements of the Framework are described in detail below.

RISK APPETITE

Fifth Third's risk appetite is established in alignment with our strategic, financial and capital plans. The Board and executive management approve the risk appetite, which is considered in the development of business strategies and forms the basis for enterprise risk management. The risk appetite is defined using quantitative metrics and qualitative measures to ensure prudent risk taking and drive balanced decision making. **Our goal is to ensure that aggregate risks do not exceed Fifth Third's risk appetite,** and that risks taken are supportive of our portfolio diversification and profitability objectives.



The core principles that define our risk appetite and ensure we are operating in a safe and sound manner are:

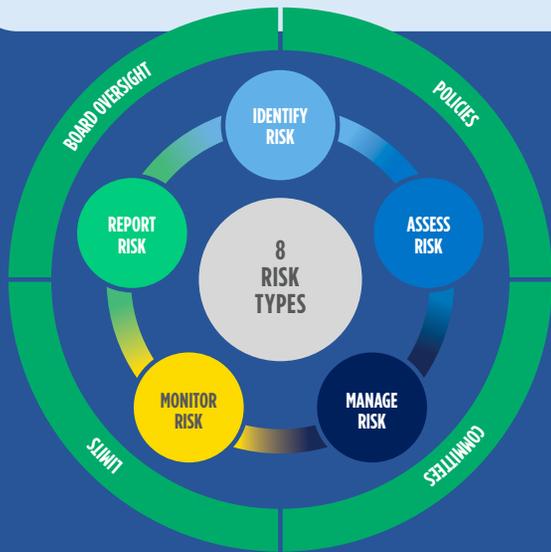
- **We act with integrity** in all activities.
- **We understand the risks we take,** and ensure that they are in alignment with our business strategies and our risk appetite.
- **We avoid risks that cannot be understood, managed or monitored.**
- **We provide transparency of risk to our management and Board** and escalate risks and issues as necessary.
- **We ensure Fifth Third's products and services are aligned to our core customer base** and are designed, delivered and maintained to provide value and benefit to our customers and to Fifth Third.
- **We do not offer products or services that are not appropriate or suitable for our customers.**
- **We are focused on providing operational excellence** by providing reliable, accurate, and efficient services to meet our customers' needs.
- **We maintain a strong financial position** to ensure that we meet our strategic objectives through all economic cycles and are able to access the capital markets at all times, even under stressed conditions.
- **We protect the Bank's reputation by thoroughly understanding the consequences of business strategies, products and processes.**
- **We conduct our business in compliance with all applicable laws, rules and regulations** and in alignment with internal policies and procedures.

Risk Management Process

Our Risk Management Process ensures a consistent and comprehensive approach to how we identify, measure and assess, manage, monitor, and report risks. We also have established processes and programs to **manage and report concentration risks; to ensure robust talent, compensation, and performance management; and to aggregate risks across the enterprise.**

Fifth Third’s eight risk types:

- Credit Risk
- Liquidity Risk
- Interest Rate Risk
- Price Risk
- Operational Risk
- Reputation Risk
- Strategic Risk
- Legal and Regulatory Compliance Risk



THREE LINES OF DEFENSE

Accountability for managing risk is driven through a Three Lines of Defense structure:



FIRST LINE OF DEFENSE

The first line of defense is comprised of front line units that create risk or are accountable for risk.

These groups are the Bank’s primary risk-takers and are responsible for implementing effective internal controls and maintaining processes for identifying, assessing, controlling, and mitigating the risks associated with their activities, consistent with established risk appetite and limits. The first line of defense also includes business units that provide information technology, operations, servicing, processing, or other support.



SECOND LINE OF DEFENSE

The second line of defense, or independent risk management, consists of risk management, compliance, and credit review.

The second line is responsible for developing frameworks and policies to govern risk-taking activities, overseeing risk-taking of the organization, assessing risks and issues independent of front line units, advising on controlling risks, and providing input on key risk decisions. Risk management complements the first line’s management of risk-taking activities through its monitoring and reporting responsibilities, including adherence to the risk appetite. Additionally, the second line is responsible for identifying, measuring, monitoring, and controlling aggregate and emerging risks enterprise-wide.



THIRD LINE OF DEFENSE

The third line of defense is internal audit, which provides oversight of the first and second lines of defense, and independent assurance to the Board on the effectiveness of governance, risk management, and internal controls.

RISK GOVERNANCE

Fifth Third’s risk governance structure ensures proper oversight of risk across the organization. It provides a **path for escalation of risks and issues to management and Board-level committees to drive effective risk decisioning.**

The Board is responsible for actively overseeing risk-taking activities and holding management accountable for adhering to the risk management framework. The Board delegates certain responsibilities to Board Committees, including the **Risk and Compliance Committee** and the **Audit Committee.**

The RCC is the primary committee that oversees risk and **assists the Board in its oversight of the Bancorp’s Risk Management Framework** and approves the framework and primary risk management policies.

The Audit Committee of the Board is the primary committee that has **responsibility, fiduciary duty and authority to oversee the management, financial statements and audit functions.**

The Enterprise Risk Management Committee is chaired by the Chief Risk Officer. It is comprised of senior management and reports to the RCC. The committee is responsible for **reviewing and approving frameworks and policies to ensure effective risk management,** overseeing the management of all risk types to ensure that risks remain within Fifth Third’s risk appetite and fostering a risk culture that supports our risk management objectives.

The ERMCom oversees key management committees responsible for specific risk types and key risk-related policies and processes, in order to support an aggregate view of risk and provide executive-level risk management oversight of all risk types. ■

Fifth Third’s risk governance structure ensures proper oversight of risk across the organization. It provides a path for escalation of risks and issues to management and Board-level committees to drive effective risk decisioning.

Fifth Third’s Risk and Compliance Committee Structure



Consumer Privacy and Information Security

We keep our customer at the center because without our customers, we would not exist.

Keeping the customer at the center of everything we do and delivering a world-class customer experience every time is a top priority and way of life at Fifth Third. When it comes to security and privacy, our customers expect us to protect their financial and information assets and need to know they can trust us to do just that.

As the cyber threat landscape continues to mature, it is our responsibility to stay ahead of the threats and continue to put in place the processes, procedures, tools and technologies needed to mitigate the risks associated with these threats.

Our Information Security team's mission is to relentlessly execute to protect, enable and innovate across our enterprise, to enhance our brand and to raise the level of trust and

Strategic Focus Areas

In January of 2020, we completed our Agile transformation by aligning the entire organization to our Agile design. This established the organizational structure for our focus areas.

IDENTITY FOUNDATIONS

Develop and drive a unified strategy and technology stack that enables future identity verification and access control across internal and customer-facing applications and IT services.

NEXT GENERATION DETECTION AND RESPONSE

Use best-in-class third-party products to “knock down the noise” and focus on the most sophisticated attacks, leveraging a threat intelligence-based approach paired with dynamic and custom detection and response capabilities.

ZERO-TRUST/CLOUD

Build out automated controls for cloud consumption and redesign how employees access the internet and our network utilizing zero-trust principles, meaning organizations should not automatically trust anything inside or outside its perimeters and must verify anything and everything trying to connect to its systems before allowing access.

PROGRAM FOUNDATION

Drive continuous improvement in foundational elements of the Information Security Program, such as Business Continuity, Vulnerability Management, Security for Affiliates, Divisions and Subsidiaries, Metric Generation, Controls Framework and more.

confidence of our customers and partners. We strive to understand cyber threat adversaries and the risks they pose. Our adversaries are nimble and dynamic. To protect against them, our defenses must be the same.

TRANSFORMATION PATH TO STRATEGIC FOCUS

In January of 2020, we completed our Agile transformation by aligning the entire organization to our Agile design. This established the organizational structure upon which we focused on **Program Foundations, Identity Foundations, Next Generation Detection and Response, and Zero-Trust/Cloud.**

Despite the impacts of the COVID-19 pandemic, the team was still able to move forward on these **areas of strategic focus** by:

- **Revamping the vulnerability management reporting capabilities and process** to ensure teams were provided appropriate information to prioritize risk
- **Managing the technology lifecycle of identity related products** to better align with our strategic direction
- **Moving to a threat intelligence-driven process** that allows our detection and response teams to focus on the most advanced attackers
- **Continuing to mature our security in cloud and zero-trust network access solutions**

The hard work and continuous planning and preparation of the Business Continuity Team was highlighted in 2020, as they guided us through not only the pandemic and all its implications, but also a record hurricane season and civil unrest. The Bank also has a cybersecurity incident response plan that addresses cybersecurity events that impact data or operations of the Bank. The plan is aligned with our business continuity crisis management plan as well as our escalation procedures for sensitive information, which is overseen by the Bank’s Privacy Office.

PRIVACY AND DATA SECURITY

The Bank has established a strong foundation of governance, policies and procedures based on a tight alignment with regulatory requirements and standard frameworks such as National Institute of Standards and Technology and Control Objectives for Information Technologies. This foundation, combined with regular program assessments by outside organizations, keeps the Information Security team more alert to cyber risk, more deliberate in building dynamic defenses to protect our customers and the Bank, and more collaborative in exploring effective solutions with both internal and external partners.



Fifth Third’s commitment to data security and privacy are available on [53.com](https://www.fifththird.com/53.com).

Fifth Third also is committed to protecting our customers through our privacy policies. These policies describe **the information we collect, the information customers provide when using our products and services, and information about when customers can choose to limit data sharing** based on state, federal and international regulations. Details of our commitment to privacy and data security can be found on [53.com](https://www.fifththird.com/53.com) on our **[Privacy and Security page](#)**.

We have implemented measures designed to secure customer information from loss or unauthorized access, use, alteration or disclosure. Information is stored on secured servers behind firewalls, and all data transported on our website and mobile applications is encrypted. To further help protect information, the Bank requires employees to review and know information security and privacy policies. **All employees and contractors are required to complete privacy and information security training on an annual basis, including: privacy compliance, information lifecycle governance, managing information and data, creating a safe cyber environment and business continuity.** In 2020, 99.7% of all required compliance training modules were completed by employees, including privacy and information security training modules.

Internal and external assessments are conducted regularly to ensure our defenses are solid, that we are meeting regulatory requirements and that we are continually maturing the Information Security program.

To ensure the Bank’s third-party suppliers take information security and privacy as seriously as Fifth Third does, our **Master Services Agreements include extensive articles on information technology security requirements and breach procedures** as well as confidentiality and protection of nonpublic personal information.

Our Master Services Agreement articles **identify expectations**, including, but not limited to:

- **What the supplier’s information security program should include**
- **Who needs to review and approve** their information security program
- **What safeguards need to be in place**
- **How the Bank should be notified** of a breach
- **How proprietary information should be handled**

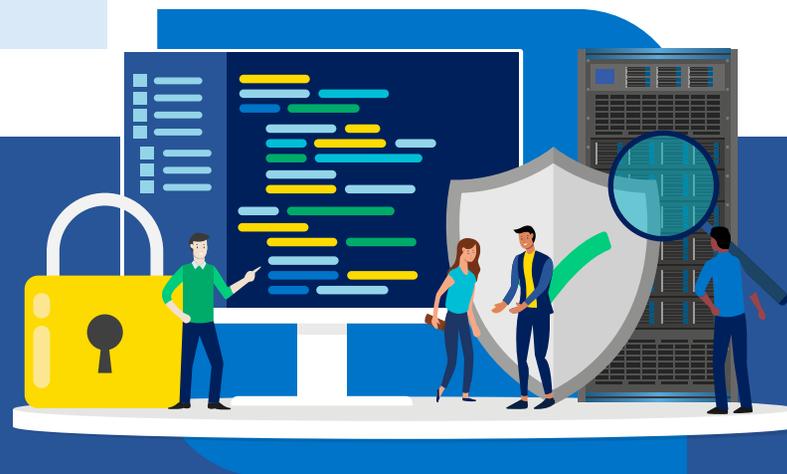
Ensuring our third-party suppliers are doing all they can to protect the Bank and our customers is another way we keep the customer at the center of everything we do.

THE VALUE OF STRONG LEADERSHIP AND GOVERNANCE

Information security and privacy teams regularly report to executive leadership and the Board to ensure everyone is aligned to the Bank’s priorities and focus.

- The **chief information security officer and Privacy Office** report regularly to the Board or Board committees to keep abreast of all efforts to prevent, detect and respond to risks.

Internal and external assessments are conducted regularly to ensure our defenses are solid and that we are meeting or exceeding all regulatory security requirements.



- The **Technology Committee**, a committee of the Board established in 2020, is comprised of Board members with extensive technology backgrounds. Its primary purpose is to assist the Board in its oversight of technology and innovation strategies, plans and operations, information, cybersecurity and data privacy risk management and third-party technology risk management.

TRAINING AND TESTING KEEP THE FOCUS ON SECURITY AND PRIVACY

Our employees and contractors are included in our first line of defense. Keeping them informed and educated helps them to make the right decisions when it comes to protecting the information they work with every day. To do this, we have a mature security awareness and education program. The program includes **annual training for all users, targeted security awareness training for high-risk audiences, weekly security awareness communications, quarterly lunch and learns, and a variety of activities**, including a conference, during National Cyber Security Awareness Month in October.

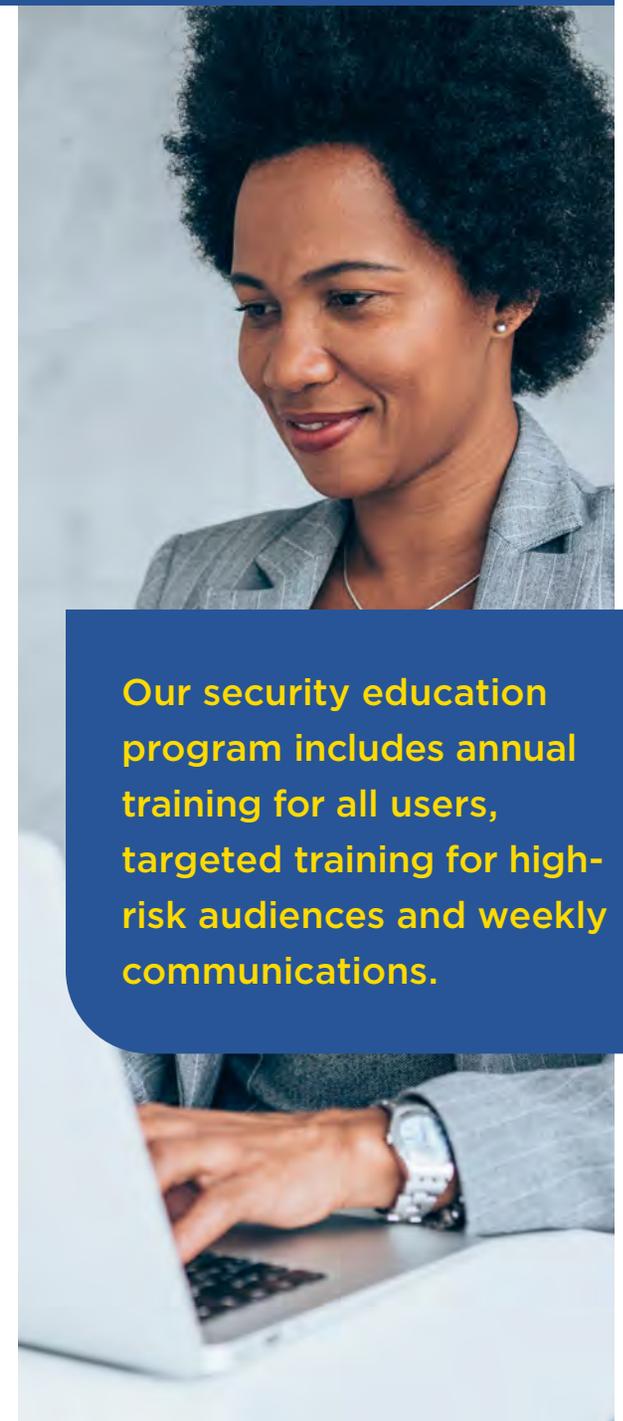
As part of our Information Lifecycle Governance program, all information owners are made aware of the expectation to defensibly delete data once it has reached the end of its lifecycle.

The end-of-life lifecycle for data is determined by the Corporate Records Retention Schedule's retention trigger data.

In addition to security awareness and information lifecycle governance training, our Learning and Development team provides a variety of compliance courses. Some are required learning for all employees and contractors while others are designed for specific audiences.

To test our education efforts and provide program direction, **the Bank conducts regular simulated phishing exercises and desk checks** to ensure employees and contractors are following policies and standards. Desk checks had to be put on hold during the pandemic but will begin again when considered safe to do so.

The Information Security team has established and maintains a qualified and representative workforce, ensuring that the right people with the right skills are in place to achieve our business goals. To that end, **the organization invests heavily in ongoing training and certifications for its team members**. This includes technical boot camps as well as online and classroom training and conferences. The inventory of training is extensive, aligns with certification opportunities and is provided via various mediums. ■



Our security education program includes annual training for all users, targeted training for high-risk audiences and weekly communications.

BUSINESS CONTINUITY MANAGEMENT

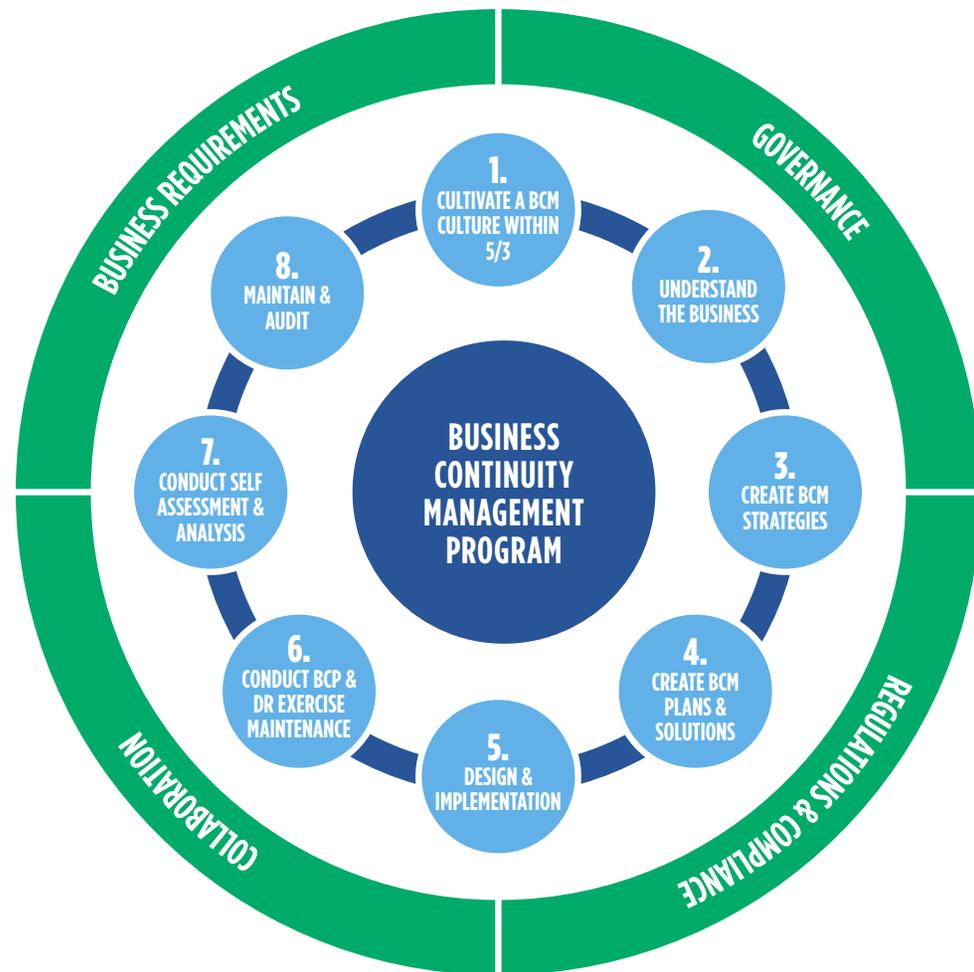
Business Continuity Management (BCM) provides a framework and holistic process for building organizational resilience with the capability of an effective response that safeguards the interests of its customers, employees, reputation, brand and value-creating activities. We do this by identifying core services and the processes and technologies that underpin them and then, once that ‘analysis’ is complete, developing plans and strategies that will enable the business to continue operations and effectively recover from any type of event, regardless of cause or impact.

PROGRAM OBJECTIVES:

- **Integrate BCM, Disaster Recovery and Event Management responsibilities and activities into a BCM Program** that fully adheres with regulatory requirements and aligns with meeting needs of the business
- **Plan for, mitigate and manage threats and risks BEFORE they impact Fifth Third**, including conducting cyber war games and disaster recovery exercises
- **Enable the Company to continue to operate when faced with adverse conditions**
 - Not just Information Technology, but all core business processes
 - Not just catastrophic disasters, but all potential exposures

Business Continuity Management Lifecycle

The BCM Program functions within an integrated 8-step lifecycle. The following steps outline the approach that is taken to define, implement, mature, and evaluate the BCM program.



Third-Party Management

Fifth Third has a robust third-party management program for the acquisition of goods and services.

Our Supplier Code of Conduct sets forth Fifth Third's expectations for ethical, human rights, labor and environmental standards throughout our supplier network.



We execute our third-party selection process in accordance with the highest standards of integrity, fairness and objectivity. Our Supplier Diversity team reviews every procurement opportunity to ensure diverse providers are included in the portfolio of potential third parties. Thorough assessment and due diligence is performed on all third-parties prior to onboarding, with focused attention on protection and security of Bank and customer data.

The Bank focuses on fostering a strong risk and compliance culture, meaning all employees are responsible and accountable for managing risks associated with third-party relationships.

It is expected that Fifth Third suppliers demonstrate the same level of commitment to ethical business practices.

Our goal is to meet the strategic objectives of the Bank and maintain our commitment to providing equal opportunities to all capable suppliers. To achieve this goal, we seek strategic partnerships with highly qualified sources who provide solutions that improve our processes, increase the quality of our products and services and drive efficiencies.

The methodology and process for third-party risk management is as follows:

- **Governance of our third-party activities begins with the Third Party Management Council, which assesses the portfolio of third-party service providers as well as the management of risks, issues and performance on the third-party population and oversees adherence to the Third Party Risk Management Policy and Program.**
- **The Third Party Management Council reports to the Operational Risk Committee, which in turn is accountable to the Enterprise Risk Management Committee and the Risk and Compliance Committee.**

[FULL PROCESS DETAILED ON NEXT PAGE](#) ►

Third-Party Risk Management



INITIATION & SELECTION

Fifth Third seeks to strategically partner with highly qualified third parties that provide solutions that improve our processes and service levels, increase the quality of our products and services and reduce our total costs while meeting Fifth Third Bank's risk management and compliance expectations. We also believe that promoting supplier diversity is an integral part of our success and we are proud of the many alliances and partnerships we have with diverse companies throughout our footprint.

Promoting supplier diversity is an integral part of our success.

DUE DILIGENCE REVIEW

After initiation and selection is complete but prior to the execution of a contract, we conduct due diligence to evaluate: the risk a third party product/service may present to the Bank; the third party's ability to manage all risk matters related to the individual product(s) purchased or service(s) being performed; the strength of the third party control environment; and the third party's ability to effectively mitigate risk.

CONTRACT

This phase produces and secures a contract that details the obligation of the third party, inclusive of standard contract language and other legal requirements (terms and provisions), Service Level Agreements, and appropriate signoffs. SLAs include remedies for non-performance, and are designed to recognize and address issues in a timely manner.

ONBOARDING

Fifth Third sets up payment and executes on the required oversight and monitoring that occurs while developing a formal monitoring and testing plan.

ONGOING MONITORING

The level of ongoing monitoring required for each third party is determined by the level of risk the third party poses to the Bank. Formalizing ongoing monitoring allows the Bank to properly monitor third party performance and remediate any issues that arise during the relationship.

TERMINATION

Unfortunately, there are events that at times may cause one or both parties to terminate the relationship. If this is required, the Bank proceeds in a professional manner, in accordance with the terms of the contract with the third party. ■